Crypto Forum
Internet-Draft
Intended status: Informational
Expires: 10 May 2026

D. Connolly
SandboxAQ
R. Barnes
Cisco

6 November 2025

Concrete Hybrid PQ/T Key Encapsulation Mechanisms
draft-irtf-cfrg-concrete-hybrid-kems-02

Abstract

PQ/T Hybrid Key Encapsulation Mechanisms (KEMs) combine "post-quantum" cryptographic algorithms, which are safe from attack by a quantum computer, with "traditional" algorithms, which are not. CFRG has developed a general framework for creating hybrid KEMs. In this document, we define concrete instantiations of this framework to illustrate certain properties of the framework and simplify implementors' choices.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://cfrg.github.io/draft-irtf-cfrg-concrete-hybrid-kems/draft-irtf-cfrg-concrete-hybrid-kems.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-irtf-cfrg-concrete-hybrid-kems/.

Discussion of this document takes place on the Crypto Forum Research Group mailing list (mailto:cfrg@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email_list=cfrg. Subscribe at https://www.ietf.org/mailman/listinfo/cfrg/.

Source for this draft and an issue tracker can be found at https://github.com/cfrg/draft-irtf-cfrg-concrete-hybrid-kems.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

PQ/T Hybrid Key Encapsulation Mechanisms (KEMs) combine "post-quantum" cryptographic algorithms, which are safe from attack by a quantum computer, with "traditional" algorithms, which are not. Such KEMs are secure against a quantum attacker as long as the PQ algorithm is secure, and remain secure against traditional attackers even if the PQ algorithm is not secure.

[HYBRID-KEMS] defines a general framework for creating hybrid KEMs. It includes multiple specific mechanisms for combining a PQ algorithm with a traditional algorithm, with different performance properties and security requirements for the underlying algorithms.

In this document, we describe instances of these different specific combiners, with specific choices for the underlying algorithms. The choices described here illustrate the security analysis required to make choices that meet the requirements of the general framework, and can serve as a baseline for application designers. We also provide test vectors for these instances so that implementors can verify the correctness of their implementations.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

We make extensive use of the terminology in [HYBRID-KEMS].

3. Concrete Nominal Group and KEM Instances

This document introduces concrete hybrid KEM instances that in turn depend on concrete KEM and nominal group instances. This section introduces the nominal groups and KEM instances used for concrete hybrid KEM instances, specified in line with the abstraction from [HYBRID-KEMS]. Section 3.1 defines the concrete nominal groups, and Section 3.2 defines the nominal KEMs.

3.1. Nominal Groups

This section specifies concrete nominal groups that implement the abstraction in [HYBRID-KEMS]. It includes groups based on the NIST curves P-256 and P-384, as well as a group based on Curve25519.

3.1.1. P-256 and P-384 Nominal Groups

The NIST P-256 and P-384 elliptic curves are defined in [SP800-186]. They are widely used for key agreement and digital signature. In this section, we define how they meet the Nominal Group interface described in [HYBRID-KEMS].

Group elements are elliptic curve points, represented as byte strings in the uncompressed representation defined by the Elliptic-Curve-Point-to-Octet-String function in [SEC1]. Scalars are represented as integers in big-endian byte order.

The Nominal Group algorithms are the same for both groups:

* Exp(p, x) -> q: This function computes scalar multiplication between the input element (or point) p and the scalar x, according to the group law for the curve specified in [SP800-186].

* RandomScalar(seed) -> k: Implemented using rejection sampling from a seed, as described below.

* ElementToSharedSecret(p) -> ss: The shared secret is the X coordinate of the elliptic curve point p, encoded as an Nss-byte string using the Field-Element-to-Octet-String function in [SEC1].

Given a seed, the RandomScalar algorithm is defined as follows:

```
def RandomScalar(seed):
  start = 0
  end = Nscalar
  sk = OS2IP(seed[start : end])

  while sk == 0 || sk >= order:
    start = end
    end = end + Nscalar
    if end > len(seed):
        raise Exception("Rejection sampling failed")
    sk = OS2IP(seed[start : end])
  return (sk, pk(sk))
```

RandomScalar fails with cryptographically negligible probability, as long as the input seed is uniformly random. (The chance of a single rejection is < 2^-32 for P-256 and < 2^-192 for P-384. The chance of more than Nreject rejections is thus < 2^-128 for P-256 and < 2^-192 for P-384.)

The OS2IP function converts a byte string to a non-negative integer, as described in [RFC8017], assuming big-endian byte order. The order variable represents the order of the curve being used (see Section 3.2.1 of [SP800-186]), reproduced here for reference:

P-256:
0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

P-384:
0xffffffffffffffffffffffffffffffffffffffffffffffffc7634d81f4372ddf
581a0db248b0a77aecec196accc52973

The group constants for the P-256 group are as follows:

* Nseed: 128

* Nscalar: 32

* Nelem: 65

* Nss: 32

The group constants for the P-384 group are as follows:

* Nseed: 48

* Nscalar: 48

* Nelem: 97

* Nss: 48

3.1.2. Curve25519 Nominal Group

The following functions for the Curve25519 nominal group are defined:

* Exp(p, x) -> q: Implemented by X25519(x, p) from [RFC7748].

* RandomScalar(seed) -> k: Implemented by sampling and outputting 32 random bytes from a cryptographically secure pseudorandom number generator.

* ElementToSharedSecret(p) -> ss: Implemented by the identity function, i.e., by outputting P.

The following constants are also defined.

* Nseed: 32

* Nscalar: 32

* Nelem: 32

* Nss: 32

3.2. Concrete KEM Instances

This section specifies concrete KEM instances that implement the KEM abstraction from [HYBRID-KEMS].

3.2.1. ML-KEM-768 and ML-KEM-1024

The ML-KEM-768 and ML-KEM-1024 KEMs are defined in [FIPS203]. The algorithms defined in that specification map to the KEM abstraction in [HYBRID-KEMS] as follows:

* GenerateKeyPair() -> (ek, dk): Implemented as KeyGen in Section 7.1 of [FIPS203].

* DeriveKeyPair(seed) -> (ek, dk): Implemented as KeyGen_internal(seed[0:32], seed[32:64]), where KeyGen_internal is defined in Section 6 of [FIPS203].

* Encaps(ek) -> (ct, ss): Implemented as Encaps in Section 7.2 of [FIPS203].

* Decaps(dk, ct) -> ss: Implemented as Encaps in Section 7.3 of [FIPS203].

The KEM constants for ML-KEM-768 are as follows:

* Nseed: 64

* Nek: 1216

* Ndk: 32

* Nct: 1120

* Nss: 32

The KEM constants for ML-KEM-1024 are as follows:

* Nseed: 64

* Nek: 1629

* Ndk: 32

* Nct: 1629

* Nss: 32

3.3. Concrete PRG instances

This section specifies concrete PRG instances that implement the PRG abstraction from [HYBRID-KEMS] and meet the required security definitions.

3.3.1. SHAKE256

SHAKE256 is an extendable-output function (XOF) defined in the SHA-3 specification [FIPS202]. It can be used as a PRG for arbitrary values of Nout. When SHAKE256 is used as the PRG component in a hybrid KEM, it is implcit that Nout == KEM_T.Nseed + KEM_PQ.Nseed or Nout == Group_T.Nseed + KEM_PQ.Nseed as appropriate.

3.4. Concrete KDF instances

This section specifies concrete KDF instances that implement the KDF abstraction from [HYBRID-KEMS] and meet the required security definitions.

3.4.1. SHA-3

The SHA-3 hash function is defined in [FIPS202]. It produces a 32-byte output, so it is appropriate for use in hybrid KEMs with Nss = 32.

4. Concrete Hybrid KEM Instances

This section instantiates the following concrete KEMs:

MLKEM768-P256: A hybrid KEM composing ML-KEM-768 and P-256 using the CG framework, with SHAKE256 as the PRG and SHA3-256 as the KDF.

MLKEM768-X25519: A hybrid KEM composing ML-KEM-768 and Curve25519 using the CG framework, with SHAKE256 as the PRG and SHA3-256 as the KDF. This construction is identical to the X-Wing construction in [XWING-SPEC].

MLKEM1024-P384: A hybrid KEM composing ML-KEM-1024 and P-384 using the CG framework, with SHAKE256 as the PRG and SHA3-256 as the KDF.

Each instance specifies the PQ and traditional KEMs being combined, the combiner construction from [HYBRID-KEMS], the label to use for domain separation in the combiner function, as well as the PRG and KDF functions to use throughout.

4.1. MLKEM768-P256

This hybrid KEM combines ML-KEM-768 with P-256 using the CG framework from [HYBRID-KEMS]. It has the following components:

* Group_T: P-256 Section 3.1.1
* KEM_PQ: ML-KEM-768 Section 3.2.1
* PRG: SHAKE-256 [FIPS202]
* KDF: SHA3-256 [FIPS202]
* Label: MLKEM768-P256 (hex: 4d4c4b454d3736382d50323536)

The KEM constants for the resulting hybrid KEM are as follows:

* Nseed: 32
* Nek: 1217
* Ndk: 32
* Nct: 1121
* Nss: 32

4.2. MLKEM768-X25519

This hybrid KEM combines ML-KEM-768 with X25519 using the CG framework from [HYBRID-KEMS]. It is identical to the X-Wing construction from [XWING-SPEC]. It has the following components:

* KEM_PQ: ML-KEM-768 Section 3.2.1
* Group_T: Curve25519 Section 3.1.2
* PRG: SHAKE-256 [FIPS202]
* KDF: SHA3-256 [FIPS202]
* Label: \.//^\ (hex: 5C2E2F2F5E5C)

The following constants for the hybrid KEM are also defined:

* Nseed: 32
* Nek: 1216
* Ndk: 32
* Nct: 1120
* Nss: 32

4.3. MLKEM1024-P384

This hybrid KEM combines ML-KEM-1024 with P-384 using the CG framework from [HYBRID-KEMS]. It has the following components:

* Group_T: P-384 Section 3.1.1
* KEM_PQ: ML-KEM-1024 Section 3.2.1
* PRG: SHAKE-256 [FIPS202]
* KDF: SHA3-256 [FIPS202]
* Label: MLKEM1024-P384 (hex: 4d4c4b454d313032342d50333834)

The following constants for the hybrid KEM are also defined:

* Nseed: 32
* Nek: 1629
* Ndk: 32
* Nct: 1629
* Nss: 32

5. Security Considerations

The Security Considerations section in generic hybrid KEM framework lays out the requirements for component algorithms in order for a hybrid KEM constructed according to the framework to be secure [HYBRID-KEMS]. In brief:

* A nominal group needs to be one in which the Strong Diffie-Hellman problem is hard.

* A KEM need to be IND-CCA secure.

* When the C2PRI combiner is used (as it is here), the PQ KEM also needs to satisfy the C2PRI property.

* KDFs need to be indifferentiable from a random oracle, even by a quantum attacker.

* A PRG needs to be a secure pseudo-random generator

The components used in this document meet these requirements:

* The security of X25519, P-256, and P-384 as nominal groups is shown in [ABH_21].

* ML-KEM is shown to be IND-CCA in https://eprint.iacr.org/2024/843 and shown to be C2PRI in [XWING].

* The sponge construction used by SHA3-256 is shown to be indifferentiable from a random oracle by a classical attacker in [BDP_08]. Indifferentiability with respect to quantum attackers is shown in [ACM_25].

* Since SHAKE256 is built on the same sponge construction as SHA3-256, it is also indifferentiable from a random oracle, which is a sufficient condition for being a secure pseudorandom generator.

6. IANA Considerations

This document requests that the following values be added to the "Hybrid KEM Labels" registry:

Label	Fw	PQ Component	T Component	KDF	PRG	Nseed	Nss	Reference
"|-()-|"	CG	ML-KEM-768	P-256	SHA3-256	SHAKE-256	32	32	[RFCXXXX]
"\.//^\"	CG	ML-KEM-768	Curve25519	SHA3-256	SHAKE-256	32	32	[RFCXXXX]
" | /-\"	CG	ML-KEM-1024	P-384	SHA3-256	SHAKE-256	32	32	[RFCXXXX]

Table 1: Hybrid KEM Labels

[RFC EDITOR: Please replace "XXXX" above with the number assigned to this RFC]

7. References

7.1. Normative References

[FIPS202] "SHA-3 standard :: permutation-based hash and extendable-output functions", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.202, 2015, <https://doi.org/10.6028/nist.fips.202>.

[FIPS203] "Module-lattice-based key-encapsulation mechanism standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.203, August 2024, <https://doi.org/10.6028/nist.fips.203>.

[HYBRID-KEMS] Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-07, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-07>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/rfc/rfc7748>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/rfc/rfc8017>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[SP800-186]
Chen, L., Moody, D., Regenscheid, A., Robinson, A., and K. Randall, "Recommendations for Discrete Logarithm-based Cryptography:: Elliptic Curve Domain Parameters", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-186, February 2023, <https://doi.org/10.6028/nist.sp.800-186>.

7.2. Informative References

[ABH_21] Alwen, J., Blanchet, B., Hauck, E., Kiltz, E., Lipp, B., and D. Riepel, "Analysing the HPKE standard.", April 2021.

[ACM_25] Alagic, G., Carolan, J., Majenz, C., and S. Tokat, "The Sponge is Quantum Indifferentiable", 2025, <https://eprint.iacr.org/2025/731.pdf>.

[ANSIX9.62]
ANSI, "Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA)", ANS X9.62-2005, November 2005.

[BDP_08] Bertoni, G., Daemen, J., Peeters, M., and G. V. Assche, "On the Indifferentiability of the Sponge Construction", 2008, <https://www.iacr.org/archive/eurocrypt2008/49650180/49650180.pdf>.

[CDM23] Cremers, C., Dax, A., and N. Medinger, "Keeping Up with the KEMs: Stronger Security Notions for KEMs and automated analysis of KEM-based protocols", 2023, <https://eprint.iacr.org/2023/1933.pdf>.

[KSMW2024] Kraemer, J., Struck, P., and M. Weishaupl, "Binding Security of Implicitly-Rejecting KEMs and Application to BIKE and HQC", n.d., <https://eprint.iacr.org/2024/1233>.

[RFC5915] Turner, S. and D. Brown, "Elliptic Curve Private Key Structure", RFC 5915, DOI 10.17487/RFC5915, June 2010, <https://www.rfc-editor.org/rfc/rfc5915>.

[SCHMIEG2024]
Schmieg, S., "Unbindable Kemmy Schmidt: ML-KEM is neither MAL-BIND-K-CT nor MAL-BIND-K-PK", 2024, <https://eprint.iacr.org/2024/523.pdf>.

[SEC1] "Elliptic Curve Cryptography, Standards for Efficient Cryptography Group, ver. 2", 2009, <https://secg.org/sec1-v2.pdf>.

[XWING] "X-Wing: The Hybrid KEM You've Been Looking For", 2024, <https://eprint.iacr.org/2024/039.pdf>.

[XWING-SPEC] Connolly, D., Schwabe, P., and B. Westerbaan, "X-Wing: general-purpose hybrid post-quantum KEM", Work in Progress, Internet-Draft, draft-connolly-cfrg-xwing-kem-09, 1 September 2025, <https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem-09>.

Appendix A. Test Vectors

This section provides test vectors for the three concrete hybrid KEM instantiations defined in this document. Each test vector represents a single key generation followed by an encapsulation:

* seed - the seed used for deterministic key generation
* decapsulation_key - the derived decapsulation key
* decapsulation_key_pq - the decapsulation key sub-key for the PQ component
* decapsulation_key_t - the decapsulation key sub-key for the T component
* encapsulation_key - the derived encapsulation key
* randomness - the randomness used for encapsulation
* ciphertext - the ciphertext produced by the encapsulation operation
* shared_secret - the shared secret produced by the encapsulation operation

The seed and randomness values are opaque random values, as are the decapsulation_key and shared_secret fields (as defined by the hybrid KEM specifications). The encapsulation_key and ciphertext fields reflect the concatenated encapsulation keys and ciphertexts (in (PQ, T) order) called for in the hybrid KEM specifications.

The decapsulation_key_pq values are ML-KEM expanded private keys in the format defined by [FIPS203]. The decapsulation_key_t values for X25519 are simply opaque 32-byte strings. The decapsulation_key_t values for the NIST curves are big-endian integers reflecting the private scalar value for the private key. This format is identical to the privateKey value used in the PKCS#8 format for private keys [RFC5915].

A.1. MLKEM768-P256

```
seed = 0000000000000000000000000000000000000000000000000000000000000000
       0000000
randomness = 6464646464646464646464646464646464646464646464646464646464
             4646464646464646464646464646464646464646464646464646464646
             6464646464646464646464646464646464646464646464646464646464
             4646464646464646464646464646464646464646464646464646464646
             6464646464646464646464646464646464646464646464646464646464
             4
encapsulation_key = 3d209f716752f6408e7f89bceef97ac3885300453779
                    27644ef046c0a7cae978c8841a0133aac4f1e1a70272
                    77f671219cf58b85d29c8fec08edd432e787a3cf9936
                    fe0026a113cb9efb1d7214049527bfe2141ea170b029
                    4a59403ab0ce16760a8baa95b823cbb8aacdcc17ef32
                    775223c791e3740163941f9bb3f63346bef1c050c31f
                    932c62719429aff14c2bd438ab135bed692d56c77c04
                    cbbffd6335b578318b513771e84b14ea821262141ca0
                    06ccb8bf2500aa1008970f216fe7f1ae34125aa29049
                    2c069a189222adc322f97649c762c7d3128ad3bb2667
                    971d0744014bc3b67445cbcd0b3e7ea69fb1cb9f9c33
                    1f97487920187292926d04a25a2650abbd44982bb0c3
                    c6301fe6a61330d24d8a3c7021dc3e3392c79a139b37
                    613bba67a2984298507b84a4d61eef18acfb979af2d3
                    9caa4c0db4513815359d76fc378c63a7f4f3053b1716
                    8d0221cf0c2eec5514ba235f81d04d67c3b5c5180949
                    17671c26a7c046457533cc32844581277a03eb065c45
                    29a779a9a5878f2aac3f81db9ed3d8c9345697058cbb
                    99d379bca16d8fdb61d129960390524791b9d3e501b9
                    00bd1e5002e095be06c23f1fb212f5801f24b6b28c0c
                    5493d246d02aa29fa3acfbe15ac4e212eb0b6f69ebbe
                    a259a2703aa4c308224bdb741c65c7a5d4bff7882795
                    07bbfe513d7aa5694e7b3cdf62ab36432742d4a0ca9b
                    3570ba742fa803b46989c8526ea586cc4fc32866143b
                    79601725fa545fd280b404530318bbc3371194710b6d
                    74beaa629eb18a36a953b75915ae96999ba5c88cdc56
                    a46861c50032c9b630bcc1445a30878979bc55a2c095
                    5bf399b231203b90c651b6afe0e242b5a543250b142f
                    7291ed753d816098f7913302a8ce91641716623d4fc2
                    ac6772aa5f3674042b7c4a18a2186289a4ac4e200774
```

```
                        596ca03e6798c7506b984999db6ac142586bae0799f1
                        e776f9f5247dc574d8556ddf9bbbc4ca3643263457f7
                        4248010d62d4311268360aecb4902b450bf2050ecb8b
                        a7a92820d233f5a14ed31225a1d17ca6f19e825894cf
                        b1807d922cbd60761134be419144bcf72006366a4460
                        137ad9136c113f05eb54c409520edc72e4150cc3a24b
                        0f819eec11bbd19ca9645b0810a60b4a8a9e9c395539
                        6a1653955b047bcf4f98433c27236c570d75f809e44a
                        af2dc33665826351872c293350ab324518c8c0c80b52
                        1c80c81a56bdc968a5650315a830c8bb17532c62ccc2
                        3b1d46412c256b224fd4674491803501d0143125c757
                        7239689965b6989ca561793c0f85c62a9e13487da176
                        62a7188c70b1040a67ed4c3f85e74e3691822fb96314
                        d6134fe6a626b3cbe1461d62a7b573b2cc75579ffa22
                        967e36ceb2a1aa0b71875a22751d706b72ca9ecd0c81
                        00ad0aa58009a5c83fffe91759e6baa0a9345af99fe3
                        b69509dbc84032868844ab3f65bb1df8beadf36442e4
                        8e339c967023a525411544c789a2f04dacd06ffef783
                        02210450b931f6b4c32aab34a3f5260b810f4c9a946f
                        c22d3baabaa80ba8d9955d6dc35e8609b4256b482cdc
                        9d8977c1a47a354e7c527fdb1672e166917b95cd6351
                        820261daab361f8a2dcbb240c55abd6a8105e5291b42
                        7b566d731e6b7047189cff20d8b120e0b3e72472d1b0
                        086812200fd3698e23f06e4f4e08bbb54cc2049c039c
                        845be659999c8fa48d7f62327c146cf1bc0b0bb1b91b
                        30174b7bc220d422023bff6b0dee263532c503f3982e
                        4d3e27071b855578a9a9aa63b8a8c339bf
   decapsulation_key = 0000000000000000000000000000000000000000000000000
                        0000000000000000000
   decapsulation_key_pq = f5977c8283546a63723bc31d2619124f11db46586
                           43336741df81757d5ad3062221e124311ec7f7181
                           568de7938df805d894f5fded465001a04e260a494
                           82cf5
   decapsulation_key_t = e00b3f9d338de90488973787b0916a4a9ae8bebf4e
                          2bc07a7bc18f1a62215182
   ciphertext = d81018a94f8078e02105beaa814e003390befa4589bb614f773
                97af42d8e8150796f2c88a4efca81b8cf93c0ae3716c54ec1b0
                45e3875f38c2dd12d7f717bd7fb701a9fecda5ed8b764c9a35d
                4a5c1d8930f6071f653eebb2d1afa77debb8302d16f17e0f5f3
                920a71a4d49beafa0e1c7e443f8abca64a65a9e81a97e7357bf
                902573363c0e1a12e5228036828e3f759121fada92441fe334e
                85d79347e470d2fed945541d832c54baaa3cb7526c3853954db
                4f73547cc7c27fd38398bfa7704952cb841e38b270e4db7435f
                0ee22f57d7ad3270bd0c88e71b4b864cf2277c65daa10a6dad4
                c7abecd95cc4ebec39c08404b522e4ecc1545713f76bebd3b5a
                0f2feb3461936065dbd13f6a1f61e1b142a2af2e5a482ba2c50
                cf0317049c0b3bfd6d5e9240eba9111d2030fdea17e33b65240
                20d30b0c4f8069285f3a6ca267d287d01e827d8422bf5426e11
```

```
                688bfc73756af1841b1c87e126cb50c914b5b2b8673488ad3b0
                74cad77a3840eb12dd688f313ee1e9ff8c479a678f276356fc9
                d65e1d5b4c1e9855b4175db144f7767c12061769190fe6b5e51
                563b91f94d131a2b796bd2980ed0dab4ae7a7110e920007a757
                158a5eb8662cbf89ddffe9d8196821313cdc00108853fc4746b
                111d5b56da638d8ed2973918960f5dfe93ead3ae521e957cec3
                c8d843e8fce234c70ad055177f235439d6098bdd771b1cfcfad
                aab4f50a7378185c62409f383c8ff658c2a2af66498cfd81e96
                2766ac6b774e88424fb4f331837d0a28502708477caf8780a15
                6d723f68fca791e1cd2397bfc2b24c77c765d9b2af36f732d52
                107517efd8157b283b440a613f756c364ca108971a8878199a9
                3f260baec3e850033cc032c2e53f823576affb4d3b116e2d160
                49152c35aaa263ab376f0ad5ede6a749607a283e3016e62191c
                0e8fde33e718cd989591c9a205d608d99fcb8a7471603d716cb
                01b56328d7d880aec2851f4e6d8b5016c25647e9026ebb44154
                3e8012dbfcf078d4012b8c39184dd64f3821b4774ae4e36365f
                8baf2bd1f6667c017a1e65ff8a1554458fb3f367c02721752bf
                a56fc7fd566ae95ffb208f919ef12f4cf8a2fdd141a8df559bd
                db7b8d1f04ee6d4cf7805d142989caf216dfae985faaab9974f
                6d9f8aa1129084db8db912b1655f595ffbaa66491ab4655fd73
                4cfd4bb0c0289d4bcc8fc5e9943b351cb147c8db059a24004d1
                c3e3bb4c14a881e5101acb736c65c5d579acb67ee85a560277b
                43338fe79d34b772c5da001da3b5a3383dd81319a0b4542e6d7
                e46eed5314cc70eb231de27b6e760db598ba19995cf69be0e44
                58e35f3f274aca2455d43fe3344e183c6dc47c857dbe9907b41
                e41006d91b25adcafc098fe66f7554be8dad493c4f4b1dbf7a5
                1464139db474afab5572f92a2232b59be56a72c0505149dae5c
                de1e602877037de7802b5f6fa47a4c9a3e52d6ca15339920254
                e9ffb53c7b834cc0288ed9905a1841e9390ea94a8898bd4c6b6
                d6027e4d43c7867242515bbeefe12340fc04428a824ea7cf56a
                d2a64ed368b71315d80cee846007cff1d2eea2c3f0f92153730
                4ae598f98dd10d1f102811a4e2d161c3fd8bbb193d4b25bee95
                0ac839c0f9d
   shared_secret = 9bd018e869bb01b63fb8f5da374a73d347ea14cb2bc570b1
                   3d0908e2288ec456

   seed = 0101010101010101010101010101010101010101010101010101010101010
          1010101
   randomness = 6565656565656565656565656565656565656565656565656565656
                5656565656565656565656565656565656565656565656565656565
                6565656565656565656565656565656565656565656565656565656
                5656565656565656565656565656565656565656565656565656565
                6565656565656565656565656565656565656565656565656565656
                5
   encapsulation_key = ec7b50cddc8360f98b189bac73d395ef947b37d84538
                       86a253269f7b18b9eb78c1b63212471a0f979793f993
                       6b3f496f4b5394ea69c2a35729f91c688f6bbbb864cd
                       5e87108676c4014c2ba98204f911becae33a71e832ac
```

012bb827578810955f8c6e2d26c0b17b7ba574990884
546ba58bf6785721f3854f434cfea602e8595c71642e
8d4c70934b7e54c638f5a13e1a136bc86565e6b40abc
163ca65650baf953de7bb99b138ac1b695023103c9b4
17853c9d42e54fdb816174659d85a783e3d4613db1cb
baa63fb667a4a636804b6c4ae821ac5d6556688bab1d
c10d6779b485c63c0ddacb91837c4ff3402e62141880
72b4186a39c65bde524c683c95d3c8b65e37104f551b
6a3602eda50b787182d703ac6a221428b4553e3b99c2
b251ef642e31256c329b21d1246a71456fce700d7f50
cfe5390a1c37bc133809f102c22914a1402c205c0512
b733afeea04411ca5ebb0bca9392b1ee23935eb19602
4732daa2a1f79358e6e74b73c965a9e74778dc692144
2b19328f6216a5e814ccc0639a863a437a614def5a61
f38852151011b04a37bbc78c1eba4d8d1b3a1622a0df
f74d25c731abb2a5fe5919f835bd3dd97330cbb7dba0
b74260c963402160c4017d92256a3713c9e77ea0f490
1accbd38715511784c9ec287dd85a769e081854b32ab
a9322a3840f6065133228c41851afcb40ea509cfbb86
145fb8853ce14c649691136b8660b0077f3b2f9da82d
483c1414c39a9777665899131a8336fb828480986df1
02628d10b54239cc20231457d4bbb7016f76029661f1
4ffd3532e2f8494e1613430730ab915683c3c8c4db2b
4373a3057a097e23333605398b15cc4d6ac3fbd0732f
21026bb0cd51fb738a740467114e7c66256b830022f2
8c028392cff8013d617c77a47bbda11c4a522f8f2b49
f2822cc06338605671fca4518df9b3c506532c9cca31
75330f8733ce11cb3fd8b95239ceebc9483cb68bff43
b622911fcf4a9c57c226caa38bf0b081535999f57301
6b14563ec4826dc281dbabc633868a1d903d59207fc6
62a293735085c01f40b5b56cbb795ecabfad709d611c
ac73eaca579768213c18c969c59be58fcef6bdd8a851
92907cd0773f81eaa24be07e0d620e9685acb0c6b0f5
4b47dffb510384241c4b733fe08dacb2852b2b74cc01
4e974a5e9db35d80d7b83ad31da1487a0170ba7fbc1c
551a6f1eecb572084180b256962748d5e3200b731ac7
c3928585a153b167c92a48cd91668c773707c054af16
aa7bfacaa161a620600e8d08cc97601a53391da0247e
5fca60cd1bb65ec0417177a9eb78cde5aa1dfae34e94
8417b3cc0b223803f5f40e8ae3a382848ff80c418582
4076423ae4c137bd30bd81f04095c20a01e0a49f664f
8f2b7f6bf6a990993cbc0596a514ccebc578c6418e82
5903ae11ac52831c6a48c67727409ed7274eea03eef3
2094271b02d4535563aa4924a2666871a4b690540c78
b06043bca31ca4e42a03650ecab74792017217d10615
d0acdee124e3222c90d79362207e4f7779e097501cf1
40b1a3431ee0cf27b23a50373d59976d82b5b1ce165f
4aa1361157afad564081c85777584dd6058a1a4663b5

```
                      3234d7264fbac6877351d1928c6780f77d4720933727
                      1e305370df9aeffb74d7c75de55c006e2b2a047a93f1
                      833da6f7c4226f8c05392ba90626e4ed81bc9dff573a
                      a243055f08a567e29577ce8dafa08297e6b04a779bed
                      852b95ec0ac14e04b1cb58eb656455bad9
   decapsulation_key = 0101010101010101010101010101010101010101010101
                      01010101010101010101
   decapsulation_key_pq = dbf77c8d79c80ad6b0763d42a3fe53f0f1dc03022
                         0c2e3fedc2aa903abfcad08330db4ba490ccee095
                         988d9355e816055cf986e280532d47cc19f2240cc
                         23419
   decapsulation_key_t = a20315485f73a3c17e18a3f155ac33e9a980896b2f
                        17dc7f96a9495d95840560
   ciphertext = 600ecf4026683898d0e339eeea9ebd437a4a802952bf32bfa32
                6b48eb74946d0cdd5437e70df4b6b7acbf79efe60ddcde985ac
                fd8c2d23775e1ecc54eb6ee03dcc9b4aac150172737831adfaf
                0e63a4782bad2a785b9c39bf5e34640ea3da447efc2a03e23a3
                37ad1f542c32c2eb46f7b88d0bfba87d8efe8cd4456e6f21bee
                bcf3dd502b53d537395750ce963d289eff74621545d4a5d9262
                bd14b3dddd4ef880e65cbe8f2f8aad826f57f727a60aaaeee8c
                69e89af6c539fd4f267c44bee8b5385a460a7c8e4a809959df8
                6c1136ee23e7544cfa7524c6c04ed9ec29aed307b5dfd0108f2
                9294aceeb517a098b8cdbad5911bc75e96258bbf38a20288c69
                11b2346f842c0943bf8e9c34a0a8e518e92c8761c6efe6b1d3e
                a8aed9b2c4feacfbf3559f3a5e46e4dfddf81936183d4d1f9c8
                c1616b14db2057435ad71655d743fad4987a19e821d0ac666ff
                3e46b7cc0e90b85e1966962279a48afe2e9bbce89c819a8ba52
                476af074a071495398bd497f4d4f34026025452975cfdaa3e7e
                183a962bda009108221ecb20d218c42e38774019d2dc3262127
                8b5e88f99b62a9e746d16c1691ccf3e7e9185c3c493e7617f45
                1f632c161fbe6d8ac3217f10ed4bfeee47e4960ec4a53e4852c
                a02415438484220 44a67567a83e09d8e74b9d11af17d53c4956
                5ca53deda7c4df076a3e1b6368b1931d81db93e87f75bea6924
                a321376fe73b5a5b07b80a98dc3ab8d14732540f1b4b7176e27
                4a905d453eac1caafe2bfe4e6c904556ca91b01b2302215ab3d
                fe6b49f46963df632a9e7cb8439cd5ee56a1f8e2cd3faae5d8f
                3462d0ff931f5038cfa70259d963163d6163ef22b0c32081bff
                2763e98da87817048d4ce755e5d2b1cfe7d6eeab0fdbe766c95
                f125537a04bcf99026f9bd5be3b26b9b7614f132f6747dd6d96
                009a85ae6cbb1a14b9231099b67b04d7849875b6492f3b6482f
                8bdac305f7ec29f28ef4739934c6a7a2800fbdbff6eb2237d6a
                085ddfab8519db1d2b1e63aa6cb9b3b044278947dc3bcd329aa
                427d13267f93a6cf2aee8a2ab74d4288fe0b676ea85586834ab
                57e863d4805703eb8bf6e71fbb11a386e7b64a0d661dbd05f5e
                2924f1419bc799a089d44dda9066c6c503f8c80be8daa99bd48
                338daeb4911acf19328103c96f40a77ffd827d52294ba21ad1d
                52fc27e8b12ad65887024f41e63fcfe654152676ac363f2377c
                5b0b437e075897e33dd8d57227fc5a536629efad998a2791031
```

```
                50e7d47e4b7d11a0d649d146c6560c48c9c0c56c811cfa6f3f6
                2cf717ae571597bc297deed887672d8a8cec2929c2b55b95f26
                bd5d10ef30c0c4a6295d5ca601538f5a20ac1064d2f4c2a078a
                f1b1629a0c203ad047125eb9dce0d1260eef19cd4ad8ec5d73a
                01ba23e266cc6dd266c5a81af58ccf1b5ce0440efdd1fe7bb42
                177679b5e5095ffa0d453bc17b8921008531c2d096a3a4a4856
                3370462a59fe1faff2a81603f2d09ca2e0beac44204a4e03aa8
                52745b1747bb6c424206ae093ecb91789704203948060efd681
                edaf7f1ab49d5f631f1122d2e0cb452a2ce5490497b32df2253
                72b80b86e5a710a64e8b4d92318414a179479b96827f3379de2
                47163949084
   shared_secret = d33a83edb4fb5a7508686ba4ddff001c17ba8890e9e3be06
                   7d50c959b512f9be

   seed = 0202020202020202020202020202020202020202020202020202020202020
          2020202
   randomness = 6666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666
                6
   encapsulation_key = 08118d8819772292c976ec971ee3039195800c823544
                       484595cc63450b9db9414330419208c509cb62626067
                       a8fd8259160105b6d8a4023b056f5ac2d6159fa5f245
                       f00c719539a4601466f6b45b2a68bdb0db7424d4cad4
                       75a8d68b0d6e086c3f012414e22900f01179e8c90a8b
                       a1d285cdcc7c7ab1c7064e2c15233acee183a1075c04
                       f092a5e3676b1ec06d15d348e7781346ec95806a5e00
                       f64d1e101bfb28bbc6829372f32bedcc0de9a70a02e5
                       08b760422505481709bef10697fbfa219b99a815f47e
                       4bacab0e789ca1e414db529deb043bd8521c2d456a06
                       2a65aeba2a40dc6b9ce02474a71fdf852f343b22d211
                       0519955b964382e74a3cf78586eaba353b98228b0268
                       f8480b02c4b4ee208198fbc472117c4be567858c097f
                       b0869a40588418973c58753da845e36c0adf39c53ea9
                       c8ae24c343bc87bcc3be69ea40d9490592ec99e9a853
                       f4f22b024a1b15962b049a62bc198706e310c8524c51
                       872718d76c6db25cd824a1b75a94a7d341ca40be1283
                       b2111b687be69d38b7297a90384b0c0269ac911cd803
                       84b326357262ac13680dca37ee18477ab23e16448805
                       676adbe1a5b7732e73c0abc3c5188e6c7ada3c1f1f12
                       4663e83ad5899674253e9bb15f39908ba4917dc11025
                       f7504425a305848661c38cb09a82026d20c9bd23949f
                       285519db298418718023c8d7e37a5bb1062951b43252
                       49aad59acc06b10161416ccc78db6c6c3f685ad3d9b4
                       916c622163017f9662da4234bab8b8b1e77290867d48
                       c28a2cb33c7d2c7874c2be936ca0d6ba907d6a823fa2
```

```
                        4a18c56cc124209ea488ce620c18d00ffc8b8f0c11cc
                        5850c30b3a0fb7faaf6e526f9b08972207a38f760bad
                        1824726017a30634fd239ebda59651b4c8162346bb36
                        52dec39f56626547829ffbb052a5a6930f2700fad33f
                        b1eca8bbc40fcfe778189398b5527a09a24a53a958e5
                        c25353951b78d85916457c1c5046e497ae0fa24810e8
                        2d360050e4fa1bf55b719ab8a080c23dcd80c0d4915d
                        8458652d476f50f3a5b80ba6ffa9a76bd9524dbb39df
                        7826cc507a9d31aa29b6207eaa52b3e224259c4931b1
                        ced9b97a42e6745752ac0603917a694d7ec95145094e
                        d089008af675fe51b2b79970abc282dcb632c1fc3dab
                        85ad14893d0ab63b9e21a368845e872bb1468aa25255
                        4f59f90c9675cd044b930e37a96a213a28277614443c
                        ca4317e4a2af9f4c7124fa76e1d48f38981d7df03d2b
                        f840610861b210300156c3f999aaac1b2983c45cf000
                        2c922037bb4055dd1c27df511ced577bb8046e003507
                        aa7b2c52194680b93e2eb40719539b8a93b8e83b9e20
                        5714927264cbf0653d4429f504816766bf97f1414162
                        2e91b20177d98b8db9351b39632be41a48f39ee050cc
                        1919143a2448d09c2fb15a680ebc07963b788480631e
                        ca37e19213dbb6c5e8dac3eee81b0292cbc681563d05
                        779b79b5d8ec37b331b3c021719cb95e69ec99a0f97b
                        723303278b9403fbaa7f71ba70d61d082c91a6aa2c8a
                        3543b5281e1605832c740bf67036f2373571f09482b2
                        7272c8ac2c69b01f715dda83377aa093a044541f6000
                        848ab1ea65cab1345135a4552be42b27c4b980065694
                        134a90d436f0e091b02a02aa99eac7339907afbbc158
                        a5127540423f23f6927eff66915d745f4d420459d505
                        7631d94214461c9be803e9d6080e108978f60af4795f
                        c34870e1c018198d85a4a116ee21df20fe81d9218ee2
                        2a9e81652b806a71aee14f84507485356e
   decapsulation_key = 0202020202020202020202020202020202020202020202
                       0202020202020202020202
   decapsulation_key_pq = 971619c09e6627cea855bbf7817dd36cdbf7d2de9
                          12d66aa2d94dd0da30c9ac1200fe81d6ea2b42928
                          de29420fb451103347536bb655a2bab5fbaba8a67
                          86fe9
   decapsulation_key_t = 96141896442e2dca19ab5f49cc2450f804fa3eb949
                         7f879679274166881596f0
   ciphertext = 413c55d5710bae6376761dada807daffd4dc45f9f70d825e0d4
                6176d4a342f58f20d61879215bbe4a7745888381753426 28a90
                5da0dbaa1346e8e913f4738defa0768445f1c625d296ab06cd5
                47b93e764a388e63815b588059796e9bf3fbead072727703b03
                6aa73223007ad1caaaea0c6cc38d385beb06fe8d372e9145c08
                e1bc3cb5ccb12f450ab0f6f9da5529629a3f1ff6312346b6d2f
                cb20461e7b3b245a97a03ef27f2e5442daf2a5ea317f454528e
                9749f06342aa7594ea9bda0cdcc7c0953c36372359ffd69f2ae
                dc1adabf8a3540e32ab36ebc1350aded1072afe3b78a6ec2f94
```

```
                3d560f4849d6bb1ee24679e8f70cc0f4cabe7d4cbc6e090353c
                e8414a93de9c84a32e197a2ac95e9fbc5d616f85fe199e80793
                f6dccac203d2f236e7bad1a4e7ff51b3f3326a9742826ac6a23
                ef5a945aaffb54faf50a8f0b8c09c55cf2bc812e30fb3e687ec
                a91b494785f121241a1ea8d0cea089216c5a96a467c06d4f0a1
                0c2a6bf551637f0fd5635dc1734e96eca5e7c545d66435b8b5d
                d88eff4c2cb3c73c49dfc9e56c293febef797a7d36d21ba3036
                1f7fec7b0e51793f6fdc2214f420b713a1598f4dda1a29f9124
                469407e5c5c5c908e39a78ea0fcfe4df3419692435a92e0f9a5
                846690706cdd23b1825be8d0a843756fd97b4f277cf0714a0d9
                da3ccf1a31a07178399b803c7b4837980bc0172f58716b3baee
                5e86441d32bf31c7ed6e9c6d55eb1ed528a4a306dec7f37b3a5
                75086385a9f4641ef28da16d35578c743c8eccb0581b2fd308a
                3c9fa15c8319954c8f4259ab09f178508720ebb8a0d893a8c45
                ec23b2c1c2e43db439ff71fea6a9fdcd8a9d3c6e0f8b9e9e71d
                dc2aa52fc5cbf22ed67217d847e4c84b72e7f201aca56c7d1d5
                e51e0c03cb596a01d20203b38e0e7d3086c83a4a19307541349
                04487c43fb96deb449aa832e63a82d132660cb7976d9d507426
                41c28c8e2e1bb00a2c65e9f8b9591501ad60568af112a5cbab1
                34bb472fecbdf24badbc6562201e022c23fbc6354292ab743a8
                63a139dd4d67b1bdb553b3c57a5c7f5b98cf145ac142e1ad6ad
                5ea3954fa3c2b8ebfb6cd05b915dd1d87262d7ab1f1b47cc0a3
                babc15a7a1415976644c54e29338d79afa9d12a669d3c67bf70
                e604157815f041556a5cc1c8429880a5449d033bb3f1f2b879f
                0e689fc2a3e2972f75f6f25b95bead0460f35ef71d0bdba380e
                fbabed6365c6e7fcf2e22361b572029f0c90f2f74c8e40c7941
                ed8b6eef5a722bf2e5141cf43ed2a69b87901d546a85765fc49
                4531e61f3d723107659b4ce1f294c352fc45c28a82cb3c242e5
                d6b9cf43d071bd55b8bc0d47b225463a5075639569cb073ffc4
                e07417dbc5a30a8e30545264d64d98d13336fdb6bdf8c71041e
                995cd433a77a9d4ee25e20f757cf76dd702f7c8f22a2677f03d
                cba47ea1996b9d783e44737ec501a8c75acb6d7606a2b6eb1e0
                69576f3a87b32e587923fb79171c77083bb629efda6b9ddc1d5
                66d72a53161c165d0ccea7674e5b1af42b040bbbc5e8bc84bd3
                3d1d3ce03ffac9a747f4c1993fddb2ec93a4116a86f022a77c3
                c17191559a4c2a1aa57e79b8d1977da2c959172f478e341e270
                28d69fffb7b
   shared_secret = d17a7ca859a18cfbb5fc7bcba2ec54aa0e9ac44959023199
                   fff5b60db9f24401

   seed = 0303030303030303030303030303030303030303030303030303030
          3030303
   randomness = 6767676767676767676767676767676767676767676767676
                7676767676767676767676767676767676767676767676767
                6767676767676767676767676767676767676767676767676
                7676767676767676767676767676767676767676767676767
                6767676767676767676767676767676767676767676767676
                7
```

```
   encapsulation_key = 04ccc68ebb7b60c6148fa94574ebaedb9c5ce5eb1ad6
                       9cc5a4d7bbf9a410295540bba271ae8a178bd025ea28
                       887ca8808aba8fac7a44260c6e39b883110155d0dcb8
                       2ae7609bc803a8f927dcc2c2033cb07ba90fc8b06818
                       8a7214e713579537e69801ce304251eabc8b34b03ad7
                       1246cc22f7671adf572cd6a2730976953535c59d7c93
                       baa5788854ad52f48e9cdc8accf4a3441392f006378a
                       450289053c2ea689a80699de7acc6bec4c2b182e3194
                       acc9fb1ce3e1b389c5879ce66bc692a3b15343d6e557
                       ff93127ae69007e6913d51ce703898c5449ed3602593
                       84819529c7b54b9f5b6c9755d0a627554772846127c8
                       a580a5b6a9ea6695449be144306d64cc810212727882
                       7dc25da96b6f4823ce5ed25a2b199f3902cd8bb82058
                       d4694b40ce0ce1cac1ea8a047a1ced942d78ac2923c9
                       ced1d563fcc24895b1683615b134856ae3f36e4b382b
                       b160171ed400902499c6a0b1b8701d89093d6d72a992
                       c9ad296308a2d44d26816b1c942a3bc479979516a0dc
                       bf16bbca1140554be69885a477d078ac0a267e829411
                       1cbb42bac3cc733269c7f84bf315258cf8cd04774f9c
                       a932c7416785796ecd781e17b6ac32277d6d14190681
                       1430da866478499a8c94c521aa4d4663af067fcd2c82
                       3252c1dfba800c7b1681955de39112c2fc5f4a140204
                       69bc22278a84494806d43528f8ad8efc88643038d9d7
                       1c79a50710dbacff686396c34f9800b0671b0da3c2ad
                       4dbb3751b3b3749b63e132a336f19ae8f37a79f6c713
                       c48b724c80465b28e578658bc8329f0c1d75d0ab1d63
                       2027a3cc8d749216f50440109ad7637f3ab1661ee763
                       7eb06e70d4c15db81a2ea25ecae4524476106210362a
                       7b35c013120b51ad9b2c88b452457b75a98fa3ccdcb1
                       83aebb1684b72c3fb5434c277907680e8ceca5d2fb88
                       dcb43b050a5557b19d159a6050a6115c1c49232cb515
                       0463e165acd4629ca4927e3ce46ddd1a733dd23f77b4
                       4dfb7b46ebe4291594015a4ab5ff00b643321856b3b0
                       62ac28f2c4cf7b30716b6c9a53271139685b3d2bc20c
                       f5c766265a6666652393af58ac25efcb502a30b9f6bc
                       2524cc615a911b1de63bf1710f9f829c91a573a960a4
                       4d43138a65c42d41000c601c7ad1537633433edb5023
                       387aad5007a09827a55b6a7e7a2911307e0f226e9e52
                       ae3ba4c0f14a1efe9571352278c5a4a08cbba7403c35
                       ec69cc2a2b364ed145b11a4e8594087236a4ba7a2d00
                       3aa89fb2c97580c3ce115727ea0e99ea81cc8354164b
                       0602e53cb33638dad5a39632b70f4706eb8bb6d598c6
                       717627fe3c02420583cbdac9460a9d55588ffafba8cf
                       748c16283b0e96b8f95100caa7a8d12029a433ab4efb
                       b9b2067a0c615d5358aceea04b4ca4bf584a452fe276
                       8cb5bab0fb52aec375c3337fae44b305f1389f123103
                       669c7901a1821c4715b5cac1c89389cc9f4df192cca7
                       89ed236f7b378fb2915106ea3cc1b90ce9d6c07b36c4
```

```
                        f09b5654e3a116c60dda685b9ef6893b1b42348a3ac8
                        7284eed683fb346d25a562b90a778e6b546e40b4fd7c
                        1d3c01983f851474c3832297019a808ef64957d79025
                        78981d9231b382169d533a2202e95d18f152e8fc25b6
                        15bb8a65482a2167df6ab2811c73bf8fefbec077f1e6
                        68494d422443a083b9619254ec3e6bc6f3020478cd35
                        c1616ff29a1960108be12b65f0a299f3e1a5efe7664d
                        dbe33852e4805aaf60435efc123144540391b81683b5
                        712fefe40126d070b4f9fc5e409da896a4
   decapsulation_key = 030303030303030303030303030303030303030303030303
                        03030303030303030303
   decapsulation_key_pq = 49b46321ef5a24c1c036750879c0ad29dd08607d4
                           89bd7eaa5869492759d994d875e0beaac3cf90df1
                           b3f1e0dd70357a5bafaec8a36fc2d9b72edf3f57f
                           9db20
   decapsulation_key_t = d20034c38088ae9e3338d75e1954dd00001bda6103
                          6eabac6a3ee56339d37ce9
   ciphertext = f40d556d507802ebe7be0e65ab82b0aa9ff26c825d24f98148f
                75d7e910d6c7f5852e7023a4e246be81b807fea96928da6a8c4
                d23b8326ea90aa7f1f0673a57277bdd08960f7f886777f1725b
                882e1996632584fce4356f7345abd8f480514275fbbd96ec6d3
                202de46e18e7a827d4dc62c1681c36018861c33cb2f4e13ba5d
                a65558441caa6ecf82a5e74842268f4ef5036deb2f0f6f5cb42
                2dc2b723a7f2f69830a52326621ee034c8a9e80f39070456bfd
                de653314040b4f41590723b66a2d7e41153932521e8e51108d2
                d98841b2983baa43b0dd6a46783be063850b22a2dd05c1f9f57
                8360dc3dfef4d79e8c20d2d0c45687ae19395355e7cdcfa039e
                3c36b6df4ea11b4122918fd6ec63ec672ace58a8ed9dfc61e7d
                3b5829d574833e0e61fa08419cbda05a85b3c4b9957a0968d58
                25d0d052013e75f138c8d74929a631a0ba2ec9555e2767f17e6
                e22890a5cb00f63f09e00b8decccf7d7d0e369c4396cb429e53
                d8cd4636ea630d6fc55143e6146a969ed0839ab05dd079da3f9
                46b3deaad2774360529f2aa7e6c400b66a5c449dd8362fae1a1
                bbf110229810e0d4725cfa2dfdc046d4c18637e1de3ec2b5205
                5c237238de0167eb0844c24a8fd91ac9f66f86efc945c0a5067
                2926efab53bd0725ae9ff36e9fcbecd58212cbe7e0f248b9ab9
                0b2f56497f196198043fa10de909b05bf3dd1d20630f9707095
                f4f80d044418e67ccd79e8f28db7acb1083a2bc63233a4f4798
                f13f21e81da6ee03c614cb367aff05410960fd366df06691b37
                4247de70fcf916e653b2bf01b49cf116324e8104da61a621b56
                6a62c97c6c058208e4825727cbb6c2ebaa0e888659094aa0370
                9659e272b4209c18366196110d71120b203fc71dd5d3c17be45
                80e5ade64a3fdeea5b85ad33fcebf30b857dc7cfe3ba52ea826
                9cadd7dda308460201e0119f8918de8980f04b318f39487e65e
                f0e0b83c2396d2fd87f4d54dd00b405063f072659d6b11513f4
                48b20deda3d874987c252b7d16d94c4f811c97134e5e00bff83
                00e718e17de3735bb4bc052100a3823f8db4be2d7554003481c
                e6d899d74c1ad9944c01d933305851458933b3f780ad6c1db48
```

```
                9da507621e39be174c71f73ec9c1ef644578bb1566136f17e91
                b475fdbf354cf4f5a6ee300d3938f5b4a7b9bcb90188a3d9c8f
                ab1326df69f5c3753a8ff9c5a7bbc4e2255954dfb6a2ce81381
                eaf9d224005e050eb5f53d05f0a41bcf4f3c0e8771e84eaa46c
                e27b0438d4ce3ebf9eb25b5351643a26f607c41b6494ac77e4c
                4a2fafac8e3cd872f31816501efd66c41795fa0d01ac0290253
                cf6c9d0dd8d5865684c1a02748a824417827ee374404a59ba87
                c3ec3caadf08b0f920667fae9ad18560edc3f8571986ca0bf1e
                f114d394c08ec5ff221e9f9ce7b6508eb6c38d6041fbe7319bd
                8874f35bace85c0bcc08cdcc642ae7fc264b9be08a26e5ec6a3
                618a078a128d0b8daf46e404eee4123b379a81680c8336036d9
                a44c12bcc23ed7b1b96442108843e5fcee042394b456984b83e
                a7859f7a0fb6475d53b4fd55236ecf4f33183c1d719ee10683a
                6b689b463a823665a40b63735647c2930f3c4b1d8787d4199bf
                c2db8499e61
   shared_secret = b3db69cc0385b1ba716128b70bd4b93288f945f418cef51d
                   122ca7a4de564a81

   seed = 0404040404040404040404040404040404040404040404040404040
          4040404
   randomness = 6868686868686868686868686868686868686868686868686
                8686868686868686868686868686868686868686868686868
                6868686868686868686868686868686868686868686868686
                8686868686868686868686868686868686868686868686868
                6868686868686868686868686868686868686868686868686
                8
   encapsulation_key = 6afa82ec0b8e8449591cb9a11be36dc43146c18a6ad3
                       f175897933d25944c3c643f50332f1cc4f6a9707a387
                       b5c40661ec41b36d2bbc4507758387672fb4a1c1196e
                       aa81b01be2864cc958a0642496f264b4042ec5f7b25a
                       5220a8a9c9633081aef104ef9abd4da0af068a84e7b0
                       3f21e6b60212a02dc48ba7865877084a1b025443e38d
                       60bb6fae8ba88ea4538d088bea758f6f9a5c26a9c446
                       99ad43080d3fdcc2d910b16b297bb86436e3d5b79dc0
                       1230124867c1be64a9cab7aab9fdb47eadd15d00ed84
                       ac9a37406a3665d7cbdd106d1e6a29a81c94e3c841fe
                       9cb583004aa471ad2eb477623401e6959a04439bae06
                       a07058cf2ed94bce1839e636a8c0b22f782483ce798e
                       609bcd784605eadc0a06c7699b1b9ece550484124095
                       a13371028101c95721c2c71b098b15f3998785b36192
                       4f89dba9f292b9b18cbe232cb76e41bb5b35cad97696
                       2fca2957eb8e06356c250525e8825dce66478fa587ab
                       6b429bb287aaf21a58c900de0946ebc284873450c7e7
                       a0e08c856dca2191195f73b3aecce1b1c1c29cb24a6c
                       2fc3c14ca1495182645cf8486cb877d067440f118b80
                       713784474bd0214f23fc09e2c8b5df357b3733c13545
                       c9490378291646fbdb8403818f7d571a40ba7f5cea48
                       0fa00ba15373c60255e54384e96c455da13fd7dbcbc1
```

```
                        e7a5e9d655b0145976e190780b55c9c86ca6c988d123
                        0aabc8558ceca8d5cbb844ca8d95b30b64c024405226
                        61c9b07c866e497b5a7daa2398a5a888a4244d902101
                        05460fab31c6db3fd57941b869c24218b2ebd7ae6788
                        5e1fd691a3dc4388b872f4cab5fcd94067ea953d73ac
                        f1f4c752776357974b0ad7872ad603c30a174f963983
                        739e5fa5304d1705c6791e9c90342683a3b176a2897a
                        b9142190b3900d089c77ece41316b40611fc6bf7c81e
                        b7b589d65524f9c6888fd7c53ba810b0c70766430638
                        595dc3134ef5da09c668a804ea1e2f1469edba0d457a
                        cd8281828d02a915bcbc05949d2edc5c1c5856fa798e
                        5cd3587472903c6cc2bb43b03229352587cde988ab60
                        049b6f872a9aa82f25b5346fc56fe8686423b27e0f36
                        8a43d36a21602b4056022d25217df44a1fa330122152
                        cd2a581ca05d3801bf9f0a31bf79b8a7394fb8c9bc16
                        52cfea9c386ca7c703b5754c8243f7b0a36bc290e073
                        3a17a94431d7b05e0b4298a8b287fb1ad3b32a57693a
                        1e7867b0f3c483c0abdd2c05c81c26a60320d91207f2
                        04c2e8393a78e7572c8c296260351eb62940c394943c
                        6a622a8710aa09a076b513dbbfddfc3105379da08b97
                        a6fc68f2105088cb35f9683144ba24673513f0b6aaca
                        32c0e77173d7387294a9b96a08a014ac88afaca949c2
                        c3760b461dfc1ba5c01a956cac46a01dc7d9a992e1aa
                        704aa15af525911857d46682b137a3719aaa71f7a8ba
                        88afd6d43b127805f6c2cb55f88d6c590775577373ac
                        87356a56b89341d0e8657737249bca66b0b4194a5c13
                        dce045039164fe1530e38981f08c66ad2bb0531c3631
                        a86f6cfa71571b777b2461601bc7a146c358955a5b44
                        130d26b5c35322138133c083aba300a5def2c4f0d94d
                        4267a2ad23420b768c77d8a1f0428536667d2df42127
                        012291511a8c72738b82f0cff83b9315330886d61118
                        0d2383cf551afec4aa7515eb138a398eb44c0499863a
                        8fd0da2530b7deefd5f1183646010555333a6cd0e6ad
                        0d6bf919678252c49358a35322a458530b7c2b60f3b1
                        70d50a5892e06a9f82ee0e34d56c99312b
   decapsulation_key = 040404040404040404040404040404040404040404
                        0404040404040404040
   decapsulation_key_pq = 79f1b2ce3b601ebf5ba31006e5a8e4c86cd58148c
                           75a89173711aead9accf09f158d0facb085bf624b
                           4de5a388fab8e60419b04710475367a0fa9c1397c
                           96d61
   decapsulation_key_t = 432eab0f3a8eeb77c6b0000b9292c6e163914078c9
                          4a161829fcfb9bb3447393
   ciphertext = cfe31862853164950123baa75549418c7a406cfb60003b825eb
                292f1ba1f25c3b5b044dce0b8b16cb254d69658d516cd3445e3
                f18bcde32c4f46b4ac25dca4c4573647ab7cefd7fcbb7c192d9
                97194654aeac0f593eddc4464e7e125672fc7265f1664b32199
                cad45095359a4dd80e9637f0140504a7b1303fa69d121d2d214
```

```
                d5ea44e0046a120fef7d573016d8edf0c20749f05edccca4a30
                565df6e79015f04b03623d3aa25cdbaff330633470c02896899
                88c27fe49acc957d3be72c4bce05f1c80f3c2ad5b4e8a2714c1
                d1ea518f431f97f6d68eafb06ad7226a29a2b3a9e5403cdd923
                400a4303054876986f834848a4902659b288d5e3ef26a9ecb3f
                1be3630037d147301498bfe198b8116f244a12547ffe6a5006f
                748c0485fd72232e0c55df090011946c8b493f8aaf92de07396
                e901fb4dd8a4f291645267e7ec0335eaedeca28ab4c36328c73
                203dbca87e40dcf007bf8687dd4a776151e9d234f52442a33c7
                566b007f6537837cf752602624030615d0cb88238b91f578e07
                28b32734363944bbfce5884dc3c777e0b3f1ee4029298895e6b
                82f6f2307dfc267e27ca8d7d9b49b90786b7f39d906ca7b6527
                d5e31316fce0214418f95ab9504c98ba9e868754cb813014cbb
                196eac152861af719c7632710754cd2c72544c25b66d1d016f9
                7a409ecd11577a358647e1726da16d0a0e2591eb3b7cac7fe47
                fbeef10c6eeb9289aa4154d42ea75b864e0a1215ae35dd0db3f
                bbef39ad399c3d04d0d4ad9f2ce442bc07dabd366307eefcb2a
                b483dbe80b3eb4fe966131a587ffb2e3664d31e2c520722dc1a
                1f5d27ed0e937c4c89963576cdca001361f11bd39e2e2b36794
                3305fcddcbce6460a8bafeff8394beba9bb893f1a7abfd2e80b
                f10f0546e72a4051883e1f7edfe12ee1505d9503a83ddb2b998
                cb2475b88d280f1df688f472968f8c718f1f9fbd39fb3073312
                bc54c755210d0ef49f9f2bcf06a1099132a1e08d84b68543848
                e1538edd881620560e54d8d6f9a71ca2fd44f8fab9d094f1dce
                52f40c5aafe1f73e98a2a395f48d5da98fa5c95e4afaf84e7a1
                38807f71eb64fcb3b5169e8bedae1dffd725ad6fba9fd50f39d
                b9432cd5f379b680c09c5313ea73517f017ddcca33a405c0ca2
                93d8c34714aec241b9a634ec65c8c0b56e59df8e668e74d2494
                bca14d8102dc0592dbf93c0ad5f9dc89ac24a7e981feca0461d
                3fce1eec98a4afbb0b7e6c46aec385c9c0fbc203264aa6aa71c
                67fff159ccbac01cdd85c28835a98e9b7d0cd4c4330a0a5334b
                5838c072df4bd7297251cbf85dd8306e1a8ec893f4b9558133e
                20e0c9598f054e2b0b77d4494c393c5dd0e83a6520243edc562
                00f1cd34b8f69d53e4a823a46852e61672ba69447ee49522978
                c64616ea42a0b0c6cc953c748a550dbabd74010cdb8fd19c886
                2473f826267c8cf41cfc36100665ebd766390d83c1b2f795cb6
                d3c38dcb8e98c6ec0cd5111108a079d57f9b16960d94a4f238a
                6d7a25b6253b0ae0088ce414406fa7d02004692681e4d957786
                be9fb7f064113526389dab6ff0a2dd6dde42c5e579bf996d6ea
                33dc52c8b15c92b6172be0781e33960066650088274ae577e64
                65e8fcfcae7
   shared_secret = 794e2f99d9a890c338c24a018035f8f51db576faf0cde96c
                   f777a81bdccce864
```

```
   seed = 0505050505050505050505050505050505050505050505050505050
          5050505
   randomness = 6969696969696969696969696969696969696969696969696
                9696969696969696969696969696969696969696969696969
                6969696969696969696969696969696969696969696969696
                9696969696969696969696969696969696969696969696969
                6969696969696969696969696969696969696969696969696
                9
   encapsulation_key = 33393446a76c2c01b44da5696d8452b29ab7b9178776
                       5366bc1a15b149792427844ff68753f957187c102d09
                       40c498b67332a7f9cbb82fd3bec9914e05a955035362
                       dc7462071c19e225ac96c12fa34a2e86e0a84a0c633e
                       044b3d93969705833a53a4257b7f4c1515ceaa8af9eb
                       7f53ca7cb402a4aba11c9d3206f8209c436bc3ea0487
                       c456a79e240fc4f5829e4977817aac9de9a0cf6cc281
                       31be92c2a6ec672bca1a8b3758092f8b87a11565c031
                       2e82939f8fd18024a71bb98a885c6ab99299cd43a620
                       8d2198a45bcdbec590157375c16a456327bbd44011b6
                       35cd1f678277347aa5a765b7208acaa4316ea523f59a
                       0671594e56121654f3581e882072396932da2e2ea02b
                       f5489e546c452b7c6f60e8a4c6112f6ccc7e3a7a4474
                       8aa1308807a08c15d78a2e19a2750a916b8c46844b25
                       7c2663a8895b3df8c40960e6b912623c8a92c9fb435d
                       20e6cda9fb456e55c1dd90a5f64a5ac2c61250461757
                       51aa742971f1728328c353f4a7a08ff16b8f978ae417
                       24494c436471505e2c17ba958ade7b2afbf9cc266551
                       8949755fd5bb8b15ac9b80b78fa615a918c4a99549c3
                       7c6ad0017c51c3963e3408b11848ddd4afe96b67cd66
                       c76e817d4c150de52a720505b9a4b09008243c0fb05e
                       f004b9c2c223f9230dc57b1dd3d1873457842b47c59b
                       9a6b39d7b61787b42a500c9f57114ec737bf7c45303b
                       8a3fa78b3c649cfbd166c60c37dea89e2df71ce4c605
                       fe45abcaf3a604f548ee5030fdf49ad4129b94516a22
                       a8b728112bfd209e5a5b565e20a8dce97748a7906379
                       0bec93bc89103c32419bbadc1ffc679e48139a0c8856
                       3f170d165729e3d710365c404dfc87d7c31efd24785a
                       9265e55c4a624315db4005019818a1e7c0367a70fbd1
                       6098e27a640b0f3dd9515d82be0637506ff171c6a31e
                       df453b40a6162feb7c3543506bc1105ce196e46097db
                       749b485808dcc3b4221470ac21880bc23c7ef4b315f4
                       0df40802f7324957b450032c3104f871250590a4c9a2
                       9687c70e02b46350781abc7c2b256c54bbc96eb20b89
                       1877c3a673f67c18197a0e3d657196d5673efb19ebf9
                       b3e49691612834cb662d2828938b1ac1a45881b9e51c
                       786c1a321814a8c396421b7f313cc2e4447e6e87971e
                       1660d94aad5f13b26bf49fa499822b1959f48aa88dfa
                       5101f463d5bbc8ca21b9d0857fd2e42d5c1c7a919276
                       5a3013eef54ca9e43fa99abfd8053e9059650b964d6a
```

```
                        ea8c26c13adc0a6d91208f2dea0da4d57a3a8a6be915
                        6a4065058cf965da10586b0945c30965bf8a436aaa11
                        5ab170071c3080f5c723c10d05963a162622438682fe
                        e1b619c2b10c207ad7d38ab1ea7eda0924d9ab6b4433
                        86af7b07fe26b8fc6911789666bc14619a381eba7966
                        e0b4ab0e528083806f46456f97e59276d5a6119b766b
                        1847d3a1ad3c4022cd0616bbc348d4e072f7d6827261
                        7b03bc9b25f569d0b11dab8c5a7ee11ee6c761ee6846
                        25322c6cdc815ee1c0acd29a8e1c826cf89f25944593
                        336643a46483dcaca9e1bae9a196f692ac0532cd9111
                        3d5d974963a524bf708c44e198dd212dfcf69213a42e
                        32e6b7c860148ed38c51002b83b0c4b979b52a753bf2
                        c3381c027623b8a8251e60f55524b56b959a14d84637
                        086a15567717dbda7aff9fd61d09589ac8c0044538ba
                        fea1200548046b8fe3681cfcb43a8a1b5df785f3b0cc
                        713c0bbbffd9fd691df9acd2258c9671a14b4cee573e
                        711cf6d8eb9ee01f9563dea7438d484b5d
   decapsulation_key = 0505050505050505050505050505050505050505050505
                        0505050505050505050505
   decapsulation_key_pq = 749fe3a6fc429b2369d9e8191f72d4fd3b292f2f1
                           22312bfaf4b6a90f1600c4670ebea7aec851d89f0
                           095c61a2caffb37f1ba7f21dd514b0e20006969d4
                           85ca9
   decapsulation_key_t = 730def4e090b60c056e1a9b653f479af7398bea957
                          71054ab4f455c9a86d7e49
   ciphertext = 6dc476cbc91fa3895cfd69bda5799b95b7c0dc87e5c78dec9b3
                67df58abf3e7852afb7b31caff856e5e4136a23a24f303c6100
                d9a0a6673164f6f44ea472f4614c2b42496d0049a27e02f1aa4
                5ba04442a74b5e0035df3d8877266a4241e650a86ccdfb0c6ce
                f22c62f376543bd5749353f808308eb74ed031e73c9f42ebdc8
                a484b30769a17906e39fe8fa65c0f88fcc3436c0bfe26a4995d
                82a41c6a99140a36d166cba6ad2dd065ac19cebadfd455c9fd5
                d15ab2facaf9f5c79bcd12d31ef88842403ebfef226f9a1de78
                d18d2a0a57a7808e5c4d9c7c510bd1813db60a2e0121e72c52e
                df77084222dbcd94a10cd4dc3b09080e8e5a8971761cd46ded6
                5c78ac4d896d818a400ed832830570d492665dec3f8c11168ee
                e66f33d0c13ce3062252f107a3777d1d91234f58598184ff827
                f6b2e73638fce0e4e51ef704e1d3f8dd5312191e36db31d82b2
                b76869d7eb03474ff616008158f3bf966a236cb3e8c52de4d01
                0cc712abc23dff6f5ce00631fd3dbaceba030c2ec18fd0c39c9
                c60134a4dfca521dcd71cda1179d8ef08f06a42686c360c9272
                f15b4258e78514c8814ad70a1092d26557a45764041b8324bbc
                d69b5d2868a6fd96c871cf83413113c898e4bb983187fa4c1cb
                b73cd41d3d4f4db185047afdd241f1b7e7007c00b03aa8ab836
                cedad6127938f87861108047298d3d945b343c62e2fe852a035
                4ff31dadc1ed08a4ddab41d91c0262283b11fcbb1ddb4e9fddd
                7cc338e925cedfadf4e306f84863fd45a70f57df0384e123422
                0103b0f693144a5ecc9d99ab1d6f725740d1bb09c3a4b4ea614
```

```
                ac01bfb1288bbf14dcd572ecbb6c822fe541b04a0d6498b5a14
                727c2d543c9647277bd67822a5fabda4a98f23ef50ad12b3213
                77fd4ee24b234b0f296049906aced9d08671de994956a217939
                4d37b585a31e405325ef880a108ec492c1c87da90adba72d8be
                4643ccf29431cae053f9cf5271f7e1c7a4de093ceb053351873
                d657737ebbef086640d417c6a05ae7fa9e30b11292135952904
                27032f26ebcd1546b9c9c1bcf01ff3d18fb1ebdbe0fee540f4b
                5318ba65877f457736d30c750e42e0e773aaa6e526bc6143ef6
                31f6b3f8811a026374dc28e06c92acd09e1f3f97c12e512b778
                038563b67de0d6b34a48157f1b936abb8b9f3da3adb88b5f36d
                0dae48627cdc1a403810c816e32e0d1112594a4f372e9abe4e6
                721ff83f488421022189b82e1f7f27a33e4d11969522e91d19f
                be1a3b9eb6eb3dbdc2b199db9e86e56bf695d0e6e79457226b2
                b3cefdd2ee3775dae268020392f0336c6fcb3928bdfdeac7124
                6343c08f2be397daa1fb9c252653307d0f7bc24111ba8df6ab2
                9923b4e7f3471be2923f46dccabb2063427f3d4e53baf6a9ecb
                88c12d9c233ff14f63ccfd76a8f046cc2d96733e72d56c835db
                c9a1aa2a5bdee915ae7eb3e5dbbc8ba24df6e634bffb4364a81
                039b06a2c5cb31c9cd8985e7fe2985c3e0a8f1d52feb2bfc354
                9c3817989cc1746fcfe8938888e12274480491e5606800961dc
                7aea82d793c00281add579d5b6724edf7a5baae285fbc7aebfd
                9c9304f962b145573b14191fae24fe3a912920593fbb7cc1418
                6b3374849b7
   shared_secret = 6f1c317d16608f309e6b59a48be62722081f4e2de9e2742a
                   6d0e94679ba856f7

   seed = 0606060606060606060606060606060606060606060606060606060
          6060606
   randomness = 6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6
                a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a
                6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6
                a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a
                6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6
                a
   encapsulation_key = c3f9a6305222862c2c89ec0dbd805c547b2120405ba8
                       e994947b1d74eacc58277260ba837de29a0a2b84a7fc
                       80589334fb2626c9f61c01c88d60b20b0728110f0840
                       fc01a6187a506ab23d2b459fe0853c44f86a69953328
                       4577f7913b69898361bb67d3711680c6c25f2524c560
                       22227477f28a194e90b4702901b0046ba798cd1b8431
                       92f3bc841c8f9748a1ab34b5336b12c58585fcd010bf
                       d6c48e775e761525b260c7f6e646e8f17690aab51bab
                       30c9763fc53b8547d0b56b0c82c458c61d84587d9897
                       85600b8e987a36423d388ca11d61765a01a4a79ca20a
                       925908494eae0a3b6db1b08cbbb7a4ab5edcd96bd767
                       25e928055b0c2883ebce0a59bc9ec282cf300ba6c538
                       0d1b70f13b2dc6f616c76087a73a70daab7a6f97171c
                       a5997bf40e87b95f33a53347ba6c7ba89bcec9041701
```

```
                      226fda1243f4b1fa047740c7b753d630fe386f09e2a2
                      f96559ae979ed9fa5a78d1310ef311f97cc3b6a738be
                      e45b75e3a0cc714c81f72187b105a2120b9beaaac116
                      bf9835c504713f2218b526f13d8a8c02c95aa0f2927c
                      27e996e4564578e056227b07bbda8af0cc5d99f55eab
                      9868b8eb4d1b14065843b229ea3e2a0a748d89c4c304
                      198cd44cf77180bb8664f9aa1a9511527233cdb68269
                      76d34276f62257ec382172bf97b310bdd34056ea61f2
                      d74ce1cc9544b02263cc3d3133a308911556345a17c3
                      2acb470444f5536fd21f81cc3c968ab7e4db9cea564c
                      55d3a601066375f6417691c0ee3b39228860f1bc0069
                      3293c4bca327176da52b7282495bafc2932d1154c036
                      72f4db49bd40967ca41fb8f8696382a5208c5547640e
                      5193459b3507f4817ae3707930508969a18b1d168e67
                      b5939532160b50a538ec9074e733dfaa4af09755f831
                      720cec8519f3bd74809539347b8786868fb2ab9ab742
                      fe020c87930d37c45aa9b836c986ba01804a5de26974
                      ac647d8b921484b748d9999447875fe2746ad1112fc5
                      7ea3999f5899374ce2536c58310033ccdabc75d63a64
                      1a5651bd08079a41c1e59894cb3a1c8bac7614e96058
                      1a1d191a3a386209b6e82efc92b655c51d91e11e8d39
                      190863909a97cc6017af2c35500b860a21c9c48d4883
                      4eb561f58c683372968fd89be52a26995317855b3123
                      acc2071683ca669d78c3cce5bb9c9f9429a643bbb140
                      1d1d665dbf45ace6524cba3b0d33582105dc7c38165f
                      f0959d325914f437a4008ca751878bb8287eeaf09202
                      1b1b3647bb4a9b562a7aae80625739f66b636c309a09
                      376ac4cec6d76ce4629aef46ae488b4c696106952759
                      4e0c22ec55226f47085bec5e0343cbfb421ffc838b56
                      e9553e411ce39c811a1b4a53b051b404af3b58bf6513
                      76360c040a607f946c6357020ba1fa99daf19ad3f020
                      431a98b1647040038383719ff9fc7d4cc75d6bcb6d4f
                      00c834874b01b9a85e0c0f5c632734a3264d156c973c
                      14cae920bf0917cccc924ba90fef187f9783119a7a26
                      8621c7f29bbb28da1cceab369609c64efc5e91a79451
                      bc8100eabc85541d1f2435b96b532fa14c1cb76b9990
                      8c418118e2472c66511ab558aa06f03fd8fc15f10a20
                      99dc4df1360d15910d2a7747d8abab40fa3d77b7470d
                      8477cd63024aa40268f55139d37548223ed5823f1368
                      05752c0b5f7f23edfd90a89dd1f90ee344df04636cb9
                      7be2406e5515641b4c5ad186a0789e8ba48ab830d4f5
                      70cfd158fdd63d38de1e9252baeca9a76c4afc776826
                      6428caae913d203f4709ef6dd7e67544a9
   decapsulation_key = 0606060606060606060606060606060606060606060606
                       06060606060606060606
   decapsulation_key_pq = f7d6c6a46a9c534d6ee0532938a99f0c450da4935
                          e2953c4daea5d5b0a59ea69c700a40817fdf445dd
                          5b73ed69a557afa27839191b8e71214ef9ef97e9d
```

```
                          9bb99
   decapsulation_key_t = 0a925a53f7ceaaa373f3f8ecf9c2d9eaeb351eaae4
                         dddecbd7eb180b5432306e
   ciphertext = 56a06e6443b53c24f647cb6798257899ea1c49cbfd4c4e3e54d
                d73a1139dc4df519067a5934733a34538f941cd9a2d9de37162
                3247f1bbcb728d8cfd59b59d6995a2430ab14490b336ac502cd
                21dea47dc7c89fa026310ec05fbbe50179b45e4b68c507fd90f
                ab06e36fb1c9b21c06115fe42beba15083385764cde8c527c36
                69507bcaded45f70a8cca789ad71e9087948e4f1d682c4a77ad
                306c25b1e6364f43fb51c0c5d72f455da72f46041f8fcb143f6
                7c7517b425e24cd803032645cfeba77e0d8d2d0cfb57768b8fa
                3238c10ebb99471710973bf9d22fea51471354e53f153dfbac6
                95a6f8ccb10524a0453e804bb013b450f38007fe21ce898c052
                a132ea74c9e69512ca4c18c32ae37884df520d12721b95acb51
                5067f3516ced73c930786d6924cc7dcc08b50a3abef4e0df82a
                a0b9c7bc199cb2dcbc7cbaa38ffbeea60e41ae20e8400730132
                f3627e1f62fc784f222213c2c479c4ed1f2159f724eddff87e6
                a4b5b3445e189590de4bb62bf66e930550144b44e23d6c045d7
                79ace9f94c0a688f729a0b94821b669b5ec49652e55a8c19cfc
                b4d389066bb3aa4d9d7195d30c496ec4250138ea1c335d6181b
                25793ff5d0feaf91b7d27c826ecda49a9b9c8ff880091963a2c
                cbdb5cb45eaafbfc8b93e753bf323e2f76b0a61af96997d97f4
                29db90898fbcc2dddcebf04d0e2a3d688fa56655b41b0a628e4
                164a31308799ea58984d44739d9720dcfdf4bcf2808217408c4
                33d263787405d11dce0854fbafe59f58d39a2995b991187ff86
                d3906e1e27812d5acd2a8d11b95ea20c7bf1e8ca9146cd9bdd1
                0f899e3289bb1838191feab937a6749c965c01b41e6febb62b5
                15efc416b9470214d78d4a47bde46b0c8a5f8c4672e8d95dff7
                1b9d7bcd2f94c1d115461c5a847baa8ee4a8a67dedef4ea4040
                3326710c23394b7b38e193b01670669f2c6e06c7963da8debe1
                03a33b49541fd5e0bc77b916dae2244d36bfc3d53f0f1ba51ee
                c5a18c2f258edefa2946f799b88e17ea475e8bda8cffa3531ed
                246820882e32f7ae0425b129a8b0d20e6205d1a7f85bd8efd9f
                bc7dab57eb45d187a25d29b71d69254a36a5125b6af9db41caf
                369183987e0f7077253969d9d1c0887a35fd2ea34eea81fc930
                b1a1aa11db1e996a11c49c39f570d0e3cfb3ef5811a678dc445
                1c5cf64898ae3b53e417c69f09438c997fbb453b9d88a1cb603
                e2016c1ee79a36f2e9df75f65eafa3db33f0f377c71e72f77af
                85a0114306e1b21921d532b6d140e3a2c5a479f33c1582386c7
                0c75e84765735b610559e8aac6149ad174213f2a1595476b290
                75b71a025f05fec67fed05e5f193f2b71e0352755ff4aa61bc6
                3f0240576033351676690615 8a2cf812fdd5d11eed2ca3e4404
                58ae1bf76cb642db5772d672d932a336cd838339d9df2dc2459
                a15c173b9e803a53112a081e7c2c945786b24e6d226aefbe7cb
                184a23dd504813975e25067f33bc90e13ecd4857473e0bb0fa3
                3b3f5f0255eb51da214717511378927c0d04d1bd4143e815d83
                2d69af2ab208a19243a0371c1c70ad3821863aa851b5447c53c
                391417dcf8e0506aab617792f24c80e4122f99ebb25341898e3
```

```
              0d8dbda4def
   shared_secret = e324b3ae9780cc6d0a54aa4262db9c9c5948ebd45df2f3d1
                   0eb22ee23bdaddea

   seed = 0707070707070707070707070707070707070707070707070707070
          7070707
   randomness = 6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b
                6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b
                6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b
   encapsulation_key = 0e12760b95266a50a52bc6ba3df697c1261d3ba51098
                       7a299a83cc0b9134c2ea4ddc47889b72c6dea65b49e0
                       66b1a2822f269e8ea904a667cfe6f7035aa83cd9c041
                       efc38d23053ea6d754c550cd5d1936d4e74ea047c4dc
                       f757de9550972c82abcbad83c32838c18451240c0907
                       a573451dc746bc491c143d14837af83c4f4b1f5aaa59
                       bd5a2b03c144ba6ccb445bce2d384ab4082327134212
                       8a2b7eb68624eba59b3b2b57d9a4ac7b630d063400a2
                       75ad71b6b08a8cfe93a64d368cef666a4d208b8f39c4
                       42400c1a7c4677658576417b5b026d99cb80e01428be
                       00c720e220a2705936a62d6e737900bd8c3d0b464ed7
                       650dd7c84c250dd73c7536abbb4013809927ccffa539
                       1bb254294c7be0596dd29aa37445957b2aa88dfc5444
                       7894773a34e8e87b05520c9c2ab4dfd69cdd9a52c7e9
                       352a3ab94c07a26d468f10b2632a6a524e06234fbb20
                       08f17cee6a59efc51b4c483fa5264c9fb325e9d7b9b6
                       6c6aae91ba9f9a29743968c5533a3750bb9554223b60
                       c8b964cfa7346948cac1000d840488c3d211b4e7d463
                       ddb15551862f01d77e87b60899e25164cccc814caa5c
                       0555f5413ffbdcb5101458a26061560463ab33cc2174
                       c61f5861986b55d6206612f386c996561b51b63a11be
                       965a1fae45b251476e96c3864925646b6246935bbfa9
                       f4bb39437195c6b98cf81a071a70f26b0ea61628fdbc
                       91ed299b6326ce7f220aab6965be645ff7c51248e456
                       adb343f10990243401d8e05ebc48b58d2a77b21341ef
                       513e66157b83596f1f447695e8c82279922e15987ab1
                       4259157ee6e07b5ee28dc41c68dbc14c39131fc7a4cc
                       f6420f65479701413d0eab484bd55dc1669e4e3a3eeb
                       cb118c899b2cca6cb2dbacf6f5a717ab0bbaf0214129
                       9d32c88426aa4866173cc12313f2c52624005e6fe176
                       ac02bf45a9964659020bd03b9ddb8a99322b0452a2ed
                       dc6ea752473f1c1c9ab051dc1973e81b1e8d74640614
                       8a8621575f7c71cd2879350a2970740156c69c9ff4cf
                       e97a3ff0a90f16e90336f6825bdb8ba0a3ccb2f181d2
                       6cc88605493b442a9d5a9f788895b720516c865d575c
                       75276c937e2252a486c90e64b1c115060dacaccc3372
```

```
                        d1475c3381098275bda23a52083c6e671825e57b4060
                        6226247432213988a7672d80ca32a2356e161b5a3d5a
                        218cf0c6788c62b786003154c90312001e73bcfdd331
                        2573504a0c402666620b31606883580ea09f690c0cdd
                        948520b19bab2b30fda60dd903c8b4f01a83238ebda1
                        636c911895480a8e5430da58462455488b71a735ca62
                        c1928722d57c3d86ce66760433c15357eba556db67ad
                        b16f8a02cd995c2525d21b49a06020daaaeaea50d332
                        952f399bdc859574c9c9c6056765d1c257e5a655c9a6
                        c619167963afc850027a00730d60b33e2b897e71b564
                        66be0fc98a1c314b67b3bae780a622c58eb05570024c
                        989b286763ba420ef234477c2dd8bc86b9c9adfed5a8
                        c7b948b6735bad758c04f08025eb01d217ab94078818
                        78466904b2e4965b2275155fd1b8000c7b2983a9e8f8
                        7243551dc31b884867b3e9418c1d5196f83b2e7edca5
                        5cb21dcee430969366fd02a85debbd759763010cb918
                        b13460c33bda4b43c2aaec2b4d19800eb45b65c915f8
                        b969eff9e9e356faea1c9cf69659599b22f50436ea13
                        cf2f1f0ec871c3a10ac0b36d877f200bfb728d9f3f8f
                        5f014f211938c615f1f10e5000eb9d2243df6e9c8da3
                        aa6f2f41be8f46294d2e49c4b78409101c
   decapsulation_key = 0707070707070707070707070707070707070707070707
                        07070707070707070707
   decapsulation_key_pq = d7b4cf68d3f1b711924ccded71a241faf8162f7ef
                           6ce748370a10e86b94befc198683377946eb96641
                           eebf10062c6dde3a010a09b2ceb1145210a9c17ee
                           fc5b7
   decapsulation_key_t = 19d62650372cc18fd0109cd6394d638ebeb5f4cae8
                          36ca4aa56825e9056e3ad5
   ciphertext = 892f7a7985caf0c231b2b35e3bc7de3e5a4739b72d3f9be342e
                326c0173d55a5089ebe9826c834792a3236800eecc2612b4d92
                ecfdbed013a6bfcd4d1ffe5c4150e7257a9e7c0b2e0cbee757f
                c86b5debe03aaf796c76a5825cc78667189e0e37f4a1c3dda77
                0eb8e6b978c89181f4871be9a295832334dc3a7f2b953f7df43
                f321137a9ad5b27e344678a79e386e402236124753e6dfcba0d
                d0dd97017461c2fe039c72e9d0073676f0749d8cc9bcd6ae0fa
                6f14db0b52575845c5b59b82aeae93c8fa1bcec6edd081517d6
                f2d3ed91575b2dd7b5893f3dd755d842bcf3e8d14afc5c236ec
                66236b33ba875953633eaa23afe2974d00179b72d117d9b8dee
                5110036f418baa0be052ec09d70fa36c943bb65050468bdfd63
                435f2edd7962cc98a0fc6b1d2a2c31a3581c31741790e4f7acb
                162a7146f399605a08cc99b48a96caccc3118ad9fbfbba58f29
                a121ccc604e9c0987f2250be2072189d8b01d594e946f0e5bb1
                b4e045ac5e5608736472386584f455be6e74b9cb31d6ffce008
                ce283b3f834c56f64ef829dd492eb70f6815c45128c66e77324
                bb03f71baf57bf0e200b5a59bfb1628e2bf209e8d3d39a2fdcc
                9c3cc7655224efa1efa86f550e72c11b5ebaa0b375e11d77d0a
                4cfe4f1f5eb048f0cff1c2882fbe01d14fcd97cb2ed5a40aa97
```

```
                c125f81c8c91164cbe8477058ff9e380604da9c2ac1b061853c
                2e4e979811bebb99948911dab9cb03d7c4975461d8e723bc415
                a3912fe1108de37b32b49174b722022c80dfad2881ad1db9f1d
                6d06090cb1421d3798fab2df0f4408c11d07be121ba66b406a6
                bcd892cd499e35e1c2c20c15c87ee0e79612cbdd04576955bf6
                1153eee2798c26e4d6d3050f3de5f6771add0495459e5300bb4
                e139839bf6a4206d7865c159d1ba9bd566e73d9a085007681d3
                307040c58616f369c6f2baa54fd59b4e27b806513ff678c2c6b
                dcd423e67047460a3a39cb04ead7b095317f0993f3ed75b5fc8
                b74c458a3bd6347c6a82640f4041f0168690f8f68f2cfaa4205
                969fb4dc9ad42d26b3fc2ba5bb08b322d0203118666b665e204
                1fbef0ee957f73f60fec892a65316d3f733112ef2a19c79c259
                5ad99a4d0c98cd148326ee8f2f7b79a161333302268c4270a96
                d5d67e3503b688a332f26543ce54c3dc3817ddd616624ef715a
                41f1a80f4510fc769892196ac3f4c62dd0391d4c5f215ab4472
                99c7bbd0ea1af7d621ad9d662abd35ef65f900a40b36f32f035
                2c97a90e76217c317f1890de7703d6009a218e75037b68c6d34
                f0f8ca6bef01af7894883493da5c47d0fa116af94f948747c96
                9b9779baeb8b279916b6ad0eea9ffc4afc1bd907673203413b6
                09b47ee0fdce780e82a6987d63887c285da97609736ced5fad8
                faeef141d8d0344d70ab0795a6668fae59aa65d411107631415
                112288c7e3284e26b5dcdabf6960821bb74c79fbc6fa73da77a
                4220943e86cdaf4a73e1c5bd918eacd53f6e085a694b9337385
                b409bb1f8604ab2b9bbd390f69cdf50ec2049f2e279a3aec282
                62115bb6dfa3236bd67d6324c60df93974d6e02c4633cbfb821
                200ce8b43977992a98e1c712fd8187eaf9542db5f05267f6fcc
                09dc523c960
   shared_secret = 5f8deab6c11f05ee208ba968d28917f8219ba2c0c30d4165
                   1c3382f4d56483c6

   seed = 0808080808080808080808080808080808080808080808080808080
          8080808
   randomness = 6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c
                6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c
                6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c
   encapsulation_key = 003180282264d14206367c682c2a282a58c114675507
                       95801e36393cc16e49f565bac995ab504448d4840b85
                       526e836ca6d641f151bd50897e1f9a5f6c718a61f97f
                       866b364a217c87e52cd28765ab18bf3c931a35150d1c
                       0c32c6b863872a23373057bec82e671986fad2cb15a0
                       6a9687a0ce923754138b4c54ba93c082c147cdf186c0
                       d5746cb6d54532a2afaaa701220342f6303ea7b66d99
                       42460722298e3bc2f0a612a22a986946737d057fbf3a
                       ce20cba6f97503fe03caa5c3974e8aaaa3c7ba62bc70
                       d1547ea9336ad15315cd8a2919b7683b568aebe54b38
```

```
                      5612f8829399d83aa3c2308c49a73379481a690afba6
                      36e14c7e6f31678c022b552b19a6b90b252a7122575b
                      a041c2daba8db6ab6cb9d13b5bb391ef0b48fd578e67
                      cab1d4d01cf4b492f136c9c4807b4a2479f35b255f23
                      4436d71a123b47384c1b6909b0d8c55575615a314178
                      675cbc94e746a415bbdc912474042a93d776a89913a2
                      102efa9377b85b0149075eaae72c6aac3d91c74f71d3
                      8c063963d3fa0c4da13f5202931f06a4515b08e22260
                      309b882252c972ea2e06160e1537bb38eb97e19909e5
                      8a3f3aa007daba597d08ae46767beb517fab0124bb39
                      ba6eabaf131b9611a9bbb26c1c52556030599be5382b
                      99c79f8d4356f3dc35b08678a2a1b24b3cbb6da29f03
                      a1bcf1bacc87a642d676abe5826e3836aecc878d2d67
                      580e39b9c55b7ac1e6b8a4ca6ec2e8934412258c0ab6
                      708135fd030cdb34429ee0a19c782623f081c0564b7d
                      c0bd8c35b831672a8413754127a45ac7572185185f44
                      4f017640b8a4c0819927866332c45374c6b25b88416d
                      4094081e832f26d44f8cdb04bde72f17e38986a6a693
                      604c637cb75805092cfa7b2921665e0803d182600e00
                      1b6f023cc39396c20018cfdbc85ac8bbe5cb6fc094bc
                      55c854e28aa3ceabc7f4e1ba13277628a1304d6c4527
                      533cf9d2b6d43a1f6c71c71586121c3254315a6cdc02
                      b9afa12184e51d3db071cc671864f2ac51fc653a1b62
                      8173061068924f890b18acc74c4524240696bee4c099
                      552ec02354bf272c94b541b5f4495e73c18182712087
                      2cb4a36388966a081010b80a9cf37c4715556f9d0c3a
                      5f41c587a7cead9ab40e366b53612c745632b0146368
                      e0a52f0b078eb20a6006cbf5591e393c19ecfb8e5435
                      a73cc0c5ce3a008f5053df1647293271e1366867232c
                      dbb8c58066c105701735f911db1ca2c1b07737467805
                      e304d243c733a77ce448b639c295392b1458b4a1a847
                      4ca2968e0c78917a2b255fc247fe493bd0d9bec24435
                      1890a895e470d298052750166b75a98a855549c386b1
                      40bc24326b044a469dfa660fe51a928271d011cd5468
                      2433f5583c5205898c216cf80cc5456bce0accf88628
                      00cd36661332261297ee9854d230b432d39c5ea66726
                      34a294c929e091329a37bb5f348f30f482699a88deba
                      93d58745f2b013a993816e4c1b90d28118d9cafe2a48
                      bd024be328490b703177b50ed619a9b293944f30bd62
                      119eb15486a6c3659eb0aa97e1832d82723627670c30
                      b546337428a7364ec49539709dad61943a545088c754
                      e27c857910713376b859e392d0554a09c04d29aa8adb
                      8754a491059903221d689fbaee7d0a714487053a812b
                      f22bd20bcc6b3aba85396dac337ad43e5494047412cf
                      9d1e0099d80dedf5f435390786c8a9c327e76394d420
                      37808c7f2c12253e45cbff4a9f544b175d24b7655a9d
                      946ab533b0fa10f5108b17c30772cf4172
   decapsulation_key = 0808080808080808080808080808080808080808080808
```

```
                      0808080808080808080
   decapsulation_key_pq = 08f68b3e03568d1e99c5c2167cf41dba4a6077557
                          4d21a9c79414bf1fb67a547e91d5f36267ef061cf
                          681cbe41b9cb15c17ee52a3579a51c20397ba3bda
                          5ea72
   decapsulation_key_t = 76a574362e7f03f27cc6f4288e046d753df47649c0
                         07741468fc4d252745150b
   ciphertext = fefebc6f6f4dab06bd9b8d0a3a688b06e4b3ce999cff7eb763d
                80f6d288d9d8c58d240d8d217064c9848a1508726829e177a02
                b99ac33ac76e50a82d31e9f952098c4731a0fc35c9da8e9c87a
                f7306ee7171e3aee3a3d2d046bccc1594a9686a7749b906346a
                7c863d8dd34acced601a3953a05e8ceabf34797b4606eff63e6
                6fbdeccaf981c13660a8b8de661c5b753f73c7e2cbc733379c4
                d9c36b93b756f5becb1ed569d6db0b2d2b1102e6064cc4311da
                3030c3f1a1126df69fcd2c5c3084ee1cc75761e5358ac39c4eb
                d472caf4e555f8da38dba8ef862c92eacddec9c270b5c71274c
                15fc38674bebabdc7cae2444dec1e7977679578f051fe3ee9d7
                a188565d5fce8fbcb842b28a4d38d77eb37dac58099664fd1b8
                069ceef1e06ba95a39bf48f7098a9bff84f6f2df86643db5345
                5be4bfa4848d93caa1fc1398ac240d186bb3334bb5381c9d089
                ae3c8637deedeaa576e6b92cc7b66bd3a31f3c956b4aeb4eb68
                8b249cf9b57a56d3656b5374f806b02875562ea15fcb619395e
                c913026dbe5a6d488cf907745cc65dbc9274ccb5e2461b9e923
                862a67744c8b8ff19dda1068fe408859f89b5b8550ed08956ce
                2b5c9a617e7ef6022772a58b63bbdbf5eb057c4bdf30083bc5d
                e8a22628fd845bc6ebcfe27277d1d7f57ceeb7beb07a20ca446
                fc65a372929920792d2c46afe34be5a052ab43db9e0b3c2d024
                cb720e42bd20db4a53e5bb32a1356989b1d5850611918549e9f
                57001c9488b8eb12a36e85595ca45934fea1d601b42c67078a4
                fbe701496e443b49fc8822fad0c8fc3a25b3910a5158b380aa6
                78cda329e2cedaec1c4a32e51b4baf7091efa5edd6ae2aec450
                e15cfec1ced9a1d158c9f8f19e21155e4163eaecf7f01d16ba4
                95fde48f39645a44d3733ea265cff5d4f2129e3c83a6ca33a62
                23f855a91ad49776d64ecfae6878668efeeac930ab6fe918337
                0c61727b4049a1dff8579947bf16ad1c0e210524c4f5ae7548f
                3d3e532e694abed9303ff260178505542141ca980de12090eec
                01da3399e8e454934bb15759d348404d647bb2a409b9d8a9560
                21bdb85ddba1978593aa56d961ede3a707e7b0bb6f325229ce7
                54c702d9ebc35a2663c0ceec6b3d04ebd91a63854736ef4b601
                495c26aa4927b9ccbae3adc808b32571ff32288d46c2967a96b
                53e756027d5eafed7dc8d7d5337f98309ffd1a300eba2c02221
                a3f100b68cb066861fbcb39252ac446c3ed3a9639708fd866e9
                fc0bfe4a7aec198696aa13979287dcf1fdcd143a44a78cc6006
                beba2e1ae70e8e857764d233e54830473fbbd2b173a34c16c20
                32d004fe19d35d8a5277824260f32ae501e24592916ea46ec14
                a9bc301fd0c900e33a1b24cd153a25afaa34ee26cbc9215fc6f
                a18972714aab79b72939b9f4d3190b9bd64282c0e630b6d8c67
                55d291e33dc3cf6b6a740b565b1cc292f2cef3b8cc6a6f13a3c
```

```
                7b06525e4e7897f63c82502f7fd77bae5a80a63c7436fdc8387
                787ee34a000ac1512c5bb3820dc6a9b49e048ae622962818294
                b8210f6b88c29739ef9e92b3953c7e073ae38dde178f60320fc
                974a311b78d6820593ce11cff1ef147dca0d291186a45d823ee
                52d4faeb861
   shared_secret = f9d4fe89be29e5438f8ed2ee8d368c365e550b6336c55a4d
                   91f3d96dafb3191a

   seed = 0909090909090909090909090909090909090909090909090909090
          9090909
   randomness = 6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d
                6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d
                6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d
   encapsulation_key = 460393d6222435d92a68eb6b2384ae414ba04199ac14
                       e561f6711facf87180a4af6156a5cf589c8ec7983054
                       764231646f07c57ae4247de37bb73758a60b4d333498
                       5238563005ab337c6075b81416c241fce764505acd0f
                       e7b0fbb859e4172390e670089414107549ed298bca65
                       8a229079866b8b960a7c7fe46cc47a1773010f106b6f
                       5cc9c2f906465851a7716649b6a67ff073807cfc7be4
                       cac44cd1af6a372cb04161d4d39861780c6f62051dfc
                       c39c143dcbe49bbf5b58a8769b927173e4c7096c9131
                       0a91484cc80c55217b76124d0db0965f84bef016040c
                       f19947d61e05a14f322bbd918392f5083be540a122a3
                       b1d7bc7c49a868f6384dd5259850d427166752bf286a
                       3ae729e3a5a5e76209de5b9c0783a4c70504a338af3d
                       178ebd114b7ef700cc17919b258682d21a1244a002fb
                       ca209a80cb2a94e4476aaeb7cd002929ef999095c893
                       624667ae2bc8712b20e35815599196de478f674b50e2
                       8313d7695ce2ba3dc02594171a1ba7a095a4351a0f33
                       06f51b4c09ccafea587693a9519f4b4976260445421a
                       865a400a63b0a03a8d9a35ce3335bec1912460e1a5b4
                       685f8fb039a5cb444ca21f87c522c7e6554f29007c05
                       62e5f02eee849f29d39bc15b58ff58b252581adbb17a
                       42f2357ce62746b1347a4123d02aa5c3974eed863eb4
                       f309c5b265d038aa6f994e8de94da384321fc65bda70
                       4a15216451465f9d44b7e8a9b7e6d356e8a399e7eb39
                       d0b46d85ec0cc93c56a6d570c9a8865aa6c74f358ff1
                       c03b80042567796c41f418747126bb4ac29d738372fc
                       a1a9646ad6e7901581c6845c91c3989058a82bd80117
                       e7c73bd2da15cff522fbf599fa6840317608e410b52b
                       4c477827877ff612cf89cf6c87c8a72b175b6c8627e0
                       a10b937cc672c1af54b64328c733c22585b88c54d30c
                       1a22bfb6a2559b178db7a0aab6001ddac9250416ae5c
                       11c0a5a26a09d38518b28f8e3a7f2eb51e0d679f1d92
```

```
                      8b77e103f4fa6218f68a1de0af5ea0bd1a26bb624879
                      ab47a28e9c40042b29cbd678f7ab65353807d41993bf
                      e11607313430e5aa8c27b9af3a5f10531aecb1a1c371
                      0f2b992c99b604f7b2a3269a49091a3a56dc8b78487a
                      d9ac24e36c97d351855ee1715083a3e9c32f52f735a7
                      6cb008714fa83bc70e4caab72c485ac8431cc97cfba7
                      27fcc0af9c542d7d9199bc4b50a9ba83db77c7dc206f
                      da0547e2795a8dc36fd1b33d2ddab089d95eb16b15da
                      94a74ed8b7e8daadf8180721e0a1e31002497c83ce17
                      47fbe78cac291ffd967f23f47a8a30485aa352cfd4c6
                      907cb8b201bc3b9281eb51985e11cbb4b5250ef7ca13
                      c70674f395c52b177541b57b3aac77e382d5bc6e0c32
                      aade73c74a163c0f43a59c616d76393f39166de8318f
                      ef1b2c47075c19885ecea7b4acc674d1c72a2e4ca70d
                      28325f12cc33ac19aa9c5e5ab31c7ac6933c1a0a7906
                      5fa1e0237cd90a13c7b759980262378d4a17b85c184f
                      84761e071a973784b1c30a9358b76a7af10727f36960
                      f21c6e078d33fb528373a436fb237f87317b81c04926
                      245982aea0b39c24a67effe65a91b211ad7334f8e485
                      8a3b7d0ef21b3e443c0cb64e089408006b103f3841ca
                      b70b046b98e2c8aed94ad683208e265424b077389c2a
                      c6571f216fac52e35cd280e51aaf6632816204c82a04
                      f09e4fda885db34fcc3be3ff41f95700e4593bf825f9
                      3ab30469733d373e450b125db222ab72f2ade96db31f
                      ee093fcf254511547ac1ca7e926778f133
   decapsulation_key = 0909090909090909090909090909090909090909090909
                      09090909090909090909
   decapsulation_key_pq = e4c190b41d18fe33b5710819eb4a962a2a6af9cd2
                         663d9766a4896481dcfc8b89687089a9797cf2f69
                         d058df1f690441dbccf3faa91ead65b8d4dfadd6a
                         a4912
   decapsulation_key_t = 00ee28df5d8544c9ea9a79badcf995f43af90ef255
                        b64b6ca0c8d194528f7152
   ciphertext = a857a7425c6077dafaef133c62869e523a4b41110cededea6ee
                66b9a6bba634d92cb41d5fbef2ccd6f5f057951fe1b44e224cd
                2314c9ffcdf4c358979d6d065f1f12a51033640c07965e6d434
                2afd7b57d528786b398e13b6eca581b96fe77778d73bfa2422e
                43093f7c96434103b18cbdf0aa6549da8e169b66f42921b89ac
                8267de35446008948d6026a0bcbe61357e97c7fe7a95337dfa3
                177ca6167c3a2af8dc38e3d708665824acf97d6d7b152bff781
                451c587a282adce031b3efa26b6d8bf4b49733c03dcc4300076
                049e278d3cd872174bc374d77038c75203ba45d30bd4110b623
                46c3f0bb1d8563d0e2d58cac839fa693ca96a56eeab1aa4d26c
                c95e013674eec4f8f08095059f081a0d4dfc0735653f3097f1a
                37da334007082ba6619844547e0d3296669eeceb02ecbf0c5c5
                a88d5d1c432398361529e0d91a628e568cd9a18cb3e8ca41315
                ccbd8ff9cbbc0677150f2e06274ec9e2733f3111cd4f1b900c7
                a3a80b517a7d6917fd0753f59e8bf03267e3a43d60e1857d492
```

```
                2cd0f14b6d28602792dbfe2b4488e807023ff4a8b65f75fe1a0
                826d5ff490bac7be071b9545f6e7ee758caf460e7e92e52eb83
                dcafb5bedeecf44a5f5ef23690bd83aa5ed2ce0420c697dfe4e
                aeff5d64be78fd3d9c96f66fcfbe015d8a1e75e93eed734c267
                fa515220e9937fdf8df271f69c8e3d6dec76152404d86243421
                1bd1e4b53cb9951c48b796fbf4287d3386c65217b41f2c414da
                ada2023c43c08f8b6edbecc7f750968c4f16c3c983a95d73c25
                d3cd4aac5bd5941fa376e1934436acecf9bb9bd4409d0944d39
                3d852aa15d6363bbd83cc24b1ea841e00b99dbe9f7b9fc2a415
                063865b43ecc9db0a95336820d40ec4d7325d5066eeb2a144ed
                3c27f5072c9a2e596d395bd069fdb8871521a08d0e9c1810467
                a271b4067a54d9d81eca8f26d18acb41a7de599aab1f79ddd01
                28c07e44cf2ccef72368cb4474db47ef43917940a80d05aea5e
                8c933a0ef8a8516a6dc2a50df273288d97a9788629f001e4874
                34e6a4192466e63f0e185810665267a021896967d833c1f1086
                45a5d17334d5dde8fd617c786665d7df9762b8ec0676af697dc
                a63e62b597aa2cf89c558accc872ce9a1277f88c5ac160b2d13
                a27de6b4027353adc3bf596d3d6527532e66225fa53e2546f6c
                eb240435bb93d10e4677208e990f622276d04ab8f2e4ce2e518
                0a436d33adbf29c2cef8704a41074ed16c164ffcd1c8f09a2f7
                52c098caab09da3db75d84ca510542c3adea1757a553bf53657
                f03feec803950747c8ddceeb31bd658072f01b7972df731af5f
                f53bf8a8361cc918c6a00693134fe6e385cc70484d2e3e6d365
                c14fbe6e2332eaf86b7afb8da619dd4c13e86f62ed63da3b998
                95d6ee47b440e16a3615f341d4be41239336b02017481968173
                2503f275bf8bc494c251e5448ff32bffb3fe0787482b796c37f
                d8d25a28ea78620046b192ce46fa4c798c0feed181961441332
                6eb373e622834afeaff81aff308caaf83504d31b9898e848b39
                6bc86cc55c519f1a01125995311ba37d96aa59ff464baf8885f
                3bdd10b1c92f0b286990048d58105a7ab5ec1755763ecb4d20f
                d1817d6b2fd
   shared_secret = a0071e94b4d0275ed91dfe4f3fe87dd4a534269c7a5991fd
                   c27ac31933fad24c
```

A.2. MLKEM768-X25519

```
   seed = 0000000000000000000000000000000000000000000000000000000
          0000000
   randomness = 6464646464646464646464646464646464646464646464646
                4646464646464646464646464646464646464646464646464
                6464646464646464646464646464
   encapsulation_key = 3d209f716752f6408e7f89bceef97ac3885300453779
                       27644ef046c0a7cae978c8841a0133aac4f1e1a70272
                       77f671219cf58b85d29c8fec08edd432e787a3cf9936
                       fe0026a113cb9efb1d7214049527bfe2141ea170b029
                       4a59403ab0ce16760a8baa95b823cbb8aacdcc17ef32
                       775223c791e3740163941f9bb3f63346bef1c050c31f
                       932c62719429aff14c2bd438ab135bed692d56c77c04
```

cbbffd6335b578318b513771e84b14ea821262141ca0
06ccb8bf2500aa1008970f216fe7f1ae34125aa29049
2c069a189222adc322f97649c762c7d3128ad3bb2667
971d0744014bc3b67445cbcd0b3e7ea69fb1cb9f9c33
1f97487920187292926d04a25a2650abbd44982bb0c3
c6301fe6a61330d24d8a3c7021dc3e3392c79a139b37
613bba67a2984298507b84a4d61eef18acfb979af2d3
9caa4c0db4513815359d76fc378c63a7f4f3053b1716
8d0221cf0c2eec5514ba235f81d04d67c3b5c5180949
17671c26a7c046457533cc32844581277a03eb065c45
29a779a9a5878f2aac3f81db9ed3d8c9345697058cbb
99d379bca16d8fdb61d129960390524791b9d3e501b9
00bd1e5002e095be06c23f1fb212f5801f24b6b28c0c
5493d246d02aa29fa3acfbe15ac4e212eb0b6f69ebbe
a259a2703aa4c308224bdb741c65c7a5d4bff7882795
07bbfe513d7aa5694e7b3cdf62ab36432742d4a0ca9b
3570ba742fa803b46989c8526ea586cc4fc32866143b
79601725fa545fd280b404530318bbc3371194710b6d
74beaa629eb18a36a953b75915ae96999ba5c88cdc56
a46861c50032c9b630bcc1445a30878979bc55a2c095
5bf399b231203b90c651b6afe0e242b5a543250b142f
7291ed753d816098f7913302a8ce91641716623d4fc2
ac6772aa5f3674042b7c4a18a2186289a4ac4e200774
596ca03e6798c7506b984999db6ac142586bae0799f1
e776f9f5247dc574d8556ddf9bbbc4ca3643263457f7
4248010d62d4311268360aecb4902b450bf2050ecb8b
a7a92820d233f5a14ed31225a1d17ca6f19e825894cf
b1807d922cbd60761134be419144bcf72006366a4460
137ad9136c113f05eb54c409520edc72e4150cc3a24b
0f819eec11bbd19ca9645b0810a60b4a8a9e9c395539
6a1653955b047bcf4f98433c27236c570d75f809e44a
af2dc33665826351872c293350ab324518c8c0c80b52
1c80c81a56bdc968a5650315a830c8bb17532c62ccc2
3b1d46412c256b224fd4674491803501d0143125c757
7239689965b6989ca561793c0f85c62a9e13487da176
62a7188c70b1040a67ed4c3f85e74e3691822fb96314
d6134fe6a626b3cbe1461d62a7b573b2cc75579ffa22
967e36ceb2a1aa0b71875a22751d706b72ca9ecd0c81
00ad0aa58009a5c83fffe91759e6baa0a9345af99fe3
b69509dbc84032868844ab3f65bb1df8beadf36442e4
8e339c967023a525411544c789a2f04dacd06ffef783
02210450b931f6b4c32aab34a3f5260b810f4c9a946f
c22d3baabaa80ba8d9955d6dc35e8609b4256b482cdc
9d8977c1a47a354e7c527fdb1672e166917b95cd6351
820261daab361f8a2dcbb240c55abd6a8105e5291b42
7b566d731e6b7047189cff20d8b120e0b3e72472d1b0
086812200fd3698e23f06e4f4e08bbb54cc2f63601b7
f85accfeea2d17964c66b5194b0f08e18519faaee194

```
                    e3c102823062
   decapsulation_key = 0000000000000000000000000000000000000000000000
                       0000000000000000000
   decapsulation_key_pq = f5977c8283546a63723bc31d2619124f11db46586
                          43336741df81757d5ad3062221e124311ec7f7181
                          568de7938df805d894f5fded465001a04e260a494
                          82cf5
   decapsulation_key_t = e00b3f9d338de90488973787b0916a4a9ae8bebf4e
                         2bc07a7bc18f1a62215182
   ciphertext = d81018a94f8078e02105beaa814e003390befa4589bb614f773
                97af42d8e8150796f2c88a4efca81b8cf93c0ae3716c54ec1b0
                45e3875f38c2dd12d7f717bd7fb701a9fecda5ed8b764c9a35d
                4a5c1d8930f6071f653eebb2d1afa77debb8302d16f17e0f5f3
                920a71a4d49beafa0e1c7e443f8abca64a65a9e81a97e7357bf
                902573363c0e1a12e5228036828e3f759121fada92441fe334e
                85d79347e470d2fed945541d832c54baaa3cb7526c3853954db
                4f73547cc7c27fd38398bfa7704952cb841e38b270e4db7435f
                0ee22f57d7ad3270bd0c88e71b4b864cf2277c65daa10a6dad4
                c7abecd95cc4ebec39c08404b522e4ecc1545713f76bebd3b5a
                0f2feb3461936065dbd13f6a1f61e1b142a2af2e5a482ba2c50
                cf0317049c0b3bfd6d5e9240eba9111d2030fdea17e33b65240
                20d30b0c4f8069285f3a6ca267d287d01e827d8422bf5426e11
                688bfc73756af1841b1c87e126cb50c914b5b2b8673488ad3b0
                74cad77a3840eb12dd688f313ee1e9ff8c479a678f276356fc9
                d65e1d5b4c1e9855b4175db144f7767c12061769190fe6b5e51
                563b91f94d131a2b796bd2980ed0dab4ae7a7110e920007a757
                158a5eb8662cbf89ddffe9d8196821313cdc00108853fc4746b
                111d5b56da638d8ed2973918960f5dfe93ead3ae521e957cec3
                c8d843e8fce234c70ad055177f235439d6098bdd771b1cfcfad
                aab4f50a7378185c62409f383c8ff658c2a2af66498cfd81e96
                2766ac6b774e88424fb4f331837d0a28502708477caf8780a15
                6d723f68fca791e1cd2397bfc2b24c77c765d9b2af36f732d52
                107517efd8157b283b440a613f756c364ca108971a8878199a9
                3f260baec3e850033cc032c2e53f823576affb4d3b116e2d160
                49152c35aaa263ab376f0ad5ede6a749607a283e3016e62191c
                0e8fde33e718cd989591c9a205d608d99fcb8a7471603d716cb
                01b56328d7d880aec2851f4e6d8b5016c25647e9026ebb44154
                3e8012dbfcf078d4012b8c39184dd64f3821b4774ae4e36365f
                8baf2bd1f6667c017a1e65ff8a1554458fb3f367c02721752bf
                a56fc7fd566ae95ffb208f919ef12f4cf8a2fdd141a8df559bd
                db7b8d1f04ee6d4cf7805d142989caf216dfae985faaab9974f
                6d9f8aa1129084db8db912b1655f595ffbaa66491ab4655fd73
                4cfd4bb0c0289d4bcc8fc5e9943b351cb147c8db059a24004d1
                c3e3bb4c14a881e5101acb736c65c5d579acb67ee85a560277b
                43338fe79d34b772c5da001da3b5a3383dd81319a0b4542e6d7
                e46eed5314cc70eb231de27b6e760db598ba19995cf69be0e44
                58e35f3f274aca2455d43fe3344e183c6dc47c857dbe9907b41
                e41006d91b25adcafc098fe66f7554be8dad493c4f4b1dbf7a5
```

```
                1464139db474afab5572f92a2232b59be56a72c0505149dae5c
                de1e602877037de7802b5f6fa47a4c9a3e52d6ca15339920254
                e9ffb53c7b834cc0288ed9905a1841e9390ea94a8898bd4c6b6
                d6027e4d43c7867242515bbeefe12340fc6b3d57762f8badb69
                433f9c6d060f85f5e5c6b6803a816d141c075f63541ad10
   shared_secret = e5ba94031ea6efd69c09c254f6d9783136ba6037e2d4c43b
                   cccf19d6f3f4343a

   seed = 0101010101010101010101010101010101010101010101010101010101010
          1010101
   randomness = 6565656565656565656565656565656565656565656565656565656
                5656565656565656565656565656565656565656565656565656565
                6565656565656565656565656565
   encapsulation_key = ec7b50cddc8360f98b189bac73d395ef947b37d84538
                       86a253269f7b18b9eb78c1b63212471a0f979793f993
                       6b3f496f4b5394ea69c2a35729f91c688f6bbbb864cd
                       5e87108676c4014c2ba98204f911becae33a71e832ac
                       012bb827578810955f8c6e2d26c0b17b7ba574990884
                       546ba58bf6785721f3854f434cfea602e8595c71642e
                       8d4c70934b7e54c638f5a13e1a136bc86565e6b40abc
                       163ca65650baf953de7bb99b138ac1b695023103c9b4
                       17853c9d42e54fdb816174659d85a783e3d4613db1cb
                       baa63fb667a4a636804b6c4ae821ac5d6556688bab1d
                       c10d6779b485c63c0ddacb91837c4ff3402e62141880
                       72b4186a39c65bde524c683c95d3c8b65e37104f551b
                       6a3602eda50b787182d703ac6a221428b4553e3b99c2
                       b251ef642e31256c329b21d1246a71456fce700d7f50
                       cfe5390a1c37bc133809f102c22914a1402c205c0512
                       b733afeea04411ca5ebb0bca9392b1ee23935eb19602
                       4732daa2a1f79358e6e74b73c965a9e74778dc692144
                       2b19328f6216a5e814ccc0639a863a437a614def5a61
                       f38852151011b04a37bbc78c1eba4d8d1b3a1622a0df
                       f74d25c731abb2a5fe5919f835bd3dd97330cbb7dba0
                       b74260c963402160c4017d92256a3713c9e77ea0f490
                       1accbd38715511784c9ec287dd85a769e081854b32ab
                       a9322a3840f6065133228c41851afcb40ea509cfbb86
                       145fb8853ce14c649691136b8660b0077f3b2f9da82d
                       483c1414c39a9777665899131a8336fb828480986df1
                       02628d10b54239cc20231457d4bbb7016f76029661f1
                       4ffd3532e2f8494e1613430730ab915683c3c8c4db2b
                       4373a3057a097e23333605398b15cc4d6ac3fbd0732f
                       21026bb0cd51fb738a740467114e7c66256b830022f2
                       8c028392cff8013d617c77a47bbda11c4a522f8f2b49
                       f2822cc06338605671fca4518df9b3c506532c9cca31
                       75330f8733ce11cb3fd8b95239ceebc9483cb68bff43
                       b622911fcf4a9c57c226caa38bf0b081535999f57301
                       6b14563ec4826dc281dbabc633868a1d903d59207fc6
                       62a293735085c01f40b5b56cbb795ecabfad709d611c
```

```
                    ac73eaca579768213c18c969c59be58fcef6bdd8a851
                    92907cd0773f81eaa24be07e0d620e9685acb0c6b0f5
                    4b47dffb510384241c4b733fe08dacb2852b2b74cc01
                    4e974a5e9db35d80d7b83ad31da1487a0170ba7fbc1c
                    551a6f1eecb572084180b256962748d5e3200b731ac7
                    c3928585a153b167c92a48cd91668c773707c054af16
                    aa7bfacaa161a620600e8d08cc97601a53391da0247e
                    5fca60cd1bb65ec0417177a9eb78cde5aa1dfae34e94
                    8417b3cc0b223803f5f40e8ae3a382848ff80c418582
                    4076423ae4c137bd30bd81f04095c20a01e0a49f664f
                    8f2b7f6bf6a990993cbc0596a514ccebc578c6418e82
                    5903ae11ac52831c6a48c67727409ed7274eea03eef3
                    2094271b02d4535563aa4924a2666871a4b690540c78
                    b06043bca31ca4e42a03650ecab74792017217d10615
                    d0acdee124e3222c90d79362207e4f7779e097501cf1
                    40b1a3431ee0cf27b23a50373d59976d82b5b1ce165f
                    4aa1361157afad564081c85777584dd6058a1a4663b5
                    3234d7264fbac6877351d1928c6780f77d4720933727
                    1e305370df9aeffb74d7c75de55c006e2b2a979aaa76
                    aaed9e76fa61e2a0a9aff50c054b3f819ee2da1cc913
                    4008b9f5ec05
   decapsulation_key = 0101010101010101010101010101010101010101010101
                    0101010101010101010
   decapsulation_key_pq = dbf77c8d79c80ad6b0763d42a3fe53f0f1dc03022
                      0c2e3fedc2aa903abfcad08330db4ba490ccee095
                      988d9355e816055cf986e280532d47cc19f2240cc
                      23419
   decapsulation_key_t = a20315485f73a3c17e18a3f155ac33e9a980896b2f
                     17dc7f96a9495d95840560
   ciphertext = 600ecf4026683898d0e339eeea9ebd437a4a802952bf32bfa32
                6b48eb74946d0cdd5437e70df4b6b7acbf79efe60ddcde985ac
                fd8c2d23775e1ecc54eb6ee03dcc9b4aac150172737831adfaf
                0e63a4782bad2a785b9c39bf5e34640ea3da447efc2a03e23a3
                37ad1f542c32c2eb46f7b88d0bfba87d8efe8cd4456e6f21bee
                bcf3dd502b53d537395750ce963d289eff74621545d4a5d9262
                bd14b3dddd4ef880e65cbe8f2f8aad826f57f727a60aaaeee8c
                69e89af6c539fd4f267c44bee8b5385a460a7c8e4a809959df8
                6c1136ee23e7544cfa7524c6c04ed9ec29aed307b5dfd0108f2
                9294aceeb517a098b8cdbad5911bc75e96258bbf38a20288c69
                11b2346f842c0943bf8e9c34a0a8e518e92c8761c6efe6b1d3e
                a8aed9b2c4feacfbf3559f3a5e46e4dfddf81936183d4d1f9c8
                c1616b14db2057435ad71655d743fad4987a19e821d0ac666ff
                3e46b7cc0e90b85e1966962279a48afe2e9bbce89c819a8ba52
                476af074a071495398bd497f4d4f34026025452975cfdaa3e7e
                183a962bda009108221ecb20d218c42e38774019d2dc3262127
                8b5e88f99b62a9e746d16c1691ccf3e7e9185c3c493e7617f45
                1f632c161fbe6d8ac3217f10ed4bfeee47e4960ec4a53e4852c
                a02415438484220 44a67567a83e09d8e74b9d11af17d53c4956
```

```
                5ca53deda7c4df076a3e1b6368b1931d81db93e87f75bea6924
                a321376fe73b5a5b07b80a98dc3ab8d14732540f1b4b7176e27
                4a905d453eac1caafe2bfe4e6c904556ca91b01b2302215ab3d
                fe6b49f46963df632a9e7cb8439cd5ee56a1f8e2cd3faae5d8f
                3462d0ff931f5038cfa70259d963163d6163ef22b0c32081bff
                2763e98da87817048d4ce755e5d2b1cfe7d6eeab0fdbe766c95
                f125537a04bcf99026f9bd5be3b26b9b7614f132f6747dd6d96
                009a85ae6cbb1a14b9231099b67b04d7849875b6492f3b6482f
                8bdac305f7ec29f28ef4739934c6a7a2800fbdbff6eb2237d6a
                085ddfab8519db1d2b1e63aa6cb9b3b044278947dc3bcd329aa
                427d13267f93a6cf2aee8a2ab74d4288fe0b676ea85586834ab
                57e863d4805703eb8bf6e71fbb11a386e7b64a0d661dbd05f5e
                2924f1419bc799a089d44dda9066c6c503f8c80be8daa99bd48
                338daeb4911acf19328103c96f40a77ffd827d52294ba21ad1d
                52fc27e8b12ad65887024f41e63fcfe654152676ac363f2377c
                5b0b437e075897e33dd8d57227fc5a536629efad998a2791031
                50e7d47e4b7d11a0d649d146c6560c48c9c0c56c811cfa6f3f6
                2cf717ae571597bc297deed887672d8a8cec2929c2b55b95f26
                bd5d10ef30c0c4a6295d5ca601538f5a20ac1064d2f4c2a078a
                f1b1629a0c203ad047125eb9dce0d1260eef19cd4ad8ec5d73a
                01ba23e266cc6dd266c5a81af58ccf1b5ce0440efdd1fe7bb42
                177679b5e5095ffa0d453bc17b8921008531c2d096a3a4a4856
                3370462a59fe1faff2a81603f2d09ca2e0beac44204a4e03aa8
                52745b1747bb6c424206ae093ecb917897fb41b1fcf75c1227f
                a08876056a5ed07ac44fe0c116ec2de80b8e523959d7824
   shared_secret = 750300db25bff9620e893c2c6fcab9bf04d7f2e543b5b394
                   20485626fa274908

   seed = 0202020202020202020202020202020202020202020202020202020202020202
          2020202
   randomness = 6666666666666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666
   encapsulation_key = 08118d8819772292c976ec971ee3039195800c823544
                       484595cc63450b9db9414330419208c509cb62626067
                       a8fd8259160105b6d8a4023b056f5ac2d6159fa5f245
                       f00c719539a4601466f6b45b2a68bdb0db7424d4cad4
                       75a8d68b0d6e086c3f012414e22900f01179e8c90a8b
                       a1d285cdcc7c7ab1c7064e2c15233acee183a1075c04
                       f092a5e3676b1ec06d15d348e7781346ec95806a5e00
                       f64d1e101bfb28bbc6829372f32bedcc0de9a70a02e5
                       08b760422505481709bef10697fbfa219b99a815f47e
                       4bacab0e789ca1e414db529deb043bd8521c2d456a06
                       2a65aeba2a40dc6b9ce02474a71fdf852f343b22d211
                       0519955b964382e74a3cf78586eaba353b98228b0268
                       f8480b02c4b4ee208198fbc472117c4be567858c097f
                       b0869a40588418973c58753da845e36c0adf39c53ea9
                       c8ae24c343bc87bcc3be69ea40d9490592ec99e9a853
```

```
                        f4f22b024a1b15962b049a62bc198706e310c8524c51
                        872718d76c6db25cd824a1b75a94a7d341ca40be1283
                        b2111b687be69d38b7297a90384b0c0269ac911cd803
                        84b326357262ac13680dca37ee18477ab23e16448805
                        676adbe1a5b7732e73c0abc3c5188e6c7ada3c1f1f12
                        4663e83ad5899674253e9bb15f39908ba4917dc11025
                        f7504425a305848661c38cb09a82026d20c9bd23949f
                        285519db298418718023c8d7e37a5bb1062951b43252
                        49aad59acc06b10161416ccc78db6c6c3f685ad3d9b4
                        916c622163017f9662da4234bab8b8b1e77290867d48
                        c28a2cb33c7d2c7874c2be936ca0d6ba907d6a823fa2
                        4a18c56cc124209ea488ce620c18d00ffc8b8f0c11cc
                        5850c30b3a0fb7faaf6e526f9b08972207a38f760bad
                        1824726017a30634fd239ebda59651b4c8162346bb36
                        52dec39f56626547829ffbb052a5a6930f2700fad33f
                        b1eca8bbc40fcfe778189398b5527a09a24a53a958e5
                        c25353951b78d85916457c1c5046e497ae0fa24810e8
                        2d360050e4fa1bf55b719ab8a080c23dcd80c0d4915d
                        8458652d476f50f3a5b80ba6ffa9a76bd9524dbb39df
                        7826cc507a9d31aa29b6207eaa52b3e224259c4931b1
                        ced9b97a42e6745752ac0603917a694d7ec95145094e
                        d089008af675fe51b2b79970abc282dcb632c1fc3dab
                        85ad14893d0ab63b9e21a368845e872bb1468aa25255
                        4f59f90c9675cd044b930e37a96a213a28277614443c
                        ca4317e4a2af9f4c7124fa76e1d48f38981d7df03d2b
                        f840610861b210300156c3f999aaac1b2983c45cf000
                        2c922037bb4055dd1c27df511ced577bb8046e003507
                        aa7b2c52194680b93e2eb40719539b8a93b8e83b9e20
                        5714927264cbf0653d4429f504816766bf97f1414162
                        2e91b20177d98b8db9351b39632be41a48f39ee050cc
                        1919143a2448d09c2fb15a680ebc07963b788480631e
                        ca37e19213dbb6c5e8dac3eee81b0292cbc681563d05
                        779b79b5d8ec37b331b3c021719cb95e69ec99a0f97b
                        723303278b9403fbaa7f71ba70d61d082c91a6aa2c8a
                        3543b5281e1605832c740bf67036f2373571f09482b2
                        7272c8ac2c69b01f715dda83377aa093a044541f6000
                        848ab1ea65cab1345135a4552be42b27c4b980065694
                        134a90d436f0e091b02a02aa99eac7339907afbbc158
                        a5127540423f23f6927eff66915d745f4d42825a5774
                        4a69ae7c493df9ed49f2f7eb1d2a9b72432b61352a9a
                        953730c6295c
   decapsulation_key = 0202020202020202020202020202020202020202020202
                        0202020202020202020202
   decapsulation_key_pq = 971619c09e6627cea855bbf7817dd36cdbf7d2de9
                           12d66aa2d94dd0da30c9ac1200fe81d6ea2b42928
                           de29420fb451103347536bb655a2bab5fbaba8a67
                           86fe9
   decapsulation_key_t = 96141896442e2dca19ab5f49cc2450f804fa3eb949
```

```
                        7f879679274166881596f0
   ciphertext = 413c55d5710bae6376761dada807daffd4dc45f9f70d825e0d4
                6176d4a342f58f20d61879215bbe4a7745888381753426 28a90
                5da0dbaa1346e8e913f4738defa0768445f1c625d296ab06cd5
                47b93e764a388e63815b588059796e9bf3fbead072727703b03
                6aa73223007ad1caaaea0c6cc38d385beb06fe8d372e9145c08
                e1bc3cb5ccb12f450ab0f6f9da5529629a3f1ff6312346b6d2f
                cb20461e7b3b245a97a03ef27f2e5442daf2a5ea317f454528e
                9749f06342aa7594ea9bda0cdcc7c0953c36372359ffd69f2ae
                dc1adabf8a3540e32ab36ebc1350aded1072afe3b78a6ec2f94
                3d560f4849d6bb1ee24679e8f70cc0f4cabe7d4cbc6e090353c
                e8414a93de9c84a32e197a2ac95e9fbc5d616f85fe199e80793
                f6dccac203d2f236e7bad1a4e7ff51b3f3326a9742826ac6a23
                ef5a945aaffb54faf50a8f0b8c09c55cf2bc812e30fb3e687ec
                a91b494785f121241a1ea8d0cea089216c5a96a467c06d4f0a1
                0c2a6bf551637f0fd5635dc1734e96eca5e7c545d66435b8b5d
                d88eff4c2cb3c73c49dfc9e56c293febef797a7d36d21ba3036
                1f7fec7b0e51793f6fdc2214f420b713a1598f4dda1a29f9124
                469407e5c5c5c908e39a78ea0fcfe4df3419692435a92e0f9a5
                846690706cdd23b1825be8d0a843756fd97b4f277cf0714a0d9
                da3ccf1a31a07178399b803c7b4837980bc0172f58716b3baee
                5e86441d32bf31c7ed6e9c6d55eb1ed528a4a306dec7f37b3a5
                75086385a9f4641ef28da16d35578c743c8eccb0581b2fd308a
                3c9fa15c8319954c8f4259ab09f178508720ebb8a0d893a8c45
                ec23b2c1c2e43db439ff71fea6a9fdcd8a9d3c6e0f8b9e9e71d
                dc2aa52fc5cbf22ed67217d847e4c84b72e7f201aca56c7d1d5
                e51e0c03cb596a01d20203b38e0e7d3086c83a4a19307541349
                04487c43fb96deb449aa832e63a82d132660cb7976d9d507426
                41c28c8e2e1bb00a2c65e9f8b9591501ad60568af112a5cbab1
                34bb472fecbdf24badbc6562201e022c23fbc6354292ab743a8
                63a139dd4d67b1bdb553b3c57a5c7f5b98cf145ac142e1ad6ad
                5ea3954fa3c2b8ebfb6cd05b915dd1d87262d7ab1f1b47cc0a3
                babc15a7a1415976644c54e29338d79afa9d12a669d3c67bf70
                e604157815f041556a5cc1c8429880a5449d033bb3f1f2b879f
                0e689fc2a3e2972f75f6f25b95bead0460f35ef71d0bdba380e
                fbabed6365c6e7fcf2e22361b572029f0c90f2f74c8e40c7941
                ed8b6eef5a722bf2e5141cf43ed2a69b87901d546a85765fc49
                4531e61f3d723107659b4ce1f294c352fc45c28a82cb3c242e5
                d6b9cf43d071bd55b8bc0d47b225463a5075639569cb073ffc4
                e07417dbc5a30a8e30545264d64d98d13336fdb6bdf8c71041e
                995cd433a77a9d4ee25e20f757cf76dd702f7c8f22a2677f03d
                cba47ea1996b9d783e44737ec501a8c75acb6d7606a2b6eb1e0
                69576f3a87b32e587923fb79171c77083bb629efda6b9ddc1d5
                66d72a53161c165d0ccea7674e5b1af42b219e4d800da968d2a
                5fcb009c784f4746c7138edb9ee4844b739e830b05cf424
   shared_secret = 87292f18b2e7af74bb8839ddee15e832d2f4bfac14dc84f8
                   24906d951436aafa
```

```
   seed = 0303030303030303030303030303030303030303030303030303030
          3030303
   randomness = 6767676767676767676767676767676767676767676767676
                7676767676767676767676767676767676767676767676767
                6767676767676767676767676
   encapsulation_key = 04ccc68ebb7b60c6148fa94574ebaedb9c5ce5eb1ad6
                       9cc5a4d7bbf9a410295540bba271ae8a178bd025ea28
                       887ca8808aba8fac7a44260c6e39b883110155d0dcb8
                       2ae7609bc803a8f927dcc2c2033cb07ba90fc8b06818
                       8a7214e713579537e69801ce304251eabc8b34b03ad7
                       1246cc22f7671adf572cd6a2730976953535c59d7c93
                       baa5788854ad52f48e9cdc8accf4a3441392f006378a
                       450289053c2ea689a80699de7acc6bec4c2b182e3194
                       acc9fb1ce3e1b389c5879ce66bc692a3b15343d6e557
                       ff93127ae69007e6913d51ce703898c5449ed3602593
                       84819529c7b54b9f5b6c9755d0a627554772846127c8
                       a580a5b6a9ea6695449be144306d64cc810212727882
                       7dc25da96b6f4823ce5ed25a2b199f3902cd8bb82058
                       d4694b40ce0ce1cac1ea8a047a1ced942d78ac2923c9
                       ced1d563fcc24895b1683615b134856ae3f36e4b382b
                       b160171ed400902499c6a0b1b8701d89093d6d72a992
                       c9ad296308a2d44d26816b1c942a3bc479979516a0dc
                       bf16bbca1140554be69885a477d078ac0a267e829411
                       1cbb42bac3cc733269c7f84bf315258cf8cd04774f9c
                       a932c7416785796ecd781e17b6ac32277d6d14190681
                       1430da866478499a8c94c521aa4d4663af067fcd2c82
                       3252c1dfba800c7b1681955de39112c2fc5f4a140204
                       69bc22278a84494806d43528f8ad8efc88643038d9d7
                       1c79a50710dbacff686396c34f9800b0671b0da3c2ad
                       4dbb3751b3b3749b63e132a336f19ae8f37a79f6c713
                       c48b724c80465b28e578658bc8329f0c1d75d0ab1d63
                       2027a3cc8d749216f50440109ad7637f3ab1661ee763
                       7eb06e70d4c15db81a2ea25ecae4524476106210362a
                       7b35c013120b51ad9b2c88b452457b75a98fa3ccdcb1
                       83aebb1684b72c3fb5434c277907680e8ceca5d2fb88
                       dcb43b050a5557b19d159a6050a6115c1c49232cb515
                       0463e165acd4629ca4927e3ce46ddd1a733dd23f77b4
                       4dfb7b46ebe4291594015a4ab5ff00b643321856b3b0
                       62ac28f2c4cf7b30716b6c9a53271139685b3d2bc20c
                       f5c766265a6666652393af58ac25efcb502a30b9f6bc
                       2524cc615a911b1de63bf1710f9f829c91a573a960a4
                       4d43138a65c42d41000c601c7ad1537633433edb5023
                       387aad5007a09827a55b6a7e7a2911307e0f226e9e52
                       ae3ba4c0f14a1efe9571352278c5a4a08cbba7403c35
                       ec69cc2a2b364ed145b11a4e8594087236a4ba7a2d00
                       3aa89fb2c97580c3ce115727ea0e99ea81cc8354164b
                       0602e53cb33638dad5a39632b70f4706eb8bb6d598c6
                       717627fe3c02420583cbdac9460a9d55588ffafba8cf
```

```
                      748c16283b0e96b8f95100caa7a8d12029a433ab4efb
                      b9b2067a0c615d5358aceea04b4ca4bf584a452fe276
                      8cb5bab0fb52aec375c3337fae44b305f1389f123103
                      669c7901a1821c4715b5cac1c89389cc9f4df192cca7
                      89ed236f7b378fb2915106ea3cc1b90ce9d6c07b36c4
                      f09b5654e3a116c60dda685b9ef6893b1b42348a3ac8
                      7284eed683fb346d25a562b90a778e6b546e40b4fd7c
                      1d3c01983f851474c3832297019a808ef64957d79025
                      78981d9231b382169d533a2202e95d18f152e8fc25b6
                      15bb8a65482a2167df6ab2811c73bf8fefbec077f1e6
                      68494d422443a083b9619254ec3e6bc6f30245fb7385
                      64e071c7c638448d7882a566c87e7399522756588c2a
                      86dad8f2021e
   decapsulation_key = 0303030303030303030303030303030303030303030303
                      03030303030303030303
   decapsulation_key_pq = 49b46321ef5a24c1c036750879c0ad29dd08607d4
                        89bd7eaa5869492759d994d875e0beaac3cf90df1
                        b3f1e0dd70357a5bafaec8a36fc2d9b72edf3f57f
                        9db20
   decapsulation_key_t = d20034c38088ae9e3338d75e1954dd00001bda6103
                         6eabac6a3ee56339d37ce9
   ciphertext = f40d556d507802ebe7be0e65ab82b0aa9ff26c825d24f98148f
                75d7e910d6c7f5852e7023a4e246be81b807fea96928da6a8c4
                d23b8326ea90aa7f1f0673a57277bdd08960f7f886777f1725b
                882e1996632584fce4356f7345abd8f480514275fbbd96ec6d3
                202de46e18e7a827d4dc62c1681c36018861c33cb2f4e13ba5d
                a65558441caa6ecf82a5e74842268f4ef5036deb2f0f6f5cb42
                2dc2b723a7f2f69830a52326621ee034c8a9e80f39070456bfd
                de653314040b4f41590723b66a2d7e41153932521e8e51108d2
                d98841b2983baa43b0dd6a46783be063850b22a2dd05c1f9f57
                8360dc3dfef4d79e8c20d2d0c45687ae19395355e7cdcfa039e
                3c36b6df4ea11b4122918fd6ec63ec672ace58a8ed9dfc61e7d
                3b5829d574833e0e61fa08419cbda05a85b3c4b9957a0968d58
                25d0d052013e75f138c8d74929a631a0ba2ec9555e2767f17e6
                e22890a5cb00f63f09e00b8decccf7d7d0e369c4396cb429e53
                d8cd4636ea630d6fc55143e6146a969ed0839ab05dd079da3f9
                46b3deaad2774360529f2aa7e6c400b66a5c449dd8362fae1a1
                bbf110229810e0d4725cfa2dfdc046d4c18637e1de3ec2b5205
                5c237238de0167eb0844c24a8fd91ac9f66f86efc945c0a5067
                2926efab53bd0725ae9ff36e9fcbecd58212cbe7e0f248b9ab9
                0b2f56497f196198043fa10de909b05bf3dd1d20630f9707095
                f4f80d044418e67ccd79e8f28db7acb1083a2bc63233a4f4798
                f13f21e81da6ee03c614cb367aff05410960fd366df06691b37
                4247de70fcf916e653b2bf01b49cf116324e8104da61a621b56
                6a62c97c6c058208e4825727cbb6c2ebaa0e888659094aa0370
                9659e272b4209c18366196110d71120b203fc71dd5d3c17be45
                80e5ade64a3fdeea5b85ad33fcebf30b857dc7cfe3ba52ea826
                9cadd7dda308460201e0119f8918de8980f04b318f39487e65e
```

```
                f0e0b83c2396d2fd87f4d54dd00b405063f072659d6b11513f4
                48b20deda3d874987c252b7d16d94c4f811c97134e5e00bff83
                00e718e17de3735bb4bc052100a3823f8db4be2d7554003481c
                e6d899d74c1ad9944c01d933305851458933b3f780ad6c1db48
                9da507621e39be174c71f73ec9c1ef644578bb1566136f17e91
                b475fdbf354cf4f5a6ee300d3938f5b4a7b9bcb90188a3d9c8f
                ab1326df69f5c3753a8ff9c5a7bbc4e2255954dfb6a2ce81381
                eaf9d224005e050eb5f53d05f0a41bcf4f3c0e8771e84eaa46c
                e27b0438d4ce3ebf9eb25b5351643a26f607c41b6494ac77e4c
                4a2fafac8e3cd872f31816501efd66c41795fa0d01ac0290253
                cf6c9d0dd8d5865684c1a02748a824417827ee374404a59ba87
                c3ec3caadf08b0f920667fae9ad18560edc3f8571986ca0bf1e
                f114d394c08ec5ff221e9f9ce7b6508eb6c38d6041fbe7319bd
                8874f35bace85c0bcc08cdcc642ae7fc264b9be08a26e5ec6a3
                618a078a128d0b8daf46e404eee4123b379a81680c8336036d9
                a44c12bcc23ed7b1b96442108843e5fcee6ca3bf39d976ab36a
                808531bd7ec2e4b4f8aae3a90134534d50f411d377a2c05
   shared_secret = 38c469d91f19aeb79dbf1aaae4d1195216c86186b00a798e
                   a3a6e544cf9c074a

   seed = 0404040404040404040404040404040404040404040404040404040
          4040404
   randomness = 6868686868686868686868686868686868686868686868686
                8686868686868686868686868686868686868686868686868
                6868686868686868686868686868
   encapsulation_key = 6afa82ec0b8e8449591cb9a11be36dc43146c18a6ad3
                       f175897933d25944c3c643f50332f1cc4f6a9707a387
                       b5c40661ec41b36d2bbc4507758387672fb4a1c1196e
                       aa81b01be2864cc958a0642496f264b4042ec5f7b25a
                       5220a8a9c9633081aef104ef9abd4da0af068a84e7b0
                       3f21e6b60212a02dc48ba7865877084a1b025443e38d
                       60bb6fae8ba88ea4538d088bea758f6f9a5c26a9c446
                       99ad43080d3fdcc2d910b16b297bb86436e3d5b79dc0
                       1230124867c1be64a9cab7aab9fdb47eadd15d00ed84
                       ac9a37406a3665d7cbdd106d1e6a29a81c94e3c841fe
                       9cb583004aa471ad2eb477623401e6959a04439bae06
                       a07058cf2ed94bce1839e636a8c0b22f782483ce798e
                       609bcd784605eadc0a06c7699b1b9ece550484124095
                       a13371028101c95721c2c71b098b15f3998785b36192
                       4f89dba9f292b9b18cbe232cb76e41bb5b35cad97696
                       2fca2957eb8e06356c250525e8825dce66478fa587ab
                       6b429bb287aaf21a58c900de0946ebc284873450c7e7
                       a0e08c856dca2191195f73b3aecce1b1c1c29cb24a6c
                       2fc3c14ca1495182645cf8486cb877d067440f118b80
                       713784474bd0214f23fc09e2c8b5df357b3733c13545
                       c9490378291646fbdb8403818f7d571a40ba7f5cea48
                       0fa00ba15373c60255e54384e96c455da13fd7dbcbc1
                       e7a5e9d655b0145976e190780b55c9c86ca6c988d123
```

```
                        0aabc8558ceca8d5cbb844ca8d95b30b64c024405226
                        61c9b07c866e497b5a7daa2398a5a888a4244d902101
                        05460fab31c6db3fd57941b869c24218b2ebd7ae6788
                        5e1fd691a3dc4388b872f4cab5fcd94067ea953d73ac
                        f1f4c752776357974b0ad7872ad603c30a174f963983
                        739e5fa5304d1705c6791e9c90342683a3b176a2897a
                        b9142190b3900d089c77ece41316b40611fc6bf7c81e
                        b7b589d65524f9c6888fd7c53ba810b0c70766430638
                        595dc3134ef5da09c668a804ea1e2f1469edba0d457a
                        cd8281828d02a915bcbc05949d2edc5c1c5856fa798e
                        5cd3587472903c6cc2bb43b03229352587cde988ab60
                        049b6f872a9aa82f25b5346fc56fe8686423b27e0f36
                        8a43d36a21602b4056022d25217df44a1fa330122152
                        cd2a581ca05d3801bf9f0a31bf79b8a7394fb8c9bc16
                        52cfea9c386ca7c703b5754c8243f7b0a36bc290e073
                        3a17a94431d7b05e0b4298a8b287fb1ad3b32a57693a
                        1e7867b0f3c483c0abdd2c05c81c26a60320d91207f2
                        04c2e8393a78e7572c8c296260351eb62940c394943c
                        6a622a8710aa09a076b513dbbfddfc3105379da08b97
                        a6fc68f2105088cb35f9683144ba24673513f0b6aaca
                        32c0e77173d7387294a9b96a08a014ac88afaca949c2
                        c3760b461dfc1ba5c01a956cac46a01dc7d9a992e1aa
                        704aa15af525911857d46682b137a3719aaa71f7a8ba
                        88afd6d43b127805f6c2cb55f88d6c590775577373ac
                        87356a56b89341d0e8657737249bca66b0b4194a5c13
                        dce045039164fe1530e38981f08c66ad2bb0531c3631
                        a86f6cfa71571b777b2461601bc7a146c358955a5b44
                        130d26b5c35322138133c083aba300a5def2c4f0d94d
                        4267a2ad23420b768c77d8a1f0428536667d2df42127
                        012291511a8c72738b82f0cff83b9315330886d61118
                        0d2383cf551afec4aa7515eb138a398eb44c0ca4c248
                        7488da7b0a98110cb697ec5031f995d7022be6c799f9
                        d3759079144e
   decapsulation_key = 040404040404040404040404040404040404040404
                        0404040404040404040404
   decapsulation_key_pq = 79f1b2ce3b601ebf5ba31006e5a8e4c86cd58148c
                           75a89173711aead9accf09f158d0facb085bf624b
                           4de5a388fab8e60419b04710475367a0fa9c1397c
                           96d61
   decapsulation_key_t = 432eab0f3a8eeb77c6b0000b9292c6e163914078c9
                          4a161829fcfb9bb3447393
   ciphertext = cfe31862853164950123baa75549418c7a406cfb60003b825eb
                292f1ba1f25c3b5b044dce0b8b16cb254d69658d516cd3445e3
                f18bcde32c4f46b4ac25dca4c4573647ab7cefd7fcbb7c192d9
                97194654aeac0f593eddc4464e7e125672fc7265f1664b32199
                cad45095359a4dd80e9637f0140504a7b1303fa69d121d2d214
                d5ea44e0046a120fef7d573016d8edf0c20749f05edccca4a30
                565df6e79015f04b03623d3aa25cdbaff330633470c02896899
```

```
                88c27fe49acc957d3be72c4bce05f1c80f3c2ad5b4e8a2714c1
                d1ea518f431f97f6d68eafb06ad7226a29a2b3a9e5403cdd923
                400a4303054876986f834848a4902659b288d5e3ef26a9ecb3f
                1be3630037d147301498bfe198b8116f244a12547ffe6a5006f
                748c0485fd72232e0c55df090011946c8b493f8aaf92de07396
                e901fb4dd8a4f291645267e7ec0335eaedeca28ab4c36328c73
                203dbca87e40dcf007bf8687dd4a776151e9d234f52442a33c7
                566b007f6537837cf752602624030615d0cb88238b91f578e07
                28b32734363944bbfce5884dc3c777e0b3f1ee4029298895e6b
                82f6f2307dfc267e27ca8d7d9b49b90786b7f39d906ca7b6527
                d5e31316fce0214418f95ab9504c98ba9e868754cb813014cbb
                196eac152861af719c7632710754cd2c72544c25b66d1d016f9
                7a409ecd11577a358647e1726da16d0a0e2591eb3b7cac7fe47
                fbeef10c6eeb9289aa4154d42ea75b864e0a1215ae35dd0db3f
                bbef39ad399c3d04d0d4ad9f2ce442bc07dabd366307eefcb2a
                b483dbe80b3eb4fe966131a587ffb2e3664d31e2c520722dc1a
                1f5d27ed0e937c4c89963576cdca001361f11bd39e2e2b36794
                3305fcddcbce6460a8bafeff8394beba9bb893f1a7abfd2e80b
                f10f0546e72a4051883e1f7edfe12ee1505d9503a83ddb2b998
                cb2475b88d280f1df688f472968f8c718f1f9fbd39fb3073312
                bc54c755210d0ef49f9f2bcf06a1099132a1e08d84b68543848
                e1538edd881620560e54d8d6f9a71ca2fd44f8fab9d094f1dce
                52f40c5aafe1f73e98a2a395f48d5da98fa5c95e4afaf84e7a1
                38807f71eb64fcb3b5169e8bedae1dffd725ad6fba9fd50f39d
                b9432cd5f379b680c09c5313ea73517f017ddcca33a405c0ca2
                93d8c34714aec241b9a634ec65c8c0b56e59df8e668e74d2494
                bca14d8102dc0592dbf93c0ad5f9dc89ac24a7e981feca0461d
                3fce1eec98a4afbb0b7e6c46aec385c9c0fbc203264aa6aa71c
                67fff159ccbac01cdd85c28835a98e9b7d0cd4c4330a0a5334b
                5838c072df4bd7297251cbf85dd8306e1a8ec893f4b9558133e
                20e0c9598f054e2b0b77d4494c393c5dd0e83a6520243edc562
                00f1cd34b8f69d53e4a823a46852e61672ba69447ee49522978
                c64616ea42a0b0c6cc953c748a550dbabd74010cdb8fd19c886
                2473f826267c8cf41cfc36100665ebd766390d83c1b2f795cb6
                d3c38dcb8e98c6ec0cd5111108a079d57f9b16960d94a4f238a
                6d7a25b6253b0ae0088ce414406fa7d020da785d9aa3cdc88c2
                401760535ad5f436dc83a542e294faaf07fb2253b009416
   shared_secret = a638747e2b93607e6a651d528435afe07e8733ccd150507b
                   96b639f6ff4a10ee

   seed = 0505050505050505050505050505050505050505050505050505050
          5050505
   randomness = 6969696969696969696969696969696969696969696969696
                9696969696969696969696969696969696969696969696969
                6969696969696969696969696969
   encapsulation_key = 33393446a76c2c01b44da5696d8452b29ab7b9178776
                       5366bc1a15b149792427844ff68753f957187c102d09
                       40c498b67332a7f9cbb82fd3bec9914e05a955035362
```

dc7462071c19e225ac96c12fa34a2e86e0a84a0c633e
044b3d93969705833a53a4257b7f4c1515ceaa8af9eb
7f53ca7cb402a4aba11c9d3206f8209c436bc3ea0487
c456a79e240fc4f5829e4977817aac9de9a0cf6cc281
31be92c2a6ec672bca1a8b3758092f8b87a11565c031
2e82939f8fd18024a71bb98a885c6ab99299cd43a620
8d2198a45bcdbec590157375c16a456327bbd44011b6
35cd1f678277347aa5a765b7208acaa4316ea523f59a
0671594e56121654f3581e882072396932da2e2ea02b
f5489e546c452b7c6f60e8a4c6112f6ccc7e3a7a4474
8aa1308807a08c15d78a2e19a2750a916b8c46844b25
7c2663a8895b3df8c40960e6b912623c8a92c9fb435d
20e6cda9fb456e55c1dd90a5f64a5ac2c61250461757
51aa742971f1728328c353f4a7a08ff16b8f978ae417
24494c436471505e2c17ba958ade7b2afbf9cc266551
8949755fd5bb8b15ac9b80b78fa615a918c4a99549c3
7c6ad0017c51c3963e3408b11848ddd4afe96b67cd66
c76e817d4c150de52a720505b9a4b09008243c0fb05e
f004b9c2c223f9230dc57b1dd3d1873457842b47c59b
9a6b39d7b61787b42a500c9f57114ec737bf7c45303b
8a3fa78b3c649cfbd166c60c37dea89e2df71ce4c605
fe45abcaf3a604f548ee5030fdf49ad4129b94516a22
a8b728112bfd209e5a5b565e20a8dce97748a7906379
0bec93bc89103c32419bbadc1ffc679e48139a0c8856
3f170d165729e3d710365c404dfc87d7c31efd24785a
9265e55c4a624315db4005019818a1e7c0367a70fbd1
6098e27a640b0f3dd9515d82be0637506ff171c6a31e
df453b40a6162feb7c3543506bc1105ce196e46097db
749b485808dcc3b4221470ac21880bc23c7ef4b315f4
0df40802f7324957b450032c3104f871250590a4c9a2
9687c70e02b46350781abc7c2b256c54bbc96eb20b89
1877c3a673f67c18197a0e3d657196d5673efb19ebf9
b3e49691612834cb662d2828938b1ac1a45881b9e51c
786c1a321814a8c396421b7f313cc2e4447e6e87971e
1660d94aad5f13b26bf49fa499822b1959f48aa88dfa
5101f463d5bbc8ca21b9d0857fd2e42d5c1c7a919276
5a3013eef54ca9e43fa99abfd8053e9059650b964d6a
ea8c26c13adc0a6d91208f2dea0da4d57a3a8a6be915
6a4065058cf965da10586b0945c30965bf8a436aaa11
5ab170071c3080f5c723c10d05963a162622438682fe
e1b619c2b10c207ad7d38ab1ea7eda0924d9ab6b4433
86af7b07fe26b8fc6911789666bc14619a381eba7966
e0b4ab0e528083806f46456f97e59276d5a6119b766b
1847d3a1ad3c4022cd0616bbc348d4e072f7d6827261
7b03bc9b25f569d0b11dab8c5a7ee11ee6c761ee6846
25322c6cdc815ee1c0acd29a8e1c826cf89f25944593
336643a46483dcaca9e1bae9a196f692ac0532cd9111
3d5d974963a524bf708c44e198dd212dfcf69213a42e

```
                      32e6b7c860148ed38c51002b83b0c4b979b52a753bf2
                      c3381c027623b8a8251e60f55524b56b959a14d84637
                      086a15567717dbda7aff9fd61d09589ac8c08808f786
                      9e6331a5689dec617d7ce2b8d5e76c307d6b15e1e3cb
                      07c9c51a4f42
   decapsulation_key = 0505050505050505050505050505050505050505050505
                      0505050505050505050505
   decapsulation_key_pq = 749fe3a6fc429b2369d9e8191f72d4fd3b292f2f1
                          22312bfaf4b6a90f1600c4670ebea7aec851d89f0
                          095c61a2caffb37f1ba7f21dd514b0e20006969d4
                          85ca9
   decapsulation_key_t = 730def4e090b60c056e1a9b653f479af7398bea957
                         71054ab4f455c9a86d7e49
   ciphertext = 6dc476cbc91fa3895cfd69bda5799b95b7c0dc87e5c78dec9b3
                67df58abf3e7852afb7b31caff856e5e4136a23a24f303c6100
                d9a0a6673164f6f44ea472f4614c2b42496d0049a27e02f1aa4
                5ba04442a74b5e0035df3d8877266a4241e650a86ccdfb0c6ce
                f22c62f376543bd5749353f808308eb74ed031e73c9f42ebdc8
                a484b30769a17906e39fe8fa65c0f88fcc3436c0bfe26a4995d
                82a41c6a99140a36d166cba6ad2dd065ac19cebadfd455c9fd5
                d15ab2facaf9f5c79bcd12d31ef88842403ebfef226f9a1de78
                d18d2a0a57a7808e5c4d9c7c510bd1813db60a2e0121e72c52e
                df77084222dbcd94a10cd4dc3b09080e8e5a8971761cd46ded6
                5c78ac4d896d818a400ed832830570d492665dec3f8c11168ee
                e66f33d0c13ce3062252f107a3777d1d91234f58598184ff827
                f6b2e73638fce0e4e51ef704e1d3f8dd5312191e36db31d82b2
                b76869d7eb03474ff616008158f3bf966a236cb3e8c52de4d01
                0cc712abc23dff6f5ce00631fd3dbaceba030c2ec18fd0c39c9
                c60134a4dfca521dcd71cda1179d8ef08f06a42686c360c9272
                f15b4258e78514c8814ad70a1092d26557a45764041b8324bbc
                d69b5d2868a6fd96c871cf83413113c898e4bb983187fa4c1cb
                b73cd41d3d4f4db185047afdd241f1b7e7007c00b03aa8ab836
                cedad6127938f87861108047298d3d945b343c62e2fe852a035
                4ff31dadc1ed08a4ddab41d91c0262283b11fcbb1ddb4e9fddd
                7cc338e925cedfadf4e306f84863fd45a70f57df0384e123422
                0103b0f693144a5ecc9d99ab1d6f725740d1bb09c3a4b4ea614
                ac01bfb1288bbf14dcd572ecbb6c822fe541b04a0d6498b5a14
                727c2d543c9647277bd67822a5fabda4a98f23ef50ad12b3213
                77fd4ee24b234b0f296049906aced9d08671de994956a217939
                4d37b585a31e405325ef880a108ec492c1c87da90adba72d8be
                4643ccf29431cae053f9cf5271f7e1c7a4de093ceb053351873
                d657737ebbef086640d417c6a05ae7fa9e30b11292135952904
                27032f26ebcd1546b9c9c1bcf01ff3d18fb1ebdbe0fee540f4b
                5318ba65877f457736d30c750e42e0e773aaa6e526bc6143ef6
                31f6b3f8811a026374dc28e06c92acd09e1f3f97c12e512b778
                038563b67de0d6b34a48157f1b936abb8b9f3da3adb88b5f36d
                0dae48627cdc1a403810c816e32e0d1112594a4f372e9abe4e6
                721ff83f488421022189b82e1f7f27a33e4d11969522e91d19f
```

```
                be1a3b9eb6eb3dbdc2b199db9e86e56bf695d0e6e79457226b2
                b3cefdd2ee3775dae268020392f0336c6fcb3928bdfdeac7124
                6343c08f2be397daa1fb9c252653307d0f7bc24111ba8df6ab2
                9923b4e7f3471be2923f46dccabb2063427f3d4e53baf6a9ecb
                88c12d9c233ff14f63ccfd76a8f046cc2d96733e72d56c835db
                c9a1aa2a5bdee915ae7eb3e5dbbc8ba24df6e634bffb4364a81
                039b06a2c5cb31c9cd8985e7fe2985c3e0a8f1d52feb2bfc354
                9c3817989cc1746fcfe8938888e12274481b1b8caa8136a07b1
                9cdc42dbff58c341de0087d8feaecf29eec0ed4fd0c3355
   shared_secret = 0594af7fe7a398ffe68f37a9f73506d6a3f7fd82b24e26f4
                   b93269684ed47172

   seed = 0606060606060606060606060606060606060606060606060606060606
          6060606
   randomness = 6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a
                a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a
                6a6a6a6a6a6a6a6a6a6a6a6a
   encapsulation_key = c3f9a6305222862c2c89ec0dbd805c547b2120405ba8
                       e994947b1d74eacc58277260ba837de29a0a2b84a7fc
                       80589334fb2626c9f61c01c88d60b20b0728110f0840
                       fc01a6187a506ab23d2b459fe0853c44f86a69953328
                       4577f7913b69898361bb67d3711680c6c25f2524c560
                       22227477f28a194e90b4702901b0046ba798cd1b8431
                       92f3bc841c8f9748a1ab34b5336b12c58585fcd010bf
                       d6c48e775e761525b260c7f6e646e8f17690aab51bab
                       30c9763fc53b8547d0b56b0c82c458c61d84587d9897
                       85600b8e987a36423d388ca11d61765a01a4a79ca20a
                       925908494eae0a3b6db1b08cbbb7a4ab5edcd96bd767
                       25e928055b0c2883ebce0a59bc9ec282cf300ba6c538
                       0d1b70f13b2dc6f616c76087a73a70daab7a6f97171c
                       a5997bf40e87b95f33a53347ba6c7ba89bcec9041701
                       226fda1243f4b1fa047740c7b753d630fe386f09e2a2
                       f96559ae979ed9fa5a78d1310ef311f97cc3b6a738be
                       e45b75e3a0cc714c81f72187b105a2120b9beaaac116
                       bf9835c504713f2218b526f13d8a8c02c95aa0f2927c
                       27e996e4564578e056227b07bbda8af0cc5d99f55eab
                       9868b8eb4d1b14065843b229ea3e2a0a748d89c4c304
                       198cd44cf77180bb8664f9aa1a9511527233cdb68269
                       76d34276f62257ec382172bf97b310bdd34056ea61f2
                       d74ce1cc9544b02263cc3d3133a308911556345a17c3
                       2acb470444f5536fd21f81cc3c968ab7e4db9cea564c
                       55d3a601066375f6417691c0ee3b39228860f1bc0069
                       3293c4bca327176da52b7282495bafc2932d1154c036
                       72f4db49bd40967ca41fb8f8696382a5208c5547640e
                       5193459b3507f4817ae3707930508969a18b1d168e67
                       b5939532160b50a538ec9074e733dfaa4af09755f831
                       720cec8519f3bd74809539347b8786868fb2ab9ab742
                       fe020c87930d37c45aa9b836c986ba01804a5de26974
```

```
                        ac647d8b921484b748d9999447875fe2746ad1112fc5
                        7ea3999f5899374ce2536c58310033ccdabc75d63a64
                        1a5651bd08079a41c1e59894cb3a1c8bac7614e96058
                        1a1d191a3a386209b6e82efc92b655c51d91e11e8d39
                        190863909a97cc6017af2c35500b860a21c9c48d4883
                        4eb561f58c683372968fd89be52a26995317855b3123
                        acc2071683ca669d78c3cce5bb9c9f9429a643bbb140
                        1d1d665dbf45ace6524cba3b0d33582105dc7c38165f
                        f0959d325914f437a4008ca751878bb8287eeaf09202
                        1b1b3647bb4a9b562a7aae80625739f66b636c309a09
                        376ac4cec6d76ce4629aef46ae488b4c696106952759
                        4e0c22ec55226f47085bec5e0343cbfb421ffc838b56
                        e9553e411ce39c811a1b4a53b051b404af3b58bf6513
                        76360c040a607f946c6357020ba1fa99daf19ad3f020
                        431a98b1647040038383719ff9fc7d4cc75d6bcb6d4f
                        00c834874b01b9a85e0c0f5c632734a3264d156c973c
                        14cae920bf0917cccc924ba90fef187f9783119a7a26
                        8621c7f29bbb28da1cceab369609c64efc5e91a79451
                        bc8100eabc85541d1f2435b96b532fa14c1cb76b9990
                        8c418118e2472c66511ab558aa06f03fd8fc15f10a20
                        99dc4df1360d15910d2a7747d8abab40fa3d77b7470d
                        8477cd63024aa40268f55139d37548223ed5823f1368
                        05752c0b5f7f23edfd90a89dd1f90ee344df0b7e3dba
                        a619370b955942588f0ce49e72f156ba743af7ccf9d4
                        a89f310c3012
   decapsulation_key = 0606060606060606060606060606060606060606060606
                        0606060606060606060606
   decapsulation_key_pq = f7d6c6a46a9c534d6ee0532938a99f0c450da4935
                           e2953c4daea5d5b0a59ea69c700a40817fdf445dd
                           5b73ed69a557afa27839191b8e71214ef9ef97e9d
                           9bb99
   decapsulation_key_t = 0a925a53f7ceaaa373f3f8ecf9c2d9eaeb351eaae4
                          dddecbd7eb180b5432306e
   ciphertext = 56a06e6443b53c24f647cb6798257899ea1c49cbfd4c4e3e54d
                d73a1139dc4df519067a5934733a34538f941cd9a2d9de37162
                3247f1bbcb728d8cfd59b59d6995a2430ab14490b336ac502cd
                21dea47dc7c89fa026310ec05fbbe50179b45e4b68c507fd90f
                ab06e36fb1c9b21c06115fe42beba15083385764cde8c527c36
                69507bcaded45f70a8cca789ad71e9087948e4f1d682c4a77ad
                306c25b1e6364f43fb51c0c5d72f455da72f46041f8fcb143f6
                7c7517b425e24cd803032645cfeba77e0d8d2d0cfb57768b8fa
                3238c10ebb99471710973bf9d22fea51471354e53f153dfbac6
                95a6f8ccb10524a0453e804bb013b450f38007fe21ce898c052
                a132ea74c9e69512ca4c18c32ae37884df520d12721b95acb51
                5067f3516ced73c930786d6924cc7dcc08b50a3abef4e0df82a
                a0b9c7bc199cb2dcbc7cbaa38ffbeea60e41ae20e8400730132
                f3627e1f62fc784f222213c2c479c4ed1f2159f724eddff87e6
                a4b5b3445e189590de4bb62bf66e930550144b44e23d6c045d7
```

```
                79ace9f94c0a688f729a0b94821b669b5ec49652e55a8c19cfc
                b4d389066bb3aa4d9d7195d30c496ec4250138ea1c335d6181b
                25793ff5d0feaf91b7d27c826ecda49a9b9c8ff880091963a2c
                cbdb5cb45eaafbfc8b93e753bf323e2f76b0a61af96997d97f4
                29db90898fbcc2dddcebf04d0e2a3d688fa56655b41b0a628e4
                164a31308799ea58984d44739d9720dcfdf4bcf2808217408c4
                33d263787405d11dce0854fbafe59f58d39a2995b991187ff86
                d3906e1e27812d5acd2a8d11b95ea20c7bf1e8ca9146cd9bdd1
                0f899e3289bb1838191feab937a6749c965c01b41e6febb62b5
                15efc416b9470214d78d4a47bde46b0c8a5f8c4672e8d95dff7
                1b9d7bcd2f94c1d115461c5a847baa8ee4a8a67dedef4ea4040
                3326710c23394b7b38e193b01670669f2c6e06c7963da8debe1
                03a33b49541fd5e0bc77b916dae2244d36bfc3d53f0f1ba51ee
                c5a18c2f258edefa2946f799b88e17ea475e8bda8cffa3531ed
                246820882e32f7ae0425b129a8b0d20e6205d1a7f85bd8efd9f
                bc7dab57eb45d187a25d29b71d69254a36a5125b6af9db41caf
                369183987e0f7077253969d9d1c0887a35fd2ea34eea81fc930
                b1a1aa11db1e996a11c49c39f570d0e3cfb3ef5811a678dc445
                1c5cf64898ae3b53e417c69f09438c997fbb453b9d88a1cb603
                e2016c1ee79a36f2e9df75f65eafa3db33f0f377c71e72f77af
                85a0114306e1b21921d532b6d140e3a2c5a479f33c1582386c7
                0c75e84765735b610559e8aac6149ad174213f2a1595476b290
                75b71a025f05fec67fed05e5f193f2b71e0352755ff4aa61bc6
                3f02405760333516766906158a2cf812fdd5d11eed2ca3e4404
                58ae1bf76cb642db5772d672d932a336cd838339d9df2dc2459
                a15c173b9e803a53112a081e7c2c945786b24e6d226aefbe7cb
                184a23dd504813975e25067f33bc90e13ecd4857473e0bb0fa3
                3b3f5f0255eb51da214717511378927c0da6244664d91d63fce
                62edf776cbfda72c88b68025f05cb0ca76c460d37fb8d30
   shared_secret = d11018de4d36cb4544612190b4613a7b76c703fc4cb782fb
                   26de49adde017e97

   seed = 0707070707070707070707070707070707070707070707070707070
          7070707
   randomness = 6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b
                6b6b6b6b6b6b6b6b6b6b6b6b6b
   encapsulation_key = 0e12760b95266a50a52bc6ba3df697c1261d3ba51098
                       7a299a83cc0b9134c2ea4ddc47889b72c6dea65b49e0
                       66b1a2822f269e8ea904a667cfe6f7035aa83cd9c041
                       efc38d23053ea6d754c550cd5d1936d4e74ea047c4dc
                       f757de9550972c82abcbad83c32838c18451240c0907
                       a573451dc746bc491c143d14837af83c4f4b1f5aaa59
                       bd5a2b03c144ba6ccb445bce2d384ab4082327134212
                       8a2b7eb68624eba59b3b2b57d9a4ac7b630d063400a2
                       75ad71b6b08a8cfe93a64d368cef666a4d208b8f39c4
                       42400c1a7c467765857641 7b5b026d99cb80e01428be
                       00c720e220a2705936a62d6e737900bd8c3d0b464ed7
```

```
                    650dd7c84c250dd73c7536abbb4013809927ccffa539
                    1bb254294c7be0596dd29aa37445957b2aa88dfc5444
                    7894773a34e8e87b05520c9c2ab4dfd69cdd9a52c7e9
                    352a3ab94c07a26d468f10b2632a6a524e06234fbb20
                    08f17cee6a59efc51b4c483fa5264c9fb325e9d7b9b6
                    6c6aae91ba9f9a29743968c5533a3750bb9554223b60
                    c8b964cfa7346948cac1000d840488c3d211b4e7d463
                    ddb15551862f01d77e87b60899e25164cccc814caa5c
                    0555f5413ffbdcb5101458a26061560463ab33cc2174
                    c61f5861986b55d6206612f386c996561b51b63a11be
                    965a1fae45b251476e96c3864925646b6246935bbfa9
                    f4bb39437195c6b98cf81a071a70f26b0ea61628fdbc
                    91ed299b6326ce7f220aab6965be645ff7c51248e456
                    adb343f10990243401d8e05ebc48b58d2a77b21341ef
                    513e66157b83596f1f447695e8c82279922e15987ab1
                    4259157ee6e07b5ee28dc41c68dbc14c39131fc7a4cc
                    f6420f65479701413d0eab484bd55dc1669e4e3a3eeb
                    cb118c899b2cca6cb2dbacf6f5a717ab0bbaf0214129
                    9d32c88426aa4866173cc12313f2c52624005e6fe176
                    ac02bf45a9964659020bd03b9ddb8a99322b0452a2ed
                    dc6ea752473f1c1c9ab051dc1973e81b1e8d74640614
                    8a8621575f7c71cd2879350a2970740156c69c9ff4cf
                    e97a3ff0a90f16e90336f6825bdb8ba0a3ccb2f181d2
                    6cc88605493b442a9d5a9f788895b720516c865d575c
                    75276c937e2252a486c90e64b1c115060dacaccc3372
                    d1475c3381098275bda23a52083c6e671825e57b4060
                    6226247432213988a7672d80ca32a2356e161b5a3d5a
                    218cf0c6788c62b786003154c90312001e73bcfdd331
                    2573504a0c402666620b31606883580ea09f690c0cdd
                    948520b19bab2b30fda60dd903c8b4f01a83238ebda1
                    636c911895480a8e5430da58462455488b71a735ca62
                    c1928722d57c3d86ce66760433c15357eba556db67ad
                    b16f8a02cd995c2525d21b49a06020daaaeaea50d332
                    952f399bdc859574c9c9c6056765d1c257e5a655c9a6
                    c619167963afc850027a00730d60b33e2b897e71b564
                    66be0fc98a1c314b67b3bae780a622c58eb05570024c
                    989b286763ba420ef234477c2dd8bc86b9c9adfed5a8
                    c7b948b6735bad758c04f08025eb01d217ab94078818
                    78466904b2e4965b2275155fd1b8000c7b2983a9e8f8
                    7243551dc31b884867b3e9418c1d5196f83b2e7edca5
                    5cb21dcee430969366fd02a85debbd759763010cb918
                    b13460c33bda4b43c2aaec2b4d19800eb45b65c915f8
                    b969eff9e9e356faea1c9cf69659599b22f57b8184a0
                    ce2e4091f1b4b03b77635cf149b6492cf75d285e028a
                    57744c424673
   decapsulation_key = 0707070707070707070707070707070707070707070707
                    0707070707070707070707
   decapsulation_key_pq = d7b4cf68d3f1b711924ccded71a241faf8162f7ef
```

```
                          6ce748370a10e86b94befc198683377946eb96641
                          eebf10062c6dde3a010a09b2ceb1145210a9c17ee
                          fc5b7
   decapsulation_key_t = 19d62650372cc18fd0109cd6394d638ebeb5f4cae8
                         36ca4aa56825e9056e3ad5
   ciphertext = 892f7a7985caf0c231b2b35e3bc7de3e5a4739b72d3f9be342e
                326c0173d55a5089ebe9826c834792a3236800eecc2612b4d92
                ecfdbed013a6bfcd4d1ffe5c4150e7257a9e7c0b2e0cbee757f
                c86b5debe03aaf796c76a5825cc78667189e0e37f4a1c3dda77
                0eb8e6b978c89181f4871be9a295832334dc3a7f2b953f7df43
                f321137a9ad5b27e344678a79e386e402236124753e6dfcba0d
                d0dd97017461c2fe039c72e9d0073676f0749d8cc9bcd6ae0fa
                6f14db0b52575845c5b59b82aeae93c8fa1bcec6edd081517d6
                f2d3ed91575b2dd7b5893f3dd755d842bcf3e8d14afc5c236ec
                66236b33ba875953633eaa23afe2974d00179b72d117d9b8dee
                5110036f418baa0be052ec09d70fa36c943bb65050468bdfd63
                435f2edd7962cc98a0fc6b1d2a2c31a3581c31741790e4f7acb
                162a7146f399605a08cc99b48a96caccc3118ad9fbfbba58f29
                a121ccc604e9c0987f2250be2072189d8b01d594e946f0e5bb1
                b4e045ac5e5608736472386584f455be6e74b9cb31d6ffce008
                ce283b3f834c56f64ef829dd492eb70f6815c45128c66e77324
                bb03f71baf57bf0e200b5a59bfb1628e2bf209e8d3d39a2fdcc
                9c3cc7655224efa1efa86f550e72c11b5ebaa0b375e11d77d0a
                4cfe4f1f5eb048f0cff1c2882fbe01d14fcd97cb2ed5a40aa97
                c125f81c8c91164cbe8477058ff9e380604da9c2ac1b061853c
                2e4e979811bebb99948911dab9cb03d7c4975461d8e723bc415
                a3912fe1108de37b32b49174b722022c80dfad2881ad1db9f1d
                6d06090cb1421d3798fab2df0f4408c11d07be121ba66b406a6
                bcd892cd499e35e1c2c20c15c87ee0e79612cbdd04576955bf6
                1153eee2798c26e4d6d3050f3de5f6771add0495459e5300bb4
                e139839bf6a4206d7865c159d1ba9bd566e73d9a085007681d3
                307040c58616f369c6f2baa54fd59b4e27b806513ff678c2c6b
                dcd423e67047460a3a39cb04ead7b095317f0993f3ed75b5fc8
                b74c458a3bd6347c6a82640f4041f0168690f8f68f2cfaa4205
                969fb4dc9ad42d26b3fc2ba5bb08b322d0203118666b665e204
                1fbef0ee957f73f60fec892a65316d3f733112ef2a19c79c259
                5ad99a4d0c98cd148326ee8f2f7b79a161333302268c4270a96
                d5d67e3503b688a332f26543ce54c3dc3817ddd616624ef715a
                41f1a80f4510fc769892196ac3f4c62dd0391d4c5f215ab4472
                99c7bbd0ea1af7d621ad9d662abd35ef65f900a40b36f32f035
                2c97a90e76217c317f1890de7703d6009a218e75037b68c6d34
                f0f8ca6bef01af7894883493da5c47d0fa116af94f948747c96
                9b9779baeb8b279916b6ad0eea9ffc4afc1bd907673203413b6
                09b47ee0fdce780e82a6987d63887c285da97609736ced5fad8
                faeef141d8d0344d70ab0795a6668fae59aa65d411107631415
                112288c7e3284e26b5dcdabf6960821bb74c79fbc6fa73da77a
                4220943e86cdaf4a73e1c5bd918eacd53f6e085a694b9337385
                b409bb1f8604ab2b9bbd390f69cdf50ec28462fb3f0798f9fe2
```

```
              c39f3823bb41cd3effe70bb5c81735be46a143135c58454
   shared_secret = eae6cff2b4d6971efa91c6333986693db4f5c46207af27ce
                   6f5964c0eb4aef50

   seed = 0808080808080808080808080808080808080808080808080808080808080
          8080808
   randomness = 6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c
                6c6c6c6c6c6c6c6c6c6c6c6c6c
   encapsulation_key = 003180282264d14206367c682c2a282a58c114675507
                       95801e36393cc16e49f565bac995ab504448d4840b85
                       526e836ca6d641f151bd50897e1f9a5f6c718a61f97f
                       866b364a217c87e52cd28765ab18bf3c931a35150d1c
                       0c32c6b863872a23373057bec82e671986fad2cb15a0
                       6a9687a0ce923754138b4c54ba93c082c147cdf186c0
                       d5746cb6d54532a2afaaa701220342f6303ea7b66d99
                       42460722298e3bc2f0a612a22a986946737d057fbf3a
                       ce20cba6f97503fe03caa5c3974e8aaaa3c7ba62bc70
                       d1547ea9336ad15315cd8a2919b7683b568aebe54b38
                       5612f8829399d83aa3c2308c49a73379481a690afba6
                       36e14c7e6f31678c022b552b19a6b90b252a7122575b
                       a041c2daba8db6ab6cb9d13b5bb391ef0b48fd578e67
                       cab1d4d01cf4b492f136c9c4807b4a2479f35b255f23
                       4436d71a123b47384c1b6909b0d8c55575615a314178
                       675cbc94e746a415bbdc912474042a93d776a89913a2
                       102efa9377b85b0149075eaae72c6aac3d91c74f71d3
                       8c063963d3fa0c4da13f5202931f06a4515b08e22260
                       309b882252c972ea2e06160e1537bb38eb97e19909e5
                       8a3f3aa007daba597d08ae46767beb517fab0124bb39
                       ba6eabaf131b9611a9bbb26c1c52556030599be5382b
                       99c79f8d4356f3dc35b08678a2a1b24b3cbb6da29f03
                       a1bcf1bacc87a642d676abe5826e3836aecc878d2d67
                       580e39b9c55b7ac1e6b8a4ca6ec2e8934412258c0ab6
                       708135fd030cdb34429ee0a19c782623f081c0564b7d
                       c0bd8c35b831672a8413754127a45ac7572185185f44
                       4f017640b8a4c0819927866332c45374c6b25b88416d
                       4094081e832f26d44f8cdb04bde72f17e38986a6a693
                       604c637cb75805092cfa7b2921665e0803d182600e00
                       1b6f023cc39396c20018cfdbc85ac8bbe5cb6fc094bc
                       55c854e28aa3ceabc7f4e1ba13277628a1304d6c4527
                       533cf9d2b6d43a1f6c71c71586121c3254315a6cdc02
                       b9afa12184e51d3db071cc671864f2ac51fc653a1b62
                       8173061068924f890b18acc74c4524240696bee4c099
                       552ec02354bf272c94b541b5f4495e73c18182712087
                       2cb4a36388966a081010b80a9cf37c4715556f9d0c3a
                       5f41c587a7cead9ab40e366b53612c745632b0146368
                       e0a52f0b078eb20a6006cbf5591e393c19ecfb8e5435
                       a73cc0c5ce3a008f5053df1647293271e1366867232c
```

```
                      dbb8c58066c105701735f911db1ca2c1b07737467805
                      e304d243c733a77ce448b639c295392b1458b4a1a847
                      4ca2968e0c78917a2b255fc247fe493bd0d9bec24435
                      1890a895e470d298052750166b75a98a855549c386b1
                      40bc24326b044a469dfa660fe51a928271d011cd5468
                      2433f5583c5205898c216cf80cc5456bce0accf88628
                      00cd36661332261297ee9854d230b432d39c5ea66726
                      34a294c929e091329a37bb5f348f30f482699a88deba
                      93d58745f2b013a993816e4c1b90d28118d9cafe2a48
                      bd024be328490b703177b50ed619a9b293944f30bd62
                      119eb15486a6c3659eb0aa97e1832d82723627670c30
                      b546337428a7364ec49539709dad61943a545088c754
                      e27c857910713376b859e392d0554a09c04d29aa8adb
                      8754a491059903221d689fbaee7d0a714487053a812b
                      f22bd20bcc6b3aba85396dac337ad43e54945218a81e
                      f4d5e62b8608e130d9278612d248353ce8338d4ae997
                      cc9f20d8726e
   decapsulation_key = 0808080808080808080808080808080808080808080808
                      08080808080808080808
   decapsulation_key_pq = 08f68b3e03568d1e99c5c2167cf41dba4a6077557
                         4d21a9c79414bf1fb67a547e91d5f36267ef061cf
                         681cbe41b9cb15c17ee52a3579a51c20397ba3bda
                         5ea72
   decapsulation_key_t = 76a574362e7f03f27cc6f4288e046d753df47649c0
                        07741468fc4d252745150b
   ciphertext = fefebc6f6f4dab06bd9b8d0a3a688b06e4b3ce999cff7eb763d
                80f6d288d9d8c58d240d8d217064c9848a1508726829e177a02
                b99ac33ac76e50a82d31e9f952098c4731a0fc35c9da8e9c87a
                f7306ee7171e3aee3a3d2d046bccc1594a9686a7749b906346a
                7c863d8dd34acced601a3953a05e8ceabf34797b4606eff63e6
                6fbdeccaf981c13660a8b8de661c5b753f73c7e2cbc733379c4
                d9c36b93b756f5becb1ed569d6db0b2d2b1102e6064cc4311da
                3030c3f1a1126df69fcd2c5c3084ee1cc75761e5358ac39c4eb
                d472caf4e555f8da38dba8ef862c92eacddec9c270b5c71274c
                15fc38674bebabdc7cae2444dec1e7977679578f051fe3ee9d7
                a188565d5fce8fbcb842b28a4d38d77eb37dac58099664fd1b8
                069ceef1e06ba95a39bf48f7098a9bff84f6f2df86643db5345
                5be4bfa4848d93caa1fc1398ac240d186bb3334bb5381c9d089
                ae3c8637deedeaa576e6b92cc7b66bd3a31f3c956b4aeb4eb68
                8b249cf9b57a56d3656b5374f806b02875562ea15fcb619395e
                c913026dbe5a6d488cf907745cc65dbc9274ccb5e2461b9e923
                862a67744c8b8ff19dda1068fe408859f89b5b8550ed08956ce
                2b5c9a617e7ef6022772a58b63bbdbf5eb057c4bdf30083bc5d
                e8a22628fd845bc6ebcfe27277d1d7f57ceeb7beb07a20ca446
                fc65a372929920792d2c46afe34be5a052ab43db9e0b3c2d024
                cb720e42bd20db4a53e5bb32a1356989b1d5850611918549e9f
                57001c9488b8eb12a36e85595ca45934fea1d601b42c67078a4
                fbe701496e443b49fc8822fad0c8fc3a25b3910a5158b380aa6
```

```
                78cda329e2cedaec1c4a32e51b4baf7091efa5edd6ae2aec450
                e15cfec1ced9a1d158c9f8f19e21155e4163eaecf7f01d16ba4
                95fde48f39645a44d3733ea265cff5d4f2129e3c83a6ca33a62
                23f855a91ad49776d64ecfae6878668efeeac930ab6fe918337
                0c61727b4049a1dff8579947bf16ad1c0e210524c4f5ae7548f
                3d3e532e694abed9303ff260178505542141ca980de12090eec
                01da3399e8e454934bb15759d348404d647bb2a409b9d8a9560
                21bdb85ddba1978593aa56d961ede3a707e7b0bb6f325229ce7
                54c702d9ebc35a2663c0ceec6b3d04ebd91a63854736ef4b601
                495c26aa4927b9ccbae3adc808b32571ff32288d46c2967a96b
                53e756027d5eafed7dc8d7d5337f98309ffd1a300eba2c02221
                a3f100b68cb066861fbcb39252ac446c3ed3a9639708fd866e9
                fc0bfe4a7aec198696aa13979287dcf1fdcd143a44a78cc6006
                beba2e1ae70e8e857764d233e54830473fbbd2b173a34c16c20
                32d004fe19d35d8a5277824260f32ae501e24592916ea46ec14
                a9bc301fd0c900e33a1b24cd153a25afaa34ee26cbc9215fc6f
                a18972714aab79b72939b9f4d3190b9bd64282c0e630b6d8c67
                55d291e33dc3cf6b6a740b565b1cc292f2cef3b8cc6a6f13a3c
                7b06525e4e7897f63c82502f7fd77bae5a80a63c7436fdc8387
                787ee34a000ac1512c5bb3820dc6a9b49ecb1b04fb2b34113e7
                5b7e22b6b8058859d0d2a505af21b5fbbf10eff906dde67
   shared_secret = 83ec9c8227c5306cb0e60bdf12678a5de9e24fe51855290a
                   64f49e9795415661

   seed = 0909090909090909090909090909090909090909090909090909090
          9090909
   randomness = 6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d
                6d6d6d6d6d6d6d6d6d6d6d6d6d6d
   encapsulation_key = 460393d6222435d92a68eb6b2384ae414ba04199ac14
                       e561f6711facf87180a4af6156a5cf589c8ec7983054
                       764231646f07c57ae4247de37bb73758a60b4d333498
                       5238563005ab337c6075b81416c241fce764505acd0f
                       e7b0fbb859e4172390e670089414107549ed298bca65
                       8a229079866b8b960a7c7fe46cc47a1773010f106b6f
                       5cc9c2f906465851a7716649b6a67ff073807cfc7be4
                       cac44cd1af6a372cb04161d4d39861780c6f62051dfc
                       c39c143dcbe49bbf5b58a8769b927173e4c7096c9131
                       0a91484cc80c55217b76124d0db0965f84bef016040c
                       f19947d61e05a14f322bbd918392f5083be540a122a3
                       b1d7bc7c49a868f6384dd5259850d427166752bf286a
                       3ae729e3a5a5e76209de5b9c0783a4c70504a338af3d
                       178ebd114b7ef700cc17919b258682d21a1244a002fb
                       ca209a80cb2a94e4476aaeb7cd002929ef999095c893
                       624667ae2bc8712b20e35815599196de478f674b50e2
                       8313d7695ce2ba3dc02594171a1ba7a095a4351a0f33
                       06f51b4c09ccafea587693a9519f4b4976260445421a
                       865a400a63b0a03a8d9a35ce3335bec1912460e1a5b4
```

```
                        685f8fb039a5cb444ca21f87c522c7e6554f29007c05
                        62e5f02eee849f29d39bc15b58ff58b252581adbb17a
                        42f2357ce62746b1347a4123d02aa5c3974eed863eb4
                        f309c5b265d038aa6f994e8de94da384321fc65bda70
                        4a15216451465f9d44b7e8a9b7e6d356e8a399e7eb39
                        d0b46d85ec0cc93c56a6d570c9a8865aa6c74f358ff1
                        c03b80042567796c41f418747126bb4ac29d738372fc
                        a1a9646ad6e7901581c6845c91c3989058a82bd80117
                        e7c73bd2da15cff522fbf599fa6840317608e410b52b
                        4c477827877ff612cf89cf6c87c8a72b175b6c8627e0
                        a10b937cc672c1af54b64328c733c22585b88c54d30c
                        1a22bfb6a2559b178db7a0aab6001ddac9250416ae5c
                        11c0a5a26a09d38518b28f8e3a7f2eb51e0d679f1d92
                        8b77e103f4fa6218f68a1de0af5ea0bd1a26bb624879
                        ab47a28e9c40042b29cbd678f7ab65353807d41993bf
                        e11607313430e5aa8c27b9af3a5f10531aecb1a1c371
                        0f2b992c99b604f7b2a3269a49091a3a56dc8b78487a
                        d9ac24e36c97d351855ee1715083a3e9c32f52f735a7
                        6cb008714fa83bc70e4caab72c485ac8431cc97cfba7
                        27fcc0af9c542d7d9199bc4b50a9ba83db77c7dc206f
                        da0547e2795a8dc36fd1b33d2ddab089d95eb16b15da
                        94a74ed8b7e8daadf8180721e0a1e31002497c83ce17
                        47fbe78cac291ffd967f23f47a8a30485aa352cfd4c6
                        907cb8b201bc3b9281eb51985e11cbb4b5250ef7ca13
                        c70674f395c52b177541b57b3aac77e382d5bc6e0c32
                        aade73c74a163c0f43a59c616d76393f39166de8318f
                        ef1b2c47075c19885ecea7b4acc674d1c72a2e4ca70d
                        28325f12cc33ac19aa9c5e5ab31c7ac6933c1a0a7906
                        5fa1e0237cd90a13c7b759980262378d4a17b85c184f
                        84761e071a973784b1c30a9358b76a7af10727f36960
                        f21c6e078d33fb528373a436fb237f87317b81c04926
                        245982aea0b39c24a67effe65a91b211ad7334f8e485
                        8a3b7d0ef21b3e443c0cb64e089408006b103f3841ca
                        b70b046b98e2c8aed94ad683208e265424b077389c2a
                        c6571f216fac52e35cd280e51aaf66328162012edaa8
                        8f37a3f6e9c0c89861d6df5d8a3a453cca19d8746cdb
                        ee424f00c338
   decapsulation_key = 0909090909090909090909090909090909090909090909
                        0909090909090909090909
   decapsulation_key_pq = e4c190b41d18fe33b5710819eb4a962a2a6af9cd2
                           663d9766a4896481dcfc8b89687089a9797cf2f69
                           d058df1f690441dbccf3faa91ead65b8d4dfadd6a
                           a4912
   decapsulation_key_t = 00ee28df5d8544c9ea9a79badcf995f43af90ef255
                          b64b6ca0c8d194528f7152
   ciphertext = a857a7425c6077dafaef133c62869e523a4b41110cededea6ee
                66b9a6bba634d92cb41d5fbef2ccd6f5f057951fe1b44e224cd
                2314c9ffcdf4c358979d6d065f1f12a51033640c07965e6d434
```

```
                2afd7b57d528786b398e13b6eca581b96fe77778d73bfa2422e
                43093f7c96434103b18cbdf0aa6549da8e169b66f42921b89ac
                8267de35446008948d6026a0bcbe61357e97c7fe7a95337dfa3
                177ca6167c3a2af8dc38e3d708665824acf97d6d7b152bff781
                451c587a282adce031b3efa26b6d8bf4b49733c03dcc4300076
                049e278d3cd872174bc374d77038c75203ba45d30bd4110b623
                46c3f0bb1d8563d0e2d58cac839fa693ca96a56eeab1aa4d26c
                c95e013674eec4f8f08095059f081a0d4dfc0735653f3097f1a
                37da334007082ba6619844547e0d3296669eeceb02ecbf0c5c5
                a88d5d1c432398361529e0d91a628e568cd9a18cb3e8ca41315
                ccbd8ff9cbbc0677150f2e06274ec9e2733f3111cd4f1b900c7
                a3a80b517a7d6917fd0753f59e8bf03267e3a43d60e1857d492
                2cd0f14b6d28602792dbfe2b4488e807023ff4a8b65f75fe1a0
                826d5ff490bac7be071b9545f6e7ee758caf460e7e92e52eb83
                dcafb5bedeecf44a5f5ef23690bd83aa5ed2ce0420c697dfe4e
                aeff5d64be78fd3d9c96f66fcfbe015d8a1e75e93eed734c267
                fa515220e9937fdf8df271f69c8e3d6dec76152404d86243421
                1bd1e4b53cb9951c48b796fbf4287d3386c65217b41f2c414da
                ada2023c43c08f8b6edbecc7f750968c4f16c3c983a95d73c25
                d3cd4aac5bd5941fa376e1934436acecf9bb9bd4409d0944d39
                3d852aa15d6363bbd83cc24b1ea841e00b99dbe9f7b9fc2a415
                063865b43ecc9db0a95336820d40ec4d7325d5066eeb2a144ed
                3c27f5072c9a2e596d395bd069fdb8871521a08d0e9c1810467
                a271b4067a54d9d81eca8f26d18acb41a7de599aab1f79ddd01
                28c07e44cf2ccef72368cb4474db47ef43917940a80d05aea5e
                8c933a0ef8a8516a6dc2a50df273288d97a9788629f001e4874
                34e6a4192466e63f0e185810665267a021896967d833c1f1086
                45a5d17334d5dde8fd617c786665d7df9762b8ec0676af697dc
                a63e62b597aa2cf89c558accc872ce9a1277f88c5ac160b2d13
                a27de6b4027353adc3bf596d3d6527532e66225fa53e2546f6c
                eb240435bb93d10e4677208e990f622276d04ab8f2e4ce2e518
                0a436d33adbf29c2cef8704a41074ed16c164ffcd1c8f09a2f7
                52c098caab09da3db75d84ca510542c3adea1757a553bf53657
                f03feec803950747c8ddceeb31bd658072f01b7972df731af5f
                f53bf8a8361cc918c6a00693134fe6e385cc70484d2e3e6d365
                c14fbe6e2332eaf86b7afb8da619dd4c13e86f62ed63da3b998
                95d6ee47b440e16a3615f341d4be41239336b02017481968173
                2503f275bf8bc494c251e5448ff32bffb3fe0787482b796c37f
                d8d25a28ea78620046b192ce46fa4c798c0feed181961441332
                6eb373e622834afeaff81aff308caaf835635de5eb039fc126a
                017b9e789e1db721cdd51f7ed3f5515d18e2f4e2dd7851a
   shared_secret = d1b5f13316ff420d4ca22c9a8e3f93d27f735d1da53ebc97
                   9cce23f9747e3261
```

A.3. MLKEM1024-P384

```
   seed = 0000000000000000000000000000000000000000000000000000000
          0000000
   randomness = 6464646464646464646464646464646464646464646464646
                4646464646464646464646464646464646464646464646464
                6464646464646464646464646464646464646464646464646
                4646464
   encapsulation_key = a10bc8b554cd51980cdbbccc3041420fd320fe8b74c7
                       a84278c63c17070dc231b61ab269b9d677d920261186
                       654b4571f51797d5c342b8070bc6c92bca16adecc631
                       e4e94c7508b111730c749c73e2d6a6f97155cb269ccc
                       06a71a21bef3d269463c935048a7f4636c7b32007370
                       9023f7b04d0530571a9a6f718280870bb63875d3f599
                       bc229b95869cd5bb5d26640856d40b828198fdf2c099
                       998ffdf772e462336c521cd326b5e4997bd95c135c57
                       bd02c7afa80a2923d510951778ee5125b2aa18f90445
                       453b85789224725b259279698ac9426c882baabc38d4
                       fb3a3f6831180918b9825e0e418154d78aebab5e7e70
                       66e69b2567476bf1177fe079a38298be6f01b098c338
                       51ab25312b52e32a5750c2b73d293c0b810473b310aa
                       f062f19914c7377b2e90388f575bf5e6853453b95a74
                       aa18d62d4ae37e6996a48ab5217488a92d7b01e315c5
                       0b68204143792afc4f8367c0ce065ab32014bdb5515f
                       e0594608aad1218994724afaaaa2df0355f46666b6e0
                       2a387b6d3da4713edb610bb048c3a2078b800e9ea483
                       f2009c96d24c71b2cbc8e1200c0277383c5c27895e29
                       8c3607701ce58702a91903274a041408234cb0021ef2
                       b1c5131419b444dc84b89d147d1fe43c43f676d90673
                       5d9ca2a59c2232d97fd4aa1ae2bb3d1b170ca553cb25
                       74954fdc6689fac623cbaa31982d82424d5a564fef7a
                       8ba51b44df15053b2b45bec4aa1ed49929123daf7541
                       75c5938258c608b24d062042ab4bbee5e553a5ea6275
                       21738ae5ab2e06bd98b020787b2f5fa51eb4c46c2bf9
                       0e55a49560340667f88ac41432b7f551dfd98c037c79
                       f79b41b985a8b1f51345550cd816714362040778c43e
                       378a288394bd028c8c31b5a904bc4a5648a596035cb3
                       8f0e276e12c9a96f8425056b05a136642dd2cb754630
                       36485ba1a50539e420e1e31dfac529cad6c68ec06746
                       749473e050a4ac92b7199beceb239b6c12c8e716b666
                       07aeca64a5850b01f99d0b176a7759781ed77cb1ba40
                       d17ac5c6cb06c942c002c2cf6efcb121f10ad2a45ff7
                       81426e7104cbdca73b81865ab22b00ba834355ae485a
                       262f354248932c2be178369a3dd7e2428fdc379346ab
                       2b754c43db657460cb09c5c48b5810cb7a5c6156cf87
                       440c9e36a4869a8ac458b382fc178915a9ce1bcdda7c
                       48807c207e656ffb80bf33e32bc8c7b20ef60572612c
                       eac99ad1c56ce5a764b29b74c17a5b510b1afcb18a1a
                       fc35c12ac213725325f9b7a2eb338fe4c0080c31a58a
                       995db7027d900e78544887f90ada467d0e383c119c53
```

```
                      99310bc6735874e8804ff6c2bae57f2c3357cb627033
                      c12a5924b20ce5abf113172bd2b77086cac543811793
                      bba71734c9f005ac2656460bc30a442b388725758a62
                      3e37ba6e293abfb84f344229f373c214ca776a7c05ad
                      c465fed93b9cf77f0022ab71f1adde369dd8f420a58c
                      057c14cc18dc47da7c12b086473eab419652967001c4
                      e42a381c8ba539a875d21a9945133bab9bc1e53a600d
                      e77cbfb2aeab6b19ced4c6eaa8998ee6a1577255f713
                      2d80a32d6c0c6ec44c9c4b28699a645bb0bc958e0027
                      5077925309519b0824c7000dfa61912ec049063a067d
                      00b059053e508a5bfee63473869c8a8510af898cd757
                      2854f5c38af96f5f97a7372632ea7bb4b6fb831c612a
                      f71191ff9806b379bcd43c6059b7b1f953741444af71
                      3c155d962722b947aa23a32a89b356a6a7508aad6396
                      8c1dea78ff18aac27a89aa7b42b0d7481dd3cc649421
                      e51397782218ac5441760ba51a0328d66b436fec32d7
                      aa4d68e0cad1bc14f7241c903480f809983fc2c30d93
                      138cf63b59bc737ac08192893d039187a811bef3d320
                      9eb7b8d1e05b5b251cef760a210b2732867ab32049ba
                      3c354e3858aee7b71df792924730d8e842e484122b50
                      677b0a306e61cf21b62091da18b937192936a09e5a41
                      8cf78b666157dd477af1c36a12320129522840e37094
                      1157808782a5335b0ac10d70e1beafd401074b84b982
                      6cc58aad217bae0f419b2da896133272d8f22c6f420f
                      cc738fccc1082fc93c7df0994c6bcf2cc8a29037b6bb
                      2b4bcef4b0ee8caf8506bc5ecba082a56806c1cede0b
                      944338a69a668254c1150ae05030e256b2b67661ba02
                      7d97576da613ac8c7c29051f1240b96b0c127e264d5e
                      1dbbfe9561a567d5c9103673b446b3ccea6c5f7f34f0
                      9348a5d4a58b0498871dc940ee97b50c0336f9a60c32
                      99f99560ac70657a27befa702265ce590583e04a2832
                      6092d3dea2118dd1df5e81d7d3014ec4b5ce67dcb45e
                      f001769dd5d5ada76934d38d740924712bfae672169d
                      8f8744c151346d285fbb653f83aa0f
   decapsulation_key = 0000000000000000000000000000000000000000000000000
                      00000000000000000000
   decapsulation_key_pq = f5977c8283546a63723bc31d2619124f11db46586
                          43336741df81757d5ad3062221e124311ec7f7181
                          568de7938df805d894f5fded465001a04e260a494
                          82cf5
   decapsulation_key_t = e00b3f9d338de90488973787b0916a4a9ae8bebf4e
                         2bc07a7bc18f1a6221518238c5c4b1760c4ea8a9e4
                         7beb174f12d2
   ciphertext = dc63d18bb9715fb6e3ba71cb439fcd3377a75305cc9b144e675
                8bf5794a272e6b4a0da33234c0ac1bb5b4e60e4c82eb1fb780d
                59e4e4616641a0595ba031e3ae69d971dcd5fff14e21731a8e1
                a221f46c7820d214630b707fa1b0de3a484698f3d49e0a75f12
                12b8c42d330dd909f15eac0402f19ee77fba9447e1c44304b0d
```

```
8c371c17c5549fdbdec1e0a2e7be9f577d7a4b5b2618d9ba67a
b95a0297cd5c5a13c89cc5a57cbd9a8ae38d66455c9a3d2bc55
b498775fee2f6dc224d376d5f526a8354c8ed724f60337e900b
85627972383e1fd987d407a8834005814a4fdc94c947e5f3471
459288cfb127952b3208f10c914200bbaac5fcebd2bc9e28484
92bab17b9288ca8b81d1c2ac9522dcc0b6d5f51e10f3afbb5d6
5fbf919edef6323c4e92c6b0690c10db25a9182de9e919ea1b3
e65ae6150635d5180ebd7d23a2264828bc3ee1fd34dba1924ad
0db30c747e05baa9148f1a032769c685e04665fd802a79c4624
f69a9198a426eac1b217d903cdacf8844e73365f3a219a700dd
a27edf6bea33602617c5fd105b301b884bfaaa1163b791ec09f
82523fef65c87b75ed063ceb127729b82c8712e1f41b547d095
f55ee71f3f8b47a306cb5d9bdd817854c74a42eebf934a1136d
ea3fbc546ad8ce51b3171913722f08b0261d197590342bfe410
8dcb08c62a98610cbfb8d3b2831f56dcac2220e29a5811f38f0
824f21a6cbebc64fd89a09b110dffbe03799ffc74fe565c80db
f6a66acd7bfd14cb90acba03405a7982d4c1c68caa75f8b72e4
dd6401d7dce4db4f6b820a7886a604b66b4e5b9eea5e5eddc2b
ca458a25977bd1f02874c5d9daf2baf56b3040f24ce7fe14cc1
4d61c7960db4decb37d9779c8e36d69a7763066d8c1149312d2
6887a693dc222daa892dd00cd8f3a558cf605e4c65c011c2e9f
0d671ba10af2bb90ee0351ae5078eb7878399ec9eb4ace87a68
269618bda12a7aed6fda0385496c5d10ac36b35255f4a31edfa
8a2c516b65c63431013ed4909ec7a787a5efb9d3c3887b80ac1
8a44934b6559bd8a84b18e86fa1b0b9e1d9f92ba495ba5595d8
2e5095612b79e805154bf428a7071662c7cefb6450165c6f8f6
954c37219bff4a49894a8aa37f940a40f4ec942c281e6c47ea4
08199927a724ff1c7460fc8fd47a98d0c9d4d1f07994d8084f6
e084935ad7c2985282fabd5ca13b942e10d35278f4ff4cb1cb9
6f3c862410e79144a46b4db1a3c3d4d63018ec5c01ca48cb670
81482e7d434b4abe5fa3071f2fbb533f745602b0da6183b28e6
c5dfa42dab7ae0bbbf7638e106be1bd7312cba399e08c96dbd6
9a128a2face2d4a02951533a25e82fe63d0aaaa2e8c75150215
c93ab06c22f9cab8d1cae7424f8baa09b3260ecfa3c7c8d55a2
76b4b317f72ec86b1b145a63aca83ef8c1204d8ab0c96ea3f74
2de39db47020616e139285814f188029ace4587f14cf12b5ed8
1086d8213cf8cb578341e04e16f519b77ff4c2644a5732639d6
58d0c4eaf992bd7dbd5011b700a5fa63dc1b24a84a3c80656ba
b5705dc3a74312c80e8bdb24a7ac6e27bcb8c07ece62c6e5777
dd3dc0657181f440c7524d907dd27950bcb252aef7f8cbf453c
ee3fe3143a665072c787cea76de323aa41537df2f3a40a518a6
94b918953bde8d57084e32d3b1fdcf9d153e73f02624beaf6eb
e23e6828a6a489583494f3cd790fc96bb6f5d8b198402965e2e
668e6581e7cf1c8a47a92198388f2b4cd38df660f0ddd48ad12
6819c4435af3a12c89113d778ac544fd8079cb8aaa97d2ff1b6
08da574c4dcd87f4979390de3be405f0e47788dd0b016628050
79fd73c64e9278c036544add3694c838bfcfb08c8a5efb09549
442123eaa59fa30fbb9198105f6be00163bac076193f6721c53
```

```
                9714108bbfae167f5db8085c5838618f32a968bbb25c40645a1
                7c17b9bec64aea45832eec5adc25b53e677f67566fbf5ce2d91
                93a06bd9b477e601d589b25f422defc49105252cd9ca6adcbb3
                6be8a01a8472b4d463f655be14ccff9b0571a2048e31c14b9b2
                3e2d43fafa3f85ece6fd41896cc5c68993dbaa926f285ec94c7
                2887de9564881d735c05f83aa474b3d4cd133a630ac63850771
                cb5270f6cb7a391170d66af3e4901b6eb0253f3f34ef57d6bab
                d97aa99ce718c3bcb53ff13d4028a0c943bb9681106ce176242
                cccb75df1d3f8d3706e5b068b042c3154d5e6292581b36499e6
                b069b9a490aa67f0675390539da8555e6a4e8a35a86fdfea83e
                1387bf4acc650ec1edae7c99aa3a48306ee1d1a5e513c0c6901
                f64d0a3ee285de3c11d49f90cd4323dafda14832f0d8b760c0e
                5a48633c967cfaf
   shared_secret = 8c028c6ea72a1c59408e2b15dd8fed8008517e861cd2329b
                   159bda1919ea656c

   seed = 0101010101010101010101010101010101010101010101010101010101010101
          1010101
   randomness = 6565656565656565656565656565656565656565656565656565656565
                5656565656565656565656565656565656565656565656565656565656
                6565656565656565656565656565656565656565656565656565656565
                5656565
   encapsulation_key = 6a0684b22b798e76a4407b87f6b7540d7ab75460692a
                       8a91070456ed6457281542abb01adcac98daf4a62f3a
                       81dc7962b6a23cc6624d96cacf0e5c8894651ec68067
                       92f1c9b457211567515a65a184fcb27c86bef2b21523
                       7c119c9b29d205c0a4171b70c34da35427547497f827
                       c8642031964b10b12aafa6c0278d9917cbb39e3c7b20
                       151c167331764b447ea7097131fb4f36814d16290c3c
                       ac0759381747b4a5a8fbc170f8afb865c2962339988a
                       cad6a17cfe12aa7102aae24124537b1042c979cbd1a0
                       3e8a15261bb9476100360a2588e19ad3dc6f124b6567
                       c25dc00ac4a4f515a23086b5035625a88458e121ed80
                       5143b8bccd95b08295bfedc2bcbe947f755272852311
                       09c7a197ab406f6c8b5e927572a766f5d2b6a83816af
                       b0513e81a02049a166778774714b7d121c6fb6461891
                       02923683b68abdb2fa11bed51a5dc30f0df593fe4a45
                       9ab2aa8eec26d69525b790001b820545656b0517989c
                       5243f6e313c08720b9052c624b9cf382b92341ab3cd3
                       1007d68353077df88126e3762e8478359778bb3d1416
                       3098c5dd35b9b9d87c5e6874004d126ddc8839f48cfb
                       6a717737010ab66188c24314fb0104c6c14895a42b33
                       781afc01f84214897c7f7ea48662f18e1050513d91c8
                       3337c10db5cc7cfb78d86b615d5b1c74062cfb5162cf
                       d2499e31a6e3e8cadc6cc2066215fb78a1b986a1be20
                       86c73a5142a35923b61f76a1b669f2690d3857c3d903
                       d9a6647d9b2d3f545703075f7b3021225c7daab74b4e
                       327496a9ac8088418de6ad08ba4b3a57967c6c4963b8
```

7ec1012f1356051537ceaef13956dc134dcab19729c3
fada994aa706c4832ce47b0479b51c13995eb6d895a7
045df0d8b696f3a8a529a1abf8bd66e91e6af46d7473
07cadb76e7191d2ca90c8519394d3c41524089247258
014bbf1a1b8add2709f50480d5d08b4d9a64688321c6
cacc03115d30e09d016a1704db4689545b3802a07f4b
3fa82142bbe8940c7ac15f19c3ee20bdfac11bfe8b26
495107a88b9eb911228a2c83cde5b0fb82725d4808ea
5a903ba2b9698a2dad9b55ebf6199f396ee19ac2998c
7f5f1b9f67e4a82fb396d7b0a4bba7343dbcacffc3b1
13c44d6d033781f289a3cb8255d8bed93b0194b95024
549614f45622e134dcfb6df598061048796649330bf8
ce4ed35097f68503e1b1d8c2a2ad43af99d830af606a
c2b013cec9367a9a6b5861a6ed618b3e6291743866cf
8661db45cfb9b168dc0acabf1945cd698ef2d11cc9f1
548bf48eed6bc301a233098b0cfec71cb479630f2aa6
567c8b2a10717ce985bd21c9b6823519c01a40f82436
ac734e4b8e15e28590ea212e992fa46438fd373cfeb8
3071c1549171c76fc80dcb17310de56eaa6240430726
32b14ab9636c37fca0f283742d0c8a7634b4c7f65cce
b1204b6ac55cdb5fd508b37db8182cdb9cd5e705f4ba
a5ae85a78c013e2e7c168f2193bee3c81c95c446741b
b730611963a01b1c385f7054dee45ffa75bb7cd12f41
b25cd09ca575a09928c4bec4b61f67447ff5f38dfbd2
044febbf8b83760bc91f5ef2247cd63ce25a7459247e
8165b848010c237967f94b11e021237ca414ec023817
1a4259a581323b3d6f091620b164725144d6b326afd7
48f3665482748d92315628339300353c370259fe86ae
62931d94e2136a8a8fe5664324d3a3cfc5acd6d00ac8
b72d67377bbfe1899dbac69004a0c2b9ab047a0150f9
03400b6d3f009a0a6a7ff388ce1ee43d9ab6314d720b
770175d3402bb7ca39690aad41904cfb54a951c64ece
057d9a6b610088630b826b682990962ab9d09a5fd153
3044fc131015511932192ecbac76711e28743c921aad
59dbb3d4978bc3147e859c40bc98bdc8680962536f15
90207ec9a7dbf795a2d48468d3abe638c7c494241dd4
a3994c2b62c65593756151e6a98ba50b7165c9e5146d
b36285a736383f391f8027092044791801l064c78d4e
738d20eb54f0e45551946e79281052ab6141ecb67834
a55a27082b303facc4bdc9ec7733d7c5c8625a8eb4cc
444501dc2180f5eb4ffd84b9f97960a1396af06c9142
9a9b92c4a54d12994364cf770a0a5ff4480738890b01
98d813813664af9708a21b435ed6bb883dc2682fcc59
28458a22101ddb594a616c34ab8322573226cc9b498a
40808330885f206b72049a068b70202d8d71fdb3cb17
7d4670d5a5fe04584e2dc615b45facdbf7dbd82ae961
faeec8274218f2e9f4a20d6aa9c78a7894b7d83ff770
d2a87504d5be54954b03ed4236c6d1485236fcbae4af

```
                    881600bb618ab00c7f20c27a3a2767d729980e360731
                    3e83cdc11aa972d4e74b4c00c2ffb9
   decapsulation_key = 0101010101010101010101010101010101010101010101
                    0101010101010101010101
   decapsulation_key_pq = dbf77c8d79c80ad6b0763d42a3fe53f0f1dc03022
                     0c2e3fedc2aa903abfcad08330db4ba490ccee095
                     988d9355e816055cf986e280532d47cc19f2240cc
                     23419
   decapsulation_key_t = a20315485f73a3c17e18a3f155ac33e9a980896b2f
                      17dc7f96a9495d9584056074085b1a8590442290fc
                      46b4705d732c
   ciphertext = b7ef5cf25fce247ee4a1ac8a0b6bfcb31ff4060ee7082c25789
                7829268f59afa7c973e233c666ede6754fe326d01dc87097972
                32a833a1353d651250437d21d5a97cd761a335683830b1e7167
                cd6ac96c812614f32cdbb6495c807f921486066c270b560a794
                70ff198b5c10fd5ec63b9fcb3199f3aa410688883513e47c3ad
                9020ee303dca0c2adfd980fbda3f7abdcb7b1c38d9df943bf12
                bbc2c3aa2dbb856fcb9c30aebd64f2925aada5a3b25efeb10dc
                7a2423d60b277730d5f3800bc8ddeb252c6824b9b805f4de372
                9f0306a38854d8f9a63535c3cfa0479937a5dfa59a3273dd357
                276d8dd4d48d23c32e316952e4c877a4a72dac1e9815f0e589c
                a62721165633433ef333b842c09b178c417b748d8cb2c5ad56e
                e3b3f1bddd7da8b263a17fe759e25c50c257689039af122233b
                c0828f0a6b380bc959ad3077998703e530b13b249b91f7d1547
                682cbb1425b6084bafeddf3009653ad1fe547c4828859fe7b06
                0a4e8c29932919e7f06de1c5101fb26bbc899a37a9239183d05
                859ef00bc9a6a3832129551c16bc75fb750447f20a38f12010d
                1d1c9ed462f593408fab42a6ce07bc8ab6e7df262649431fe85
                ff80d3027a862d140d75c9ea16f73eb8f38052a535fa72b370b
                19802c8a4d75a0e59766c81c60e582125522f15aa3f2e187d55
                cd2a0ebd8982ff5c671b95ccab54ac3cc544f6b07c6dbf58293
                502c27ec25ebcd9a44e2adba24a220dfe5ff3fa92ba509b2f43
                63facaa29ad7f9ee279f9a112f5307ff98cb1be7a237f56a97a
                c74343e5b5f6ac04676b560fbd5ac7e633e1b2b64d63586b13c
                735e7073855442002c0ea27d8bfd9b5e5147a62ac903efa1876
                e1a026abf31c3aec9b01d58c38c8c4dc5742bac200ba347f3da
                2e5bac62b213fe93f500a7a4340ff9f468519aca36b1bbd44c9
                ae4eed93d4daa1c847fdc072145939ff3473623250aab470703
                1c24efedd9e14680fd9a017729d8db87a132bfbce8fb4a524c2
                e32d469bcbad71ced78fb80c1cd9232b60c2836f019330a3f6d
                eab21832f60faa346fd7b251768905b538d883cd23b0c2a7c28
                3d33e083148ea24064e3b689f922e7f5ca7ca4da9bb8412bd79
                09f31e0f2963f958eb1431262a522f79d86c748460df92272dd
                dc45bea7cc9cb78c35079baa70c3ca12720109bc514efb3dbf3
                b60fed6c49824535f50ce417475e0efbd7599d9071cbddc9479
                0ee5251c685fe5abaf4f05f11413cda68af6e435f944eb69ad7
                8ffc67ed25fdcca7e4378e9c282cbfb4779c9230276d487496a
                b7e064ec3d2acf6daa062616fa21cab9ae9b1c69de3d986f491
```

```
                25d9316bc38695a27e406842e9304b5863135e8b93b2b656e22
                92e6995ac80b404f6fb5b4afecbb3c2d07c43c1c3f031ca1be3
                52f2c5d6ab020f7a3d97f8fc4e74a0877fb5a01898eff75583a
                c512f23067b9d9235a6fe9251f8581f68ceeaad4fd2e649e887
                b8d6ffd6a76f79f12408928c78a8eaa870a0e213a1598a5eb00
                9d36eb0500950d6a32457c7d8c2e1605d755eb48959324bc0c9
                abb103f09a0907188bfe949afdb079ee5b30caed68bfa901b31
                531b78584727783e9593c20cb937ae6a19503ac2877f7225ee0
                7289170d7700dccd64f4e5cc1846405b327dc7cae6731064a11
                78fbb178fc4e36ce169ac7df5d981081256e03b5987dea146cd
                f8dda5618fa7f956f5c3ee7eeb530b84407ce251ef012f1a942
                7d3679233995845ec09dc6c998fb73d123d87c07ca68453458a
                e7131992ae1151adeaac646d85d1c58ee99dc4853ce1305733b
                d4b903b1f18d2071f101957338b4de94f9ff27618873ecc05a3
                52a1ead8d63e484911465f79512042e9d9182e667ac055077de
                3ea66abe4c71f635d6b1f37f43ae1801ce8764cfb9342b1f0f1
                358b68f2ea0a9ac93996bb93c1b6e9776fc9dc95351c40b05d5
                c1e69568d93eb85b0ea0a4cfa2d90065ecaf7f472e44f14e15e
                04d1cb17da07bfa76b1eb2ecbc054298e5dd6c5be7771e2e56a
                8d8212d5f8381e7357255e1a669c32009ce129622fc19b18f93
                f06f407384045713ea5ab64e7c55e204095c57bb1e8075004e9
                ebdd2e63e1a4bd94134b7d1d1fa08e1de070682ad8894edf639
                578b70804e4ca3ed6f4dd22d570fa42dc3534fb3498609f5f5b
                8e77115bcd295657f9c48f3aa96cffe6412e6c969fbc49332c2
                a8d8ec5d6e2c3596d878a361104025f5f77f84dc9ca38e6037a
                bc429c6f69d3a237ea0e396e4f659e41068f4a08e4fafa287f1
                7bbccc8b357b6e49ed038b5bf39d7b22836f0309969ef69f189
                8cca11479f4db4ce2eaa3e7987dd35516c0b8f3157886e5732c
                d865f794a2a29ed
   shared_secret = b258b8edf4851b7c1a86cc820743811c52d4bff678e8b94c
                   f6bb5f3714b7dbd6

   seed = 0202020202020202020202020202020202020202020202020202020202020202
          2020202
   randomness = 6666666666666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666666666666
                6666666666666666666666666666666666666666666666666666666666666666
                6666666
   encapsulation_key = da2020c3757b1fd29fcc785aa999bfb9fb1ac97a1efa
                       300bd08356087ca3b8e685c00013ba18266cf1cacf42
                       879ef4cbc583a3e277328fa0385f34c179a230534061
                       fa65a280c53c5016ca2499881c1876d9635741ca65d7
                       60070b5cbf7186c3c3747453021e2e880b8ff8578cda
                       8d84bc3e600b07f7960107b8cccccc8486db30695848
                       6dd3cd24f89f2bd93f63757620ccb2d40cb5b40b8fec
                       178cab0c8339c5be3af98567e1678ef79adb21437da7
                       1d710250f166577115b290b81ea5a153130cb9b0bc46
                       7a75127af4702318c99a8944218a6df1763550eccb1e
```

e500b7ba9d8e180af6ea84f4b278385ac57a37b0cfb0
6872ab40c2f017aab9c1876004fc9b3484da407a8538
fe86754c407868d5222c069088b95f49e83f663c9551
712db139c7bc4a024b3b08fb32a5fd926109183284a2
afa6e894da8838cc24549c4029c5d099ec8a4af2a23a
6ac74ca2b07fec86a812ea7d2f7679a5f72445c347c6
dace5e7a6c95319a58055b86d4cd92863df4fa1f96c8
18dde32efcd140d0332357d442fc3a6258a242005a8d
7f279cc9074dbc0862ff553541e4671a879dc9415a89
7aa13176892a2a0e39119b8bc5159b487ea39196f090
93da51a3274087f59400a8ebbfa32481596a2b224174
89d0992059900c55c9321823ca5c1b3f17930ccb8195
60593720a417f58ac9263a74094499b74d448c9d9a96
acff9b50b765cd49ab1791d82def1c80307102ac4060
47106f3cd787c280b42f002a35920e1839b626cc29bf
922939a7bf7c4b0294368b4ef397a9015d7937ac8f79
26ec022755767a2a296506242aa5c95c712a9cba5c4f
20080083c5bdcb0bac0ffa0b726b1f4eb5991f8b36ce
582491536f0d32ab5c651c8389b2bb85a1750cad8ff8
801356266b77baab0369b6516146dc7ac0e2140fd41b
0c701b4c583d7fe01b7073422ba20662d5c22f407ae4
c61322151c5eea77d3712e6a442fb93939856062d1eb
495f402abb764db0d43999b53abf1ba582085dadf87e
1c3a6f9d11aa61016f2148ba07d4269eb543a5345198
23c73a570931533aa3bc7ab591c7f8cb20fc339f7bc8
6fd1c02fa296c610f97e93c8326273a3d1361eef7707
74c059b777a3e6fcbf3a3544bf22000bc574211ace2d
cbb3a51721fb6295d4324400ec4ff5822947d0335926
193f155b4b3aa5c07b896f9c57c957b217ebc9bce916
3893b0d759875157234c4708ece63cb905a3ea231359
7b20a93907f8144f28ba2056501288666f37f2560890
1270b5bfbff78c6f994f80854f26344c0cf49d89b45c
53b9b56951ca819a48ac5144c43855a585809ad53cb3
5087b1e783ad0b6a4d1bbc1604c86fe46d0d286ddbbc
53fb90ca779b79813220b8c224fe2317cb9740e21b14
a6ca8ea473ac1c195ccb8371cc649575f3879a3a8de3
f150f3968a0318b511a47a2df378b525731815c2ec36
84a40aa6f96484fb646befd10895a2c40056a87ebb51
257bb7e2fca1a0b8b4e6d99dbfd8625853cc455c0790
3b84fef6326b7a1b793aa482d59113e79439eb3d7c6c
4e43e5068f369761d4454244ca235200e30bcb1a92bd
d70532076bc86dec10afbb97924c8175a8b69c8b72b9
b0805a621dedf28fe73679175b44d5dc97668795d791
3ca8b8635c470be0947e60fa621fd0783d301b9577a6
da919a1a5c2417cb6d3ef71258f72107d45f79e7204c
791b9aa86af78a9ba721cb8cd29997a68ad850862b7b
acf3236ae0d290f9e861396c5bcc0b7e2cea2e2160bd
86fb3257f75a8ca1acd4e436b1dcb67c48c1a58496a0

```
                        d4b26605cfa1766a3ed264a5a3cee8c9b9990c4fe985
                        a3edbcc39df9908348120fb81285c8b19f2cc3128643
                        3bf949814221cbc15a92b12e3e059675075d31a16f0b
                        44bbd1100e87c0105354109f89312b491bb4ac9e6dac
                        c6f107282d77bee5b726e0573910cc9feaa138e7ca18
                        69b27e6c1a4e11a2a6ef9557aac75434259792556cc9
                        e077a1e4c28dc52e22b40dc4486e13a76aaff3c57bd8
                        9f5508908697bc9033623f416027b72740583400c106
                        9af8227a1233aff04a9552370facbde5f728812614b6
                        974f4612334971167388867e88151df0ad07739bd472
                        cf80ab52cc66563dd02062695bb3223ec4163aca8c3f
                        3bd3a04d43284be0c3c09065dc305741099a50578228
                        d5e480b0b4eaff53ed5c441b045d40cf107477beeb65
                        464dbb33ba8204eed3e2657e4e77785bafa23eb5ff53
                        7e3fbc747b6fff2bb8adb2fe0f4b790097f85d4da3e2
                        52de3ee068ac3c61d3eaae8585377f539b894462178f
                        399cc673b645df5193a70442206d10f8be2229770ece
                        52cf7ac559de87e38fa44e11596658
   decapsulation_key = 0202020202020202020202020202020202020202020202
                        02020202020202020202
   decapsulation_key_pq = 971619c09e6627cea855bbf7817dd36cdbf7d2de9
                           12d66aa2d94dd0da30c9ac1200fe81d6ea2b42928
                           de29420fb451103347536bb655a2bab5fbaba8a67
                           86fe9
   decapsulation_key_t = 96141896442e2dca19ab5f49cc2450f804fa3eb949
                          7f8796792741668815 96f050146a740e57b208f385
                          bd4a4544d482
   ciphertext = dc29c7e08271fe62f2ddb83c28f8d2b9c9d921679c2db284a2d
                ab0dad7dffb16c6e28261d013b872f006cbaaaf683c60ae425e
                946d0b7bfd01ed9f181af60ed1fab63327869456446ef94dcd3
                485cafbd6c4414593428a7d1c21021b2cd4c92a49422c95c669
                239d22864c60035b77811f59b0995a21ac2fdc12fdc20b660dc
                bf2b39b3c6ea082bcc463d8300b9ac620922fbd18e7f2450b90
                2067d6645d3e09a90e525ee18f3f7924365a877fe78204e2b77
                e81530f65d3c8a999da301d5ccd4acab70412cd6c79cfdc7802
                5b3bbb7637c36093bae04a1b78924280ddb6a79bd5c2e2ee30f
                73ff7ff878f028021967adda04dabd8b1b8db747e87e2144232
                bc1e1aeabb6ce697aaad4bba725b54bb4dc2b52687a60b68384
                124dcf5719e643ad63b3af8f1fb0b1d9ded7066860a7cf6a5a6
                61d7a207dea2d330d02b1cc4744234944d0ec1ddbaf83727fcf
                521ff2cf04fd0360d7460dc312cd1a78231dcdbc62a378d1e6a
                d6fd677327f3db12c904c582189213e642683e6fb40f912d035
                e145d80822bf7631bef6b2f417bc9c011f5b41260b298d8efa3
                91e777166cd9a61ca79f482244af217cf7bf600c17a2e02153d
                6185b259afa4cd98dccc80510857a27e4d76539feb08c06c98c
                ac68d81162df5b6d311da9b1193a6c65070e579adfbe15ed7ed
                1d996bf1e70ad7a3f08500c989dd7ff9d9950c43ebcd865a6f7
                6e5ded66ae606edeb48d492d44a3a9923c6c15a53db2130b2aa
```

```
                45898e80b0b2e45b986a5e47ab95b01e36d39fe0e1c3af35c88
                74a72a5154d088afde172d5dfd800443552ea614a8aca28d808
                dbc7ced4b519bce7ca0109e6d53ba8515f45d3a283c51eb6567
                748e9ebbf3fdb90d860ab9a062d941641d17a4051752e5b94cd
                20a04cd737e02a5e240e668f9a20ec8be368197255e265b3c47
                da59607a4f0ff49dec1db4c805fd78315d07cce287de286f757
                4319afdb00e806e4f1b30b56bcbfe2c86c495431edf3176b654
                98ce8b7a5b2bd2568cd9003686048ec8940cea9b73eee194d39
                4408510baf0fa576be1058a6ac74ed2de2015d0a6757052dbc5
                5ce385acc31e266e165f56f68a9019896e4b78a1d8e1c36d3a7
                a3c3a9f239a60d987113af9a76ce960e9e2e9855142cbb88168
                1e0f2944f7550b27efcaf2f165eb4138f06143f59a2f9dec289
                b68a164e68b4a911e8b2ac96f532287a01a37a21768dcc450ce
                25b4c0460a162989b150d87538652b645d4c17e625eb949138f
                26ff01f19f8b83bad74b4e66c82291619022129bae11e53812a
                759a41d7e4fc922dd776a67919cd40ca26bf908996b36750006
                e528033b85a663bc7a717b027e8b17f761d6fdf6a4c7dea2cde
                ef9e72de0108a5608343f12076ff0ae0c5dde2ede197c0f72b4
                732f5599ba11ccff6e16768e3bbb661ea4ad0cc2c69a725f80c
                c820fb94bdc9dc9c61ce1a955559d5427d6c0b354cd3a83f3cf
                dc4e7d1f01a4d5ef1ff54239e5d9d8e6384c5516290797d5641
                fb290b2065be0426c7a05898df9dfd3fccc0841a96cef6d312e
                f36ca01bd9be5dee8b9dc95637789b1e7ca05b51bec1e8e17aa
                f198e2b8eec015e921b820da20126926b460a3cefad98d6111e
                5bb9143328eb270d38bbcbd430a7a6f3235333684a77e040bd2
                a3a27aa350cfdcb34edd48fea62bfc6152527300b9447c67340
                ad97dc43c1fccdc6812e45ac28b379ecbe8c06da3b6d3546e4a
                cfccc0faf26cb3240eecef89690f0f884739b880c3a3940a0cd
                c5fedcfb5bc7044bdb7d8502a5dd6f6ab3e029c8141209b5f9e
                196261921d5be6f79544fa7361651039f2a97fad392392932b5
                7259ebd740a7100c959901d587da7df9f6961052cfabfe55a12
                746a5dea3be2c120b25a1a50a2177d7cb4c81be846c7c67f221
                4f85ae223271e83747aecd899e7efe8ed67aca9936df81bcb56
                02e0eea600dafcde932b0d6da9e96d4021a4be612ce6e25bce8
                a71ec218b254e50998d436ada860cbb920b79ca917669be9d54
                eb63701706b5d0da2d8dcdba97ffcbd7bd76b1b5a29cef2c7cd
                9f5ad00fe40969ddf9b8920b1af9f86eb690f93705afae26625
                508ccc2c475a8ec94646999444d9326ceacf92559427b33c68d
                cf7c7b5fa76866ac88803d1a9ebda8700afd31af16746d1efec
                44259a281875066f7e30fc9631da7c0ff98727f84418da3bb39
                d3e63f03e8f3fd6dbe001fa9104e36e0b36bc7be4eb11f50c9b
                88f5afbfb0022de2db3a8148dcc1f91575b55f47bedea0e916c
                aca594e6f6bf709c634f8fc292d6c0b83b120d5f26f21682007
                e17d25807dd9b42365550ee4954c5537e2d846ca833330bc465
                fea5d7d6a5c5bf3
   shared_secret = 64a60015ced50f3972d4bb5cfb566f2a800056693945b309
                   abd0ddeee3c1062a
```

```
   seed = 0303030303030303030303030303030303030303030303030303030
          3030303
   randomness = 6767676767676767676767676767676767676767676767676
                7676767676767676767676767676767676767676767676767
                6767676767676767676767676767676767676767676767676
                7676767
   encapsulation_key = a7a3aa9b70890e37309eaa5b38333f8ca91ef7b72c01
                       781d6cd542c2db1e1383c49b78757b678856016995b5
                       1709a2150aac314a815630c408fc5944004ac3709a5f
                       a6f13367b3397338c8adea1d72e8b092e9b6659c95f1
                       a3c25937766e1c8f02b66a7e95935022161472420086
                       678d507dcd660df1212ffcd84c80488e33a269d192c3
                       f09a1ba6a2bc5a5061cb32c7c18958902bb767d6bda6
                       563023d7ace28bb0c7642c839547e46103c0c5311e5b
                       ab4f41aeb16abad34a0a92465c5aeb7085d88659a175
                       c6e717b4778ff3ea8d19e6c793d5ac41b0532a043b6c
                       3826352090b47a33a2b0567d555bc7484cce1120b45a
                       55a9aa148bf135045c941805bd4243a96c2c7a9fe51a
                       a8705c0da35b6f6689e0578ade37c2ff134d7e366ce7
                       492b7905497502159a964cf7b1b87c1186d79892256a
                       7f5e7228de625fb03c91560c8f52f4c6cc7714f5d707
                       29d7a42c6057d26506b910599b10925562c02e743545
                       51ba0b7b959610ca08b540346c3620d4b83d9b170775
                       5432567fbf66b3df324a0a8798f16a4086ac56287435
                       70642ff5facd9be5085e99a31a7670c33c5ba991cb1d
                       14cdb5231704336df02c51384a2bbbaac9c210063eb5
                       763dd291671aa511cb5738f265352661ab6cc7bac275
                       5d0a87a0a7bdfe435ecd0714e07439eb04076f654d4e
                       51cf86289504640d3709b6c7717634b11cf55b87a303
                       bd28965a0d31089a6c8313fcb10bb31cf7b4a6b45c7d
                       18189d5ec43294483ecb3073e2558c5054102e5b3f37
                       27579dfb4277890e900c20bdf5a1619ac89e4b9c2ef3
                       cba18748cf8b95e3ac38820476a3f254ec323eee9053
                       626707c12a9518865372053102687b7508c7c2ca80b4
                       fb7685509f80a3206bd28af2551c662580232ca8b644
                       1971116723e04077bc37e0e2640b8000b9f80c372c1f
                       69662e24d53862006fd7d445acd5457794ceb3490cc2
                       4a5281b6324e760985847b7b9612ba3ba0d0e492bfd0
                       b47f4069a2e54373a05628957bbaa04cfbd2280abb1a
                       9ad89d3b688656e76ec539ce8838a269b11c124b5875
                       695ac0cb3d2d940a6cd85a2b93266d56a71618be0a57
                       7357a78817379e83abb820d1a206d779aa887e5ec402
                       d92c9da9b9254d03a27c17aef650ac8c4381f830c588
                       022125f4181ecb5c4d5636b7065d93454c47d784ac35
                       a08501c520112a604b3d1ff81f94a20fc090a3cfc975
                       4e578cd0ca9c34360ca4f08176e35cc0945f69294eb6
                       44a6a31177220c02c0149d1ec4a613bbc2168136aee3
                       07e62ac4288b0b64f39e5432983103c57771a030d3b3
```

```
                        2f053408351e48f11435b693a9560415450138bb3c70
                        3a29f2009bd8a890d9b650419bc5f1948d1358a9f041
                        047d030d2e1026f75532ada2763f98003f8a4a2540c1
                        9aac7eb5c817d2aabff9eb556e449c8d447015799d17
                        9b8fb07684415a5b770c10a2eab05ec3908d547f6e16
                        058fc399af653d6c440f7784bea7619056b79474eb88
                        38cb4b83a029a0d9148ce8bb188cade92024d7f90f37
                        c12fcf73bcec61cf81566b1117172522664623013415
                        8762a4c5d1b609c660c9b2c93f0a72b7066b8c219a07
                        c893b89b22705ed94da06c97e31a95246b2d4773593d
                        1b5e2c07bb6d3a5149b0ab21539f200c8445160c916a
                        35d17930a74659321c65876342747710c4c573f69c7e
                        25fa3c697b32d3746e2e7b34f54147b5f348d27534c7
                        3a0d6382a8b622a665da907fe40b19e0856593be36c7
                        954976233c8219c8a86cbafcc8c5d20c0926757dd17b
                        81666b78c0346a352a18c2ac7294b5d0a8b8d8643689
                        c809fdc47022492dee3b15b713b07990b81230c4c090
                        6476a09fd65445aa3061d71b277d806735218389cc90
                        3676c6eb776148396c2d32a49b6a5172a8cf56267f78
                        0a2b10175eaef72efce516812bbf3469582b1c6798a6
                        2709131cd419ab2faa5855b6451866809ae198859914
                        d8855ba9d109419b2dc18c322da220fde6ab21ab7ead
                        f10deab29a6bdcc46c6bb65efc06485a9e6673b66503
                        6cda98bf2c64884d08cf76b086a9ca7866b5c8ab6134
                        fe202b82794922e083c0e354b1546ee9c6c59898c972
                        a12a423c32f23670762c8ef95a63d4d5ba20fac2eada
                        0abd647e2d77157e8cc7ea2c901b3a873e5b017596a3
                        0f66606ed85e452437fad731186aa9acc4c508ad2a4f
                        246fcc0326ea60a0341c81a88c588e0fa10e146db47b
                        f379320b4dd504621bdba7406b8a3238a2e65070ae95
                        026f6bfc7d946e1530c334f92a50151a6e73b55a4567
                        697045286ceb5bfc150519382c565868a75ada2db86b
                        091661e0209b62470616819572f4580dcfc1b799f5c7
                        e5cf37bcb9fad65a9bcdaf332e3663
   decapsulation_key = 0303030303030303030303030303030303030303030303
                        03030303030303030303
   decapsulation_key_pq = 49b46321ef5a24c1c036750879c0ad29dd08607d4
                           89bd7eaa5869492759d994d875e0beaac3cf90df1
                           b3f1e0dd70357a5bafaec8a36fc2d9b72edf3f57f
                           9db20
   decapsulation_key_t = d20034c38088ae9e3338d75e1954dd00001bda6103
                          6eabac6a3ee56339d37ce9dcadd9ac162a590a8432
                          a230f06e0b11
   ciphertext = e6d40ddf8ba0b0a4a08042ab0a9c0915b51e330251fb8dfe8bb
                1bde64b387785de977142587424bb00533be0429643d77c8736
                ed8a1dcc6a8d8f6a5e5c1aaf619344eb42cb56d135b18c1eaaa
                5e87be1ce67eebdf514399f2161f6c2a38d597550e1e7490951
                938c80909063d9b6dd19434c8aef5f2ce5b4a4d393ac36c0c8e
```

287647f6dcc584b8ab14c6f357a19fd535ca7381a76e58e6095
adb0179be4a19114bcc0423f604826f5a8d813c52ae802b7bef
f1edda7ba0f301b552e916e650808323dde239be8dd561da9c8
d07986d010219eb364d15788084725ca425218af2722a51c574
1e81cb787fc60ae97e3edcd3e683b3dfebf2a8a0269c737b5ac
44a03342257de219627d4b302914d09d9aafb95388098631c3c
e81c0edfb7c293622868d0e080c019c9c34efd4bb8f3fb148e7
267b1b9bba2f7d23d387d5accc137333e45b76182cfd29f22c4
77aabbf4b6e5d24f7eb2efd3c1c4e6b6e70159e44df6682b186
0d329b5f5986b8a2f4f73beb6200a78edcabc6168bd63fb41a6
63a263d2c4f74b84fe04d393e7e5bfb684b4549887c30e26d02
ba8ecd2bd0e6a9be1e2e8706305f7fc18b6baf0ecca93f82a97
8385227fb38cb2f0ff4b7606a5672fe2abb9bba4f27c3b33b56
7a4e4a18bef73672c013544ac2978e1eb589bf42242892b8ab3
ffb240a1d778267137695b031fd148583ad6985a92c8c6dddd6
b7f82b63c738ec8df6b969098ee7687784bf8234ff52e7fe4ba
1b892ab8a38a4a5750828c50b68ddd9a8ea0ef34d2a3a779d69
16c1f56e0732e44eef7535e6e1f1717e3553db771059996e78c
3469d0c60b461e89f6afdfce270cc8bb45729e26f4db325d925
c81585f5d29268f3e6fa4e2ecf8456d6c2edc61c025796b708d
08dc497483463fe63ae5cd69c57edf7766ad1f2b231dcf37601
0eebe13806a1b3c51610d7b35b2b00fce2ff3b815c9197776c6
b96ac1612d9af7521ccfa92fb3af0cde612f9d7c55912f98f14
a14fbc4819e49115cb3007abe2c3f5069dd950ed40a79451186
952e02c381b8d33c6a6b6a5538bba5c23e78091742fd816e932
cad065642c13a99d64d828275683cfd16a3a6b853bd2414f3b6
09f9f1f5eaa3ddc25863fddcb09fc60f82ccf49679c35e2d9a6
399d97d71c7ad808953deb2696f39c62d753fa291b95015b192
c2914ce4a31ee540b9b396828053e45458220b52947409df006
ff165f9f5cf43729274783db7562439e34fdaa4ef6de9d3ccb5
5bc79e3e18a5018d2ae90b1605dc397c72fab29be1b155dc21e
62db17890c376564484655f0807830548892bc9a2fb70ca653d
70a15d73936fd71839fb55fb83060756807e71d5f87d3999d2e
86dba0116bd90b8c0d45e590425fe7cdd9dea7585180bd18171
86cc52ea79bb221f8459b136e39be7feb7a489b988c3bfc9890
ca8d2b91d3c6197454c138f5e12e231bc3b690829031356eeb3
8741553774016515994243e071f12996ace3f812efd6b79f84f
d7c10f72fb751689606d94e01dac7bd28491b5ee592ab3ecdfa
7bca01fb07e7cbaf94ba5bf9ec0b00ce7baf47b8cc9b9251ba5
05ddaea9f7f6f14ea36ecadc09cee557fe254c4353cc2b558bc
9016dd0d079568d2a4de616099083ed9e13a493c9413b9a4a15
1d22b0fbeaf773e7e69cb37736593b1885b11a4f441d0718128
ff0b5bb66a061484569d6616b57666e47a8e3696871d24636d9
d1e23ec64f8bf11e7b7315d060539ef9b94051feecd6a1efd6a
0c1b662a04eefd6db64ca7f7dbd36a8b637b98dc39dbec46f6d
804e35d9b10d80479e45f664ae1d1f6abce7ba153bda6000224
4dd33ec57fd4b27d9ef5d7b2c04757baac4a222afd09dede3b5
e19f6744330238410c4edde037a95faf805285e7758435128d1

```
                6384186daf0a72652f19e4902112dd0c78c10446eb00dc312a9
                eaa190057f0dec993322d9e2c338d694ff204e7602c9898610a
                c462aec8bcc66ed439da1d85b6f6cdc24e0b01a018130204efa
                313e1ba53469b526734dff82b98489d63c44240fb93ac53858f
                fe056dfa935d565ce33bce416ebe9937206fcc78237ce755b1f
                b22c3a4ad0601e84495765f7d8b48a7e4c421a881c21b5a7796
                4ce0e94e428ba8c4d4de25b644140cab513687dc242732f07c2
                f4773d8952cf1c66fb345331679bbbae98ff5162ff31e6253d7
                1d26b054d5c7ab0fad20a2f0404b6f05e2da70b8a532584a456
                1e870d472388e85868a5a9040342dc362b319bc554f1b99e3ef
                29dd6d7b39df6ee9818eb4539eced50a45fe98cd5f5f786f1d2
                832bbfe1b058b8e0dca415a90f99fa7aa33e5219aecff4f39fa
                8b5c3edf699a9ff
   shared_secret = fc5e3871973b49b4940905796346030 99faf8f0bb022c4da
                   ba472cb771f1bac7

   seed = 0404040404040404040404040404040404040404040404040404040
          4040404
   randomness = 6868686868686868686868686868686868686868686868686
                8686868686868686868686868686868686868686868686868
                6868686868686868686868686868686868686868686868686
                8686868
   encapsulation_key = 27160bd008ab6864b35c32ceec05a51637cd44560833
                       656624e34ff9cc88279b60f3a97a1ea43c2397cb1243
                       bc2531c3db46124113c14d59b50e988bdcb86419878a
                       4f8721f68ba3c9e8382539983b3c59808c3a50d5661f
                       655395517027 8667cc2372d82343af3a1fed09be0991
                       9ecd257fc25889fffc407745983c092e7af35cd4b23d
                       57d935d9c399f4a4cf53967a0bc4309c106b1e391431
                       6b1e22ac9e4a55441b35cfb54959af1332cb6435d9ba
                       77f18ba709aa83fe4b671c89888d52304979ceaa8833
                       9f24b992648af55c4e7f4aab5e815f81936a74001b6a
                       5ab5204935983a8073e61dbe49938c685e4c3a14cc57
                       8f11dca9a48491f05acce985bb84f14eeb8bbd62ec20
                       3bc573acd1212ef84bca45b4f523b9d8d5c15887be74
                       447c2d877d64c175a0d45ccbb8bb82b26232256709c8
                       a568662f08a1675baa3a698bbea2d5532287a9de6290
                       9512641295a9627bad0296ae59e3b2051372624384aa
                       61b4e9b19f0dca1bac6c10a31277189a1331f5b05a11
                       2c26f70859163147215b4b2c00d2a4057fe39d9d2896
                       8798a66b3732a7763934f81de2a91d69e01b1d7807ac
                       dc2ef893be10224794099c3d6904deab0d9c48ab51f3
                       1b85295accb4c96e9c2296fc36ea1b826c499912275b
                       368499423c2abb70cd08a005f17c2215972936ac5f25
                       b2cb3ae1ba9f86be02668633e582bd2a9e5226ca2b19
                       46c9d7503708a7877505da727cadc693420acc892701
                       619c9ec8792c00669bb5c5a26c8045aed7390374bad5
                       d52390730cde23237eeb2546b0aa469b3387f147bb41
```

3b170aa4812604898801a45905214b0f2fab10058a53
2f379bfcf96a76725704e07c3e24c5c86b504a74ad31
ac8b29f9c99889a28c42256397c78ad0870aca087b36
b2d1031e1e84351030722621 56b93215a7f0ae8f0c5b
7f7c81d5713f26d77d0ffa243241c95fd30f95164c50
197b7b1a2ea1dc4efee0ce52976d89ac9d29e11ac539
2ce313bb92679542dcb364ac9f764c0c192b3ed3b535
de1a51f4e5895d48a5c106b0e959165f536db2ec4cab
684e8c956777bcba1bf23b66730d5a2abdbca85a3c26
5dba69c5af5b7364018092d97a97a85a2fa38969688c
f8fca69410b3b02c380352b800227b99a57144f352c3
f6c7a092659553b7ac4a392b2512b90825cb28283708
b2c067cedc208cdce82734d819f0447eebb17bd9d292
72d15c0708760c517d8d5046b87aa51929314361a70e
a4491137b288b55cbbd005abd9bf4c878a29e7b5434a
15ee9731ecb42f80709993e570f7285045f8338649a3
35da2e03489a9a0a0257d042ce220f91b4475ab64228
d64e0dbb3ee264883f605c0b7240fecc8f33ab94e000
5a6df218bd393f73d3a18aaba6a8d15df009238fa3c8
5ae7c9170a013382a57b684964761ed6e1172f0c7e9a
ac6b9e040c389b3c67e04b1202aff784b954acafde9c
7ac838b0407078fd1a5bed71cdb74018a3b94aa24a18
960a1e22c31ea251c125013b5d7a46db184d82a35bfe
a1a9a609909d2686247555695a7686f69846d576212c
72d1958bf27c037e2a13d8b84a7f5c10e546757bd87b
3ca85a42238a4d837490742f28694b8db5c5221baadd
9c7e6f09acceec5f7e39b717337970b8921d7c686117
9fbac3154051ab236a56a1aa077ce90cd0157fcdb9c7
a92950ea0b29f02c3478d333cb3a130cf30d9916c810
b12bee8473bf2b521b278a8e458b5898a512b77f87f9
840550450be694c5e9ba4b38b703519cac558296ab08
881a7986c7818017393593315838b3fbcb8d95f854d3
91afa6589090a8ac9964b9a09c721716407f29c97e35
46b4d90d60da11ef608567f0730ac09d5bbb0f93a930
d8c533fc245833c4902ad0b53a8736b5770d008d2c97
2605c4319d78a69a64a4358929ca1e15a5329393493c
ac5ee83a834681268ab4dfca1e7c13c4570c56555195
bf6c7af3c5a1204555ca8380d814c0e9ab830a376f46
570b27171c910c41521810ea21685fc4c5fadcb56842
05800703abb9b39818a2a6d4af4ce52fd73b4b620ca9
a5133257d40ea91b2b6d6bccaf54c991d68222fc81dc
c5b32e936d3f28157339cae6fb931c05247913812dc4
1682f91f75f3173bd072171aa880b1a12470276826a5
bda028b23bba0708093ce795c4fa8f37c43cd70a2d06
a2a858ae4dbd792ad37fbb40c43d94064c5dc13597c5
981a8bddf98e045825acf2447c53b568af3835c532fb
0214aca9d4626da03f97563cfdcc97c4cc773e2e79c6
0029468539d898913b7cedfe6179cdc1ab2b27170be8

```
                    a352d83ce3cb78809392091fac41712d0ba2401e1093
                    9d93d16c77b5a1be9e9b056a8944aa
   decapsulation_key = 0404040404040404040404040404040404040404040404
                    0404040404040404040404
   decapsulation_key_pq = 79f1b2ce3b601ebf5ba31006e5a8e4c86cd58148c
                     75a89173711aead9accf09f158d0facb085bf624b
                     4de5a388fab8e60419b04710475367a0fa9c1397c
                     96d61
   decapsulation_key_t = 432eab0f3a8eeb77c6b0000b9292c6e163914078c9
                      4a161829fcfb9bb3447393f62bde9a0b539df13d28
                      c280b521fd1b
   ciphertext = 94bb545f2e6e3baf2b0a9bfe14dfe38c34d73d7a2512ae51b8e
                1c92b3e335aeee4b9189567877bf56c6073b81f3f6d35c1c11a
                4925c4abce2da026b67ba02b2edcfe6454165ee103225987d46
                54f45517a4d05cfd42a18cdd4462cc6e455c54e845c5fa6b50c
                cf8229a35245a1adf27779aae1c97c6143223539d97d2ec7a91
                f602774e43be57aede2297f31cfe7bd24450a408f611ba8ec59
                77d7f8106df0361b7d959ea971a1c57513b99c8f61e1c48a106
                48d2a987bb5a86841852b5258d8df8c7c48ee5d1f24c68f4300
                e6f0e727cd487f747b5826edb7ecf1e291f6de1e80fdf6caf62
                97a2f76d735fb70c21877a9a22177891da422b1b06a0c98aa2f
                2847c862169829e8ce2477a494aea4bb94aa87bd0517044271d
                ba667d4e3d0f06f52b424a1bf8b5d1d1fe2fe0eaae058f05193
                be403fbb8cfba5b8ea821c057cc3f5a44048d1f2fdee5567858
                bfc8aad944e3e2335733b16ec3bff838de5697ecfbff71d19fa
                6e466120728bf8d95873eca59566ecec7cfce924572ef4c4b66
                14c6cfd4cc6c9febf08045d813865cb810a8b67bdd2e3057b2c
                d5ad1385569178407beb92c7190ec91ce403f0e9636d414c299
                502446be23baeae5cf25976ad6f2f21ed0a582b8969e390803d
                2683bc91c5af92ce637c5bba627bc1dcf0d4936e84419a615a9
                a8ddda4100ad3f1fe6aeeee1c865b4b59efa73856a1f2bf06d6
                61b069005ab96944322a4aedf0420893be68cfe9cc59188836a
                7a1fcbe7fb26806de62931f72fa5403587c425a974defaf228e
                9f8f71428eecf487eff5a7c71fe62c31c5911d9c96bde7f766a
                4bf26ae88f9d53de35e6dac62ce3ef51576a45e8b907f1ff0a5
                292641850cae8b2116bc5502ccdc26e27027560cb776a54114b
                a1ccba9f9e1f91a99f80293f50d5397121f8816c1cdbe60352c
                f9f9c779333cc72e7ae51cd2819394822a2c3f2edfbb0099b27
                2c2f883fa11c3bbeaec067ca54caf11ddc45b1ea79c573b84cb
                96e89fdbb899571c00661e8544a64ae0a96af5ccb65268ea808
                41f6ef8a832ff83b9d65d313309ee8d4a15eb03b233272a83cc
                0fbc587d06a6deba39e2c6ab6f7b8fc7f23841f5b4b7751fafd
                6fe28c439c3e39f03db741b81757d443f4aa8141789e81401ed
                afebbd6bff34bc7f1f3f5006aed3033fba74f369fe37864a592
                da2379ec49d97433d0f8aff262fd5465c9db351215c21fc1adf
                5cdab6ccfc49f28627296f6ae7075bfbffe1ab2c72fc404256a
                a253300b53042da954e6fd16dbfb6759f186b0d215ebfd09d21
                b7f5385a27c77f65d5dca4ae62550f05b8689c7c0ee04165217
```

```
                9d5aacb1d338ef667abc1aa74a11aec98d91f92d878c6452878
                baa22b0595d0dd888fd498670ba01471ebc246d5faec58946f5
                7d09b8fa49419995b75a6260f56c8657abd288d00cb6b296993
                94f48f02180a45dc4c595cb7a62700ad7130f19cefe07814134
                059f428d1f19a0c786edbabe2e1d085859fad0d3c455a3ebc10
                56fd1017fefd7bdaa370191fa912d5c1e8005c8f6a6a2c9b933
                ba2d90181202c7107ebd5d7c1dd70f52ca0ed678ede21346ac3
                08f846c4c26cece324b2dc83d5d4b68f0fbb0a9d6a9fe5ea71c
                6f53fecf61913573606e5f29f23c1f683f31688399bb2856f15
                e11a8c3f5d9425b708d2bb74064956c43983979d6ae434610d3
                94e5a81acb26951f81ea965d2c4dd12edfcd5954214d58abfc6
                20a76e4f6ff37859d110a0718c397133cef8600f44596559b16
                3626cb1557be60772374be9e5ae26fa629c1e11f93197806796
                9231405614f602261f7fc7c77acb57d2b82e8054d0aa811cca4
                6e0209a733f4b70fe37776768512cb2ec63d90cfcc0493aee22
                fc46c3ae9b4702423899322840658 3e200d641165fe3c4c1dcf
                3614842ac0840108db7a5fd136ddf7ab814d5026c4e54f9c3f4
                0c8ab9d33b5118f22146938b0234c6ff71ac1b08a04968ec277
                b84a3f4b21cd20ef50c0dc2f2c71ff2171927c4cf68fb460b48
                37d66cf9e92051237497f9c1efdfe16a04d317263e6a825daaa
                91f4c073e09dbded783d13cf65cd5223ada3416d7704267c8a1
                a64966aa43a93b7b0524b1058b01d7281d43ed038d1a95139e2
                80546e3123011b9d766d6685f9b5b93d8e927663a09634f38ad
                b3f16c7c2c63992983ca5a4fcaf8c240d194f87567cfb51daca
                300b6c7bf21ad968b15dc1465040ad9fd3e2cfa1c805fed13a5
                5a17e9c5922adb096d5b253299024718b53d3bf0c98bfdc0a7b
                4a88c321600ddf539ac791808fdf8b189c8ad00dc5397814d33
                0521c1e357f39b9c60867b78895038ef2468175040231cdee02
                250b2dabb6f6ff5
   shared_secret = c3f7adc77f966a24f642197c478583b6eb8c2fe3fab19809
                   25b628b9ed5ffeef

   seed = 0505050505050505050505050505050505050505050505050505050505050
          5050505
   randomness = 6969696969696969696969696969696969696969696969696969696
                9696969696969696969696969696969696969696969696969696969
                6969696969696969696969696969696969696969696969696969696
                9696969
   encapsulation_key = 5b91a689d96b5c8330d76361fbbaa995e78b4c5229ab
                       4a321513988b1a8c58664d9aa70e056813a064020e51
                       c7bd033105c72fc1aa5da5f16973919d17445a75b3cb
                       d5c20f42c8c14717b78608b241d37c80ba20e50c2004
                       8aa67f17ccec332c4b58266b0bb4a42a099723063765
                       578cd35614dbcbcad14755159b185865c2e6bac9c4ac
                       5242a0b4eb63c96c90ef63869bc8a7b00a3bb62b5d35
                       ca3bd1e0b90cb75f24d5c78201874eda2fc098582309
                       0ba8c56778cca9c3780e2c7c3c5911515efa88ac3706
                       8d12bf95e262d9bc0c540154f168a6d2eb4ed1ac21cc
```

295008c3ca1954919a0a76a4963090e915d2293bc094
2a01eb8c5e4c3db93b32147ba890d9a5574b5e119b14
d732431bf27a2bc74e8cfa205488b273c16070287b50
5a4c6d4b564e4188c5146532f0c87070816cb42dd80a
ad7a028d9105343b6724fb81952751765a0917305714
dd60360cb7add1473f4651b4716577138396a3798447
d549fa01cbd8d18b395259b1dc4b66d7b08e2284d9b5
77d3828714d6887dc243a0707d5f097c8ec33ad6247d
aaf92fa834042ed774b3c35da3195a290c6513d0c008
d6b2de4aa0efc9500a42949a5407338890c2720f8f3a
5519640436b85fb2c53ae9e8cc202c04ddcc6de99bb1
a1181608a3887906cb1db845ac73c1269b1aec2582bf
5865fe837355b4b3828059d812b6e2186bfd5679eaba
1e2fe4a367157feb1b0f5d6161924aadf9c637e17bbe
ef2a8504815b40d8c43280c3c3cb9a9bf5c7d15926c1
a464f90577b3fc72b9b679cd4a8a67f9576c98b5f1e4
218d498af76782cf2b5c4eec64767645b338455dc4af
8585ab98c8a8002c27891429850b9f0a84af0043c831
778dfe79acecf868dcb6174e2bb15c96374ce968ffb6
c9ec60972353b1b0a77c066c2ef9d6691ea5a7bb28b1
19ac91ee371865bc89d4780c3fe8955212cbfd5c1273
2c2e43aa0c52d133739cc7b5007a414374b5029bc983
ba203000bd7a887dea2c00cb110233b5f6876d02d539
c5d6027f0319fa2b9af0eba53619a4f447ca71ea97de
c65ffb5541af64c406bb25c2970b2bb457b0b755ae94
aaa398c38a945274a75c2beb2c4610031b7a41fb694a
1a880f97bb88d3579eec2390b246ab36f208e79c65d4
a6194b770ef2a0caba95b41b315545d0080e6927ac4a
793a95acaa870451b6c5cad62669465c9f130548cb73
ac57b616343dece0a9c1e249edd4487023a216b95862
474cf8330524f4306fd640b7eabd0ce87ef55b80e721
ccac2c5b0e0b16b5bb74f6139fd2d49813765988689e
32358ea49b3425101a50fa1766d5880f3a3c35683000
f6b2e296b069994d83b51232914d5c1325225a06ef52
a49497142d06c16f485e1c10553e11a253799eb15565
9de16bf9eb127ceb86230cc369487c7a276991541460
b6246c998bd72152770c094c5364c41357ef8105fd7a
25306b33c696562a05c33f1b11d46906f9e38a4e8368
ab4a5b62971d9c1b094f286077f6906f463be2ac1ba0
5204a129bb1334082bd71810e5be4ec75350709e57b6
b266c9c5b9113675b0a7b6b5b9bb18718b90bca8f791
84060e3fb13b1f75c87616cc52348e99c79458e149f3
f6a4a9782523213f07b2bc9e4accab111feda22e6619
b64bc04e769b7cb4c445fe5338c2a5362908a818a6b8
51aa1832933e30a69d9dc339ad0177a3407332221147
8878768b350224c3026b12ae40254d302e6392422c50
6cdee44f819b4bc11525a26b891ad5053623870b1957
a274904e4ccdc562ae169605517c7ee3148409a78568

```
                        daa374982c9c920d5821a085a529756171dc59aa2538
                        78a2d3bc6c53c8b7cc51be85233603211c87573ed90c
                        c1d59819ba11e00a4eced6cfa6d26af46a971699038b
                        66475e82bc23b5410c02466acc37a7d79f1a6848aa97
                        3a9d628afb4c90f1a7074698bf34f13674f62f81db54
                        11395e9914095be77f14020711254a4078a4999c854c
                        2ccbd196b60311305fe322ab32983a535fcb81162e6a
                        75eba885f6d2228a28ce72f697728a1abefa9493e138
                        8910c8977cce95ab4a5625a600fcbae4f03f2681020b
                        18092119584d27799f7c3d0154c8a050296a4c70abb5
                        5423c57c597701770031fa2c8d5d4413f8f15cb615b1
                        5f936a93d61f8ad971c68cb4d7b239ca53a5eff8b3d9
                        9488032e03682ff7c9c54af9d21b77d559c7fa678a94
                        87d60781bd1004f92f4a2fb94044ebc13e4afff556e8
                        3312d782870ac897002110583502b4c062955262c9ed
                        bf352a49bf3247a5144186d78d3b28fbd76413278744
                        4fa933c565091883535c7eb9b8daab2638fafccd40c4
                        9de6050e28446c1cded052f676a243
   decapsulation_key = 0505050505050505050505050505050505050505050505
                        0505050505050505050505
   decapsulation_key_pq = 749fe3a6fc429b2369d9e8191f72d4fd3b292f2f1
                           22312bfaf4b6a90f1600c4670ebea7aec851d89f0
                           095c61a2caffb37f1ba7f21dd514b0e20006969d4
                           85ca9
   decapsulation_key_t = 730def4e090b60c056e1a9b653f479af7398bea957
                          71054ab4f455c9a86d7e498e80d0832a48d7dd46a5
                          b7a168b80a04
   ciphertext = 913ebdd7649538471b99c731ad2351ab626b20bd6d9a4bf713e
                6669c80f750d8b1277b3f22ec2e7a73c5fd422327ee91bc5ad7
                046460bd27f6c10dc4d5e9688c871b4aeaee4051dcfe085a1b8
                7354c8fd8fe4f72051b0e87f30c21f02a8dc65ad004b0ebc8fa
                cf684c8c67b0fd7d280bb5349209856ca86edb80ec2757f80d9
                a00c85b1b92a013a969ffa25cbee722c788d631c67914e36048
                1cdb6414277cf71f647765924bb568df6c37c0578e145b95f48
                7f4814fa9eaedfc235b87e5eb417c4f56a8e19c92f018e6330f
                bfae0c082a9c6f179bff9b79fcb0a880e14472c2b4a1ac4b246
                6755bfbfcb1167b8147606f8331c2d5ed62216fe475310c4e2e
                a6e426dc2de4e67d93bbda215aef0b3d536a6c99078e513f4b7
                7d22728fe23efa6e881d92a5db5249b4f89aba7a703fe2333e1
                7072199d266050cb2ff4a2319c219122988448645968fe098be
                68d7a30f6b13ffa8ee05f01b9d5728db03b4c37761d9cc9eae4
                59159edcaa87442e067224d0b84b54293da273a80697158cd93
                ad7a08cb9427bc8d0395af0aead90b10d8c2a47f9cec11953ad
                f2e74b5467ee2f16e0f3cb2b693a2d2541d643fac3d7bec1b03
                b30cc482b7b8105167f0f4478bf71f7dbd2c4199878887fa713
                6cbfdb329edfa2508dc5b305b844d05aaf0914b6682dec0f57d
                ef521e606b9d15ab9de438106fef0d0834c9839e765c7869b9b
                76aadb4cfc2d9f02393d4979bf54f59f8d55a38e4f2d653f5a4
```

```
                bb5c250abb6fc65d6a8496b778a19fa1a1c7fb8f4fa6f6fac1f
                47b3fa97f2bc9fc1a6fcdea508bebfa8b1542878dfc06413dfb
                414e2cc119c3709e5049e5c891d9b5188da8fa10527bc44440c
                eb347b7acee506634ae57636dbee18a460485cc2dbb90f34489
                df3b6e583ceabee9f075a72e8e2d43ef7d71ceddd61af0c7fca
                81a049b7e454477df86c0bdddf676afa186edd716273ccf9805
                c690fd8ccce852c70bcd9eceabaf807867989d52cd9280d0a48
                16b093335716c6b4321954c9aaa6f8fda48549987fad3d95213
                f6d66f62c406e101a4958588250d15d879f2f83f785a5446b39
                6f73074ba69d98ba1be0b6ea340fcc2d0eede24972a6c460c59
                642546cd8ba9df1bbc050b1b7c0c4d2b123fb8dd66f32126a74
                4b8f1af573ad36e6f8c8aeea44e04695e0ce7df7cd35a4fcdf2
                9eca300eaf35c04ad9ec68e286fd991fefe9d58b96e6c2b86df
                a6abc314d9f83432357747d7d129d69dcad7994df4b13fae302
                8a5b402d4fb1731ea32e6969770c0599bdc7c52e27ef1477d0e
                00fb97c3d8e5eac967956c05d6d35c9d956c36606e17c9e5661
                95341ecdd6a87a98923fc7833bad39249823c3fa905cb2b69c7
                0e8f984c3b5b165b3621a50ae69686185da98a0035d112a05a9
                a3a5615afac3cc95ab4cdf385c1cf3471fbcad069e6ed6944cc
                c27a99e85257ebff3d331fc695fdda1246ea63646a02b91764b
                9ba025f27c7c66fc1311d8fb6ea45b0caa563042c18a3caabe3
                cf8e2c3ff062e20960c73d8c5b43a9b0d47dfaa852190ff58db
                48eb73325211c462ee43aeeacf83d257b23a0f1f89f64e1338b
                2232021e0b8e2cb910b28b476f0cae0d757ef65b6a0f799ebb9
                a9a22b67c636fb1f1def2064b362ef6c59ec8e780054c7164d9
                49305ea7e14fe9293e4276a3aed2e40bf46ff87565379fba60b
                71e57092afb970c096442d74f1bcd902e5d987f15e03d844e00
                a9c34b08d1bc94091e7e0bb40e92504bf12a13b8bc8a84b09ef
                32947f6394b0f7e07754079e77f7dac507798f3e5ff05b8a8d6
                30f39fe954ef891f17069022e79bb677a73c4f7e4adc7e8ff5e
                bb48676b4e4d21a6aa9b667dad22e62338d0be0ea51694d2ef2
                89e64a169e6c5b755c729e12aecd0f98e9c8091b86f92fa0315
                312289beecf266ceb67ebfbe7b1cb657be89fb8ba9f232b413a
                bdae08a20bf7c81b4398e092edb84302a44bac26325fef80bdd
                0cff5dac1e0b9b59559a3c55c32aee31ef884b648f55bee6a39
                93eeca7cd840a60fe2fd247430eda76868c776bdee99493496f
                36c5c0d5af6f89fd0292f8e8fcd11547668b67da74dddad2029
                35f91951960dc256b418d78b3dded73591bd07bae1c620d3b94
                125020c9bd6b0eeb0cc493858f7a83765a40e94ae875807720b
                e76a35bb5e1784c09090efb4dac017dcd80f3445aacc24053bd
                b6d550fa85e23710b8a471dfb0490f44dcc658982c31b1e161f
                db5abe572bfee732c8c1ea15d0eb993387e604ce6ddb7f5456c
                0811bb60555ff065939a2587a42b5184449fb2795853647a62b
                002f4b5c791869a9df2cb91fe757eb2c84299819332193e9465
                ffa0af6b6948fa5
   shared_secret = a75ad7dfa8fdd4756fe5c0bdcf287e258562c5b3b394bfd9
                   49231966dcac02df
```

```
   seed = 0606060606060606060606060606060606060606060606060606060
          6060606
   randomness = 6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6
                a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a
                6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6a6
                a6a6a6a
   encapsulation_key = e6db2e7d848e7c8c6ed67c3e8304ac26d3214d361a30
                       86c1c064bde1157745b79bf863b62a043bf31740adb2
                       50fa338a7df37dee88830ec31e511c3985c111f29913
                       5f9ccd0ab056ceb3476ee730d0735f1ecc36b2779525
                       e184ac19bade2c8b8af42bc4b00ce5239feb4879c15b
                       47f88bac364328c1410c92fb0e15c2c0da79bc6b8080
                       d20b9340f346344a69da81931f79aa9232a7d54834fe
                       71ca3e802525f16a345cce38eb3f3ec2c4adb2afe868
                       5fc0c544127559a959074e784598f05dc6c79be84ca7
                       42f775c377cc0ecc36b8d00976b64c19821cd580aacc
                       4a8f27841f6374bcd59b094e94ad0e1a576f6508a730
                       8ea6cab2584a7ef50b887d8807aa76460de35d8dbb17
                       68c335e10b05ed2a4d9ce83920fca30a00714b6aabc4
                       e6823ad2af6fda9fda50b908a2a1f956589cdcbed50c
                       460e3aa21511620569593c80774e7966b793639a616c
                       ca6c8f0bf5356e05ceeb27292e76b15ec82f70aa4a8a
                       fc3aa24b887d92b4c2ea81d9d1c10bc1210ab2b644c1
                       a35a990c035ba07095a7e0569c3b4c39bd100762c6ba
                       6fd9c0b3978b22211f6129a8dccc5032283bcac01b25
                       141c982808c1cb11e112819ff558faa9396bb77cfdda
                       8085a602981889cd272e56850e0e2355c0989a9ae38d
                       2c546662a5cce84520c88973e01205dec9c6f523b34c
                       10055d6bab3fe63864337fc6058540aa49216996c48b
                       1d3473bc94aca4586a21e92093dc8204a1d651fcd036
                       08b368a17c6182c52b437b7db0fc2426c03c21684962
                       f633f2e05e293a095d40a5f5558fcb26303c8b728201
                       15b324519e61cec83953ef3a1e8361a719a4cdcda41e
                       f5eb89961554bc326da195bf8c2ab944c368533ac86d
                       e9b23e13951c8867e35b6fa933a432682ac365ba2aa7
                       a529b6871d728ced34418ad58f8469972722a1a159ba
                       04972162671815f36739723fc54768874029bc3584ee
                       292c5c58beffa0bb51282850fc6a73fb6483eb1c224a
                       c0ed2c1321eb42f976644340c994b2c55c035aa5c0c8
                       c60964f263b02be9b3d6b87038722f2cf741b265b7fc
                       ba6bfe203291a09564938bca82ce69492c831a0cbe98
                       6739b54a8004bb4c5b7d0ed471f5627c67350a2d5069
                       c80c04d335c75f4083818c6cf8a04d855b11c2c6743e
                       ac9d1d947efee59a34461f4cc0c9f1a78cfe8c883417
                       480c3c725b958207b35b3885129fcc08719292e27491
                       903567b3a009ab6b5f38015abbd03fe7b5ccf6b70d53
                       b77e131640ddd37bae220b60c15a83f638e5f92d8974
                       76573c2bd5d7092a60cd42124abf32197385a1f90435
```

```
                        be101216e81261906d2e599c2f698b029c193c177604
                        17b436ba86fb0a41bd37ab93a37a462346cae3a65437
                        b26fc54df4580439e22ee71c6ac82765aa7acd5b136d
                        6889a2dc136791cb6492f7c0e655ad4ee0b3627a2cb1
                        b8992069c6accaa9fbc5c1a098250fc148b23c3e1487
                        bedba4a4d59722c56a9f95fc9d7234274071a16f5b58
                        75892da1691e3be71bb017b6f97623ca01204f970eb5
                        88270c68a08f67607498122ceca637b90e0b3743e678
                        3a0c08579433a83f0272cf863917f757ef1a18b5bba1
                        4046696dd0a473188c5dd70ce7f39d6c1123e2241843
                        e002446145b5cc61804950038b6e4f7727d2c5043db3
                        2d445c4d0a4756fc91cc27d9330b09b8ff8c8561475b
                        1ae3051b84343e21b3ae25029837bd48a12c95e76eea
                        f09011a72d378c8a0eb4c9f396ac00ec1811bc9399c9
                        87c34a3ef0777e5f575c4c227f8883a66cb43b3db754
                        94ec0060169dc69973fec3cfd9f27d048979d48cc188
                        668fa7729f16d489b7a73e6ef0bcfb31a41ad8179752
                        253d38348226687f489f4d7569e74325c1e8246cfa68
                        47b35072b553981c0b3f566d6f449f3a80a1a8534eec
                        3136489103bfd55c3cc929e49730de9a34c89a302833
                        6dffdc2e6df7b2aea1c43cc835530a6b99b2372556a2
                        0fa078b5c80232d36068120074707948b062b289a5d7
                        618b74d65a7ad2b6b743048466438de17a9e571db546
                        30c4ba881aeccdbfd45c4818b01e0240218ccb1aba0f
                        ad273899817869409f7409b77c3a2693597740921648
                        c5669d788c479cb7fc8a743bd23228c02753ea619152
                        3d09180d0bdc944ee37ab0e83d39d5802cd20e21c8cc
                        ab7033320cadc2104e29bc4d1612a38638cd39f299a0
                        b95caafe5fc95956d82859b1f37ce95d3fb88d024413
                        7561cd922cc4046f4356c2e3e6e9aaf6243a71de6c76
                        f1c63106efae0a85abc53039d3b5d9a8e32ee03fb7ab
                        b085f9c304b8405192ce3c9508e104def48d030e57e6
                        cc3ec1eafa408dec210645a6243de6a6c4f593c29fce
                        358ba48539929ef3c584e5ca42af8f
   decapsulation_key = 0606060606060606060606060606060606060606060606
                        06060606060606060606
   decapsulation_key_pq = f7d6c6a46a9c534d6ee0532938a99f0c450da4935
                           e2953c4daea5d5b0a59ea69c700a40817fdf445dd
                           5b73ed69a557afa27839191b8e71214ef9ef97e9d
                           9bb99
   decapsulation_key_t = 0a925a53f7ceaaa373f3f8ecf9c2d9eaeb351eaae4
                          dddecbd7eb180b5432306e440b31473c870419efd1
                          69d9b1df4019
   ciphertext = aa5a25b8315b9e6c940207124c6f2ceb59a295b7683fd6762d9
                1b7ac37f593fffd172954d708d937d99801708a7c9ab15d5fae
                5111ff6584c845a405376bafd33cfbb120247e010b9e82a2eb5
                fa7097882eb54ea99b37f5612aa95eb830fca30301e9f7e5ce1
                cc0e3fbd39c3ecc3cbb9b1662c8018c6039d07aae9e32d1a768
```

f72c659b8f98af17a8180077c5918acf645d355d29a8ef0937e
e354909ba30bbae355d84f954f6a909dbff2f69512960885e60
e6a9da86011af4e1402be1e3fb8e83f26b7454de4fb64b9724d
90ef8f5b7213acdd079dfd75e8b742ee3d161404f0b600e5906
baade188d3bc192842dfcc3693709f8d3b0dc692874c7c45425
6004d66843ab5ee32e9c61f62b8984a28c333804af2a028dc20
b9ba5785d2342112e2534480972c65a3a547bb856b8e9d34870
1e67f7fac37322714032415b4ad524b7fddf623501467470bac
b0b79f815d3ef0f9e2237f23e601acbf3b56725bba4f158fef5
19fe53d94e27149a658119f6305887189c1c0f655558ddb98a1
778e6b1a5deac60651bb97ca4313e1d45742f0dd0dec3b28b36
9ca52eb87257b37d9a50cfd825880ebe2774808be2ba9325c92
8ff7c2da2c9d46dec148e682d174608615da0261ba4d138b0fc
e3d0bf2911df0133fcfa5e1c78c419b5c4f9124d20a89a7d61e
0cb2ae397e83fac851c34a058392f8df965085b7b935e98f94b
1e14230b060b3df8b533d0d028b75db559b65a9d37e4158cbf9
a51881c7644d56d25cff7ebce0d5b4aa43fcb01cb15b138d469
d8db30eb7b72133bf2a815f65b96e1077e03715547f0093240f
8c2618304b3a3ecc33396a6104b167636b9adc65e8d5ba70a9f
e7323d369083f51a284d7d21d47fcb393e4fee816c36b4d46bc
1239caa431c01dcfc87b865c9ce69cc2dbfd263671eb5e093c1
44717d07f645741b85ac5d0a214389ad1b958bdfe7f45204f49
648a21494941f482c626e7af0fabdce53e76dd7ae501c50deca
d7203113482eaa55a4fe29ab979604a1a67ad0f446c5ba998e4
8abce37d387102594843f86104229c995aacfa59cd0491c621e
f2abb03b75ed090545bef7f875a32aa630dc056d45e5389aab9
e441ab89a3b33a651e420cc9e992ec474c7ec37842e8a0633f9
fda5e39cc975575077850710ffe0db9fd220408d98efdbe5010
25c05345440437d7213d5523aef7d5c283778d218811c7cf11d
ef4b665b9a62b699d1a3ce33a7c247a5e99e2ddf9c9a4b06d1e
cf27c0a57b18d17d5990b2cd310629d4a7faa2343a66d6a40c4
5442899d5fb20e6d236692e605d2a30b535ca70518258438f7e
b38b9589e3681c552cd174f88c3e729d50381299919485c3ec3
a5a86da59f375304d4867b26ffb7ee194b3b1f15330cc9bfc4d
abdd59446e85e4f1b168d1c05d14ae55087e1fe353205f1e873
d4750cb0c425f94b822aa1d54b1f1a6bb7ed1009e19084d97aa
d29066a5b453211423969aab9ff456444e8ee80d37b59698bf8
07156e4f404d8f3d99aba1230f25cb5155105d2249e581b122a
be7c8bf62b3938665acb49caa6be426ce44f9c018b59b97290a
46f0978e110f8d2d07fec0d972a5d0ff0e9f56d0f55a7d7f8d1
1600332877a114451575101d18907083d4760b861eab94bfa67
e5f58ba8883dfec7df4632178073322ca7ac66dd2b44ce73c3b
410861071f166c888078c61c9dee4f810e5c0278e4ee53abb39
5966d82002d09d2a127ac44351a6a8ca45dedc05e4b3c45b64b
855fcba017b96de8bc128c74f4569a3da57fc7d1e91d51a9d49
5045e203c863a2ee3711eec0d28989b03a43402b125f752f8f3
dffb8b2f0eb043b2d1342633563c07b32857e487b5bac705045
e43c8ecaa261e21887022203990b58ed87eea1ba73f46f69e48

```
                3cec4567f285bf1e0a2d9f0e6c68771144410739bffe823b7e8
                ca2c31bfc381a2d6499667098d065f8e3ab61094baff3a33664
                8ea79454f73aca9f9d45d2ffaf52258e92fa381f2478a6afb40
                3563d9e00dd789de64503dcb08d41dd24dfaccd1babce39b344
                c5cdb8a3442ee66695eb4521e5f88aee992f2ac5cce42bc1baa
                45d9a9621b126d7c0576cd48e081b28727484dc4f135257013f
                3106cd8d3e1ae8cec97f8360922c2cb6c929ab81e20ae1505db
                a6d5178325640ebcaf0c6ab8ef74740f72a070c7bb548487a89
                fbecbeabf67e02e2679e3c5e50455914a6caba74acdc6697c2f
                4c089984587a729fdd6aee5bf96bf2c523beea2eabef56675c5
                05e2cb191ed3428379eee81be9797e045622bfc163fdf6f4d4c
                c72784e2a47f1804db75d94a278a63952c7e310820983d3fcb1
                18aa0f69567e41a
   shared_secret = 8f81b7d72b0c023dbe66df377cfaed177c7516a06650aafe
                   c6046410dd0da9b0

   seed = 0707070707070707070707070707070707070707070707070707070
          7070707
   randomness = 6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b
                6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6b6
                b6b6b6b
   encapsulation_key = 36f2b5d9481ba9714e75c63de35c4d847ab513d440e0
                       ab2a2e42231ff448de283cce31a9b391ac3ecbb29d00
                       5dbb819d44b88490d82ebd13a4213052741b3c6f797e
                       89040490430b4246b782c049e556824ed9744295c878
                       773643c57db8ec4c8b6a43f5488e29e509274722bc89
                       6371f58ad761c2a747ba00e50b152c4368f8b7500003
                       d50965aa0caa4627337290549d9aa2f23b63e84c7075
                       c98f4a342d8fd4ba96357576ca49d991b98ca497d54a
                       3a4a984d0aea4bd61a187f639957e27b1e69b549c923
                       ad253318f02c2b4931a8c8299d5b8a32038f2bd05b6b
                       10824c08a4f02c9821aa3019a45654dc40574b9cec01
                       a758f2c9e2a94b73d982a671c54cd8ad6ae95c6f3713
                       807aab89162dfa68734b6657aa47212c8a17fd45bbb1
                       5a9a5eb40adc0b158caa14659ca60a073d51b1c5ea89
                       92d24b4651581095e4bd1b5151e4f33c7113a32db916
                       af09c43d3062ed113c9d38027ef545cdb1252f34229b
                       45b3317597dd6353e5d32674f02b0f7975ce97cefa1b
                       8b97d1249f5108b1068eb3da77af88ba4dea14346463
                       293260474294cdf77ff10c75e5d9a33c751d5a5a6114
                       6917f94a789a770f01500ce3a5b545e6af8660882550
                       7ae7cc604ab5718c4481e68a064a420aa853c4d55909
                       5c53a01da46004e6c89dd9995847473dc85fba5c11b2
                       22377995a90415aba01472357b3f7c524c1d413c07b1
                       c23bf9a331a36c24e4c9edd568bf2b2bb8fb5e4ad613
                       bfa36a9d0c5142e60aa0e5b9e5a48c2952270faa185c
                       a59a24a098ae615fd1678e07fc7d2a727753cc2c74d1
```

89771995ed266658cb24b8dcaf067213cf6067e95c4a
51b9b55e9c05e4d0c184039d88869b6b1846ac9b31cf
59221ff6c5eca2274150cd5873072d8c583a35488d18
7f4fa1314c6a116db548b5795da2532655da402eb906
9b77295205516fa810a6f9aa9af60b51819e28da1ab1
e950359a9fd0ca5971c8aab5250d3f7230a07b9244b0
19b8ea5534e805452b0ac3dac8954b36e97b80e53147
59c3886cfb5192b234fd0172d5f565d1ac8465d205bf
b55f741c366d425d95e4a4483b84becaa6d5ba48bf9c
9c41723c1fe54909c02fa67b62cf6a7c776748934a81
7c97062907850a86269999b4342c8f9f803da54a8e30
79a6d7548114968a48459784b4c6eed326fed305682a
39202170367571a95cb8ddeb7bce9c93ab311d656663
cc88bcc6c1b2e1fc9c633830d955aef7f019726167d5
f5b81c369546083e611b6314f73b3dd90b4079c5d62a
6eeaf14ea5426b7551c16b371ecf537bbfe6a0fc577f
be56242dfc9db6a1035305182b6a265bda1c42982d76
a59009e5aa546824233c7e60ebb865146b21408d925c
2cdd01187ce7732c60643845a3a6b82ae9d848468893
1f612fb7dc8d3225b392993463748f90d8689f124642
35a607d68ebdb932053b75e25408a7907e03e936da36
300b9b3d98f51d7b61afac32b015d3057a55022af238
7701c5b04020a4217edff1c62fa25a49c407e0fa18cf
d513793b86532524b64b67929727b7482b14e14116c7
44c4893d6f6931bce982a9c46dc6048ed8e99f304891
4d4476f355cb59472cc092805910a8f53aa8dcf93969
8abb30730bff24be1d49c7626bb439d87621785eef26
aa2da7801714c704609fd3955b9d1058dc2052aff863
4076bb01426bb0f3c1696bb773f3a920d90e4aa7c839
b14b69d9138b1413000aa8f3895dc0a893a6faafc2e7
940d62616ed37d46578d6c03505f1588495b3537f95a
de1aaee4c1c3dd0a35ead94cd30a5ced265a08427454
76a164d9ad12a5aa7e3b55709c1ef6f7357442bbf632
91321981d7682cfe480d03c5a12015ba4219b76cfa99
7736c246d888a65c470e98bc3d574b4d7ac0072b0622
67bf81a91181f14ba3d202bf99ae47f1cfb564966f3c
3582c85ba7c66ed9058a11856730f71807e4191673b4
cc324f360cc527a060e73b511ebc10f1ca2bc79318c6
c748effccd928277deccb7ba36ad4dacb2b98749c898
92aaec7d07c162bb6b7a3c52873993a8b7392b36a86c
853494d0150b0d97171e08360b9c3f598b5673c67b14
5b20781a7a7c16270d2166bf633e861b0fcb6535418a
6106a0aff085cdf6e73d837941e823ac064424e388b0
2473096c8a8d6c816a9311a5ef68897fc92cbe922749
dd602e7ccd9a5faff76e5f193bfc19d784de0c826d9e
b5b1585ce28204d0fe95ac293d3aacd0dc58f6fc9d80
1516045da004311ca5a20587611c5c4a513c4c702981
b88f3de97bf00bfdf6138bd6ed1a11d3c0d2df7b7b9e

```
                    bed10ffbb85db1be4abf5e9a62de86dd46530d6a7478
                    fb6805fbd32d4495530ba393d42801
   decapsulation_key = 0707070707070707070707070707070707070707070707
                    0707070707070707070707
   decapsulation_key_pq = d7b4cf68d3f1b711924ccded71a241faf8162f7ef
                      6ce748370a10e86b94befc198683377946eb96641
                      eebf10062c6dde3a010a09b2ceb1145210a9c17ee
                      fc5b7
   decapsulation_key_t = 19d62650372cc18fd0109cd6394d638ebeb5f4cae8
                     36ca4aa56825e9056e3ad5b950e3d963388feef1f5
                     d26aad4b6a3e
   ciphertext = 4dc3b02448f339df1362f71a0929acbdfb2a0425f54adc2f98a
                62f468dfe9f756e898689ffc2684d66e00b15e67d85cbfd059e
                f9f5f72743dfdaaa99f0668ae422b41bf76584a5bd2fbabf699
                ea7f56be4b1f75d5859ddecf9555472ad5c56e26eb060316e25
                efdd57cfd367e459bbbca12ab0e3ef02111606dc4935d9d80ce
                9eae8348f57df27ae3c575113588e5e311f96ab3497774e0ef1
                e27e2c5b397028f9888fa82dee054ff4883b98b8e9f01ee8a26
                f35a967cbaa5c93082e67e6fca4e6bbf9c2c53a9c699642ec2d
                06f2db513235040a74ef68bc7f601477019bcbd47c19fc7c2ed
                ac12a570c9797a81b0d59597b1865a4d904c6ff99d0e7e6b452
                dfc4ccaa79e4c633079d9c280b52aaff716cd1936c4b56a5170
                69cd1b69b1c9f08dd03403e6765d1c18fc5e3ad219d80a83c16
                ef440a53cd07221f12b2c4351c0cc22cbfc9a8bd648f7258194
                faa9f7263c1235d517c43f62fcd896b7c63bfb25d80857d6c3f
                5fd352221b80e780ce76c7d7a9c573de96f06173f4d9c2d8b8f
                3ac87e4154934b7884a3103e9fea436224e632c83bd3b07496f
                2b628ef8198f945de14cfc3a90998475e4a332f5646bb6f5f9b
                5a944ccbe0631204a110d66a7ca111b9da15245a982c2b63446
                bc2a2084a26f1d69cbcc68c6d4cf64efce166d4b8a6d9552a3a
                81999fa270ba3a9e8e7cfb280da4251875824efbb56161f2996
                e9d2cd6a66980256b41f10704a93d2f4cd87868a6b2967ca92a
                20a71b8104b5536e014ef837fc78d8dc8ee3a297395aac377b8
                5ecf5393b33aaeddceb1e10c24f24f9480ca4e4ec275f0abdb3
                6124ff7d7c79ecd11b678ea4bc125307e023cd4c3649e49906b
                face2d2b73250910c1d4cf081038008ec7f0756ca945d3362f5
                bcb9138e8289f77e0f8e1e54ebd2198ceff11f4ef1b53d0cb02
                8b3cac0bfd0cad0015a1d83413f1929d6a505fc51329ea46c96
                80786582378724ddd4300e7147ad2b5a1f9221723bfd57c2a2d
                3a33e7b1cbf50ff99ed27bd1e5f541e9a5bc522685a74c7cf2f
                749a1ef3de87e069ffc0784e6c19b39168bed86bbcbc4b771b4
                6839c275d0dc767ad1420f56143d031622fb792c020dd294448
                86eedf3b671b2a3bf875f4b6bb604de6a0dda58d8a794697829
                ebabc37d1249ec869b46657fbdeaf5dc5da782051107b192382
                b3c0820b64e0f2ec15083de32369da090b914121e41dac1dd7e
                dfaea4e1ca0c3d98763252bfe365535c42af6460abdf64940a0
                1f6d6ee98d28ded7098b2160a486166ab36fbaf392e57086c2b
                a71538c6008a9c459ed3bbb0c5340e3a11ac84d6eb2e752ac58
```

```
                1b53a62c418f2264a79d7a1ede8861db4a4e7e404038f86229a
                80e184fe3d7ac24a2bb97146db09e2014d7f665a202edbb8879
                3569f47edd5d13903913c89bdb2f64dac267307dd2db2aace86
                fe881de213094de8bab534ba01359ad449aa6500de2064ecf29
                af5b3b86c96883ed2579ebd703a97c3e982747e2c4213c6af9f
                b78cadd8168b007f79c9b3abc58c83e487ace180e1fb41334bd
                b1ce9ed54be7eaaa52613c8dd2280a87c94e94f237377a811a4
                40ce59dd98ea59878f1496e8bd0f1b842a5ff1e9368172fbe2c
                800fa52bd6014d2065c6ccf2a1382fa5ca3097696a1a69a759b
                daa4f529a41b70681c9aeddb1488aab7c10e290a0f353ea1400
                4154f4b7c23baf6ed314d2b84a7c760b3df187b5b1470700aae
                1eb3ea84d3faf246411e282ed5d40790a1a1fc67facf4ffffd8
                cc6a8cceda432ad04a454bba7d0247b6042e5be5ab2445d5b73
                0ece63c2b336fcae8232db3794d67e0ab3e98e45aebbe634e42
                c3be695676ec04fd8b013445bb0599a04d43fa26cb4405db6be
                c6188c8cc94dacfc435ee64e3356b97d45125520964d30772b5
                d87fc702ce02fa137f2b4c4fcc12e852fc746715d95023903cb
                3a7e3c2eae8196443ef3b843b979bc29ed63b31d219349a1f21
                b7328c3dfce4c6362c96f0dafd01f081515232700d00d00f7fe
                a78f47342e52641ad6413d227895c49b7eded1adb3809aeb7ca
                d24bf122269e39d7ae9e35da8f193092d2dd284e88b5bd5cfae
                f220b6ac9245a063676d3f9d0d3b844d6164fa23dd7cd8c60f8
                0fc5b5e3454ed7748c65b4cf3db68384529251cd68e2dbdb302
                0e8d73e212f057f2fbb146a845af750fc2fe2a7e26f2e47dbf0
                c2968712074ae8534c356728f04ecb409f3bf877d3fda4ab6cc
                03ef31cd88d3804c75fcbd3ade2e41e99d0e0400c563187cb0a
                d529a1341d48e54d2f5aa141e925fe47cc85329490de157d7cb
                d77c9216fdfe4e8dc03c3b29966d08237a9db8222fe4bfd74b9
                2d221d80a4aaf59
   shared_secret = 0e5a2eb3ae0f3af82978e6a71b5e2a0830850af49d877a0d
                   eec5144061ce44f0

   seed = 0808080808080808080808080808080808080808080808080808080
          8080808
   randomness = 6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c
                6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6c6
                c6c6c6c
   encapsulation_key = 438844d7cbc33abcc0c58337f8e8c084c0795812ba66
                       03a9c64bb47c84acbfd95c148414fe5410427b4f04b1
                       c6b96cbd24958fc7e33387c22dcec51ea94c6c551688
                       ee2981a5e8cacec65748359fcab62adf51bad4338f34
                       b86568b679530cbbf42b475c2909cff88ab126583d80
                       495f05a410f27b6fc3c895d492e3175c8973a18ea53f
                       88a99ad2464a4e19c4caf5a035d77e7f173aa9e4c09f
                       7b595cf5b69af91931d5a58edc9c7dc92ce2347f2537
                       166879cf353c2ec22609a3c3789f80857b207ce860ca
                       cff65b504b8795993a2305cbd9e26b14d36b9d24bfa8
```

22b0a83643cd8a09f1a22a2a923081083afab30f09b0
85f55571de75aefae2939a387343fa602255b4ed9392
b633c2945807eec74f0b212d0e685ae5075f775b0941
1a96ffea4d9a091d20c5200b481265150ebda2016bcb
3064b08c2c929c0992c338bb58d45724fd2799df7542
8f7ab6ffb2785de7b66ad0c01033807e8741ba8731fe
f560e9566359720081a39d8615aaf99bb4dbf335f648
b4dcf3991223235ecc1da6460886657e3be2c065c3cc
51f30393f42c9baa84d4cc4d0d872512ab42e363acba
1594d4769190c444094891c975c74d0baa484b622dc4
8538264837c3855d00c6f6026fa29106c3669e822b2d
719b4c41e550229a145189cf2836594356b0bb9b7a95
d69e22c867f314753e8c589be21268a94cfff9506f11
12eff38494e6742272a0564959202164354692075 9b2
c96570dbe05345c14cd4d6b112506f92e99948952442
fca689c87fa003cd24d2857377668668c1eadc8584bc
cce5517e605b0730a23e46055e177503c71b44fda564
89f10a2051730757caded74932f673f30483ca10c633
8ca0efc509b6486bbe33b857b746d8229a14e62f8370
bd58c1b0c163a8ffb5411946cfaada15faba918e24cd
16d40fdff6b66f8627dddb2c6c3c2b43f48a42986671
624a2c8290d9091c9f05cfb63c4d26114cbb6bc8a96c
4dd5b77c83c2ba88810bfb346eec477ccf84aecbd4a3
4891074b331d1cf7b9bb8779a3372d7db423ef79cf73
4b8bc493bb52ea94536533bab89480ec86eb83214b5c
1e77702124b4bb8ff2c71f976d567cce51245d6ff22b
1df00bb920b42a0532951371f3c39fed7cd95343f47
923a41e6496d938190665eb49b80aed185281ace2191
c7c1c7ca8a808f5518b8884984660b8c8477bcbb178a
b7f87a0f572436c1c19bc7a731e6a03495422823acb6
2861777944999180460c1d6573205779cbb3962bb779
aeea3c9f5d821befd1b6f8f65504d868d1916794a05a
bd53b51468b9856130c6c4b81cab8ec393652aec06e7
603445b83c06458e51e04bac3cc0a3450d061735be15
4b7e19299fc70a5fd72e11658e2cf62ff696163e7cc3
8406ca8fbac345b06c8a27c08f7924b53562e8472ccb
c1081bf36bc9fc3e00dc005969691c3acc5a01ada084
b5b7888cd03bcaf9da868bc400483755481631d5766a
1b873a55d33811b584fb0280973560c5c4a75db01d5d
a4bc21b08bb0005013ca8972831c17209cbd4222a1f7
5527949ef30c3f1f7873c4e792f7454fa6a9173fc67c
b66c0878998563328237 2038b881bf055862470a4703
69b00049196682cd8827a691c60e046909048a850472
51b7fb2a0f0ac9ed271ffde282db57480c10bcd74890
cdf91f7790b0fda7608b6c612ce5c18d30452852c3cb
370642621fef811530061cc0f612fcab47ab97a43376
74972c4e9542332978499f234f64d8788504031a579a
b6a02add3c40366b52388368a60ca0df9a0ade438c23

```
                    accb062bc586d428582a752cd4767fda155c812c0399
                    574606cf90c009e0a7944dccbe887aa596864a713556
                    26018105f705d0e05075362884b2c2ff929d0fa05fb4
                    771bad5b73b5b8a9695174801087d9f64e17a026c96c
                    b608675fb8174e74226e120c2199dc2eff362a45206b
                    1b4a26ab511aa875ac8df8bea946c305023812ecc888
                    227759b03aa2c260fc7b965657c2bed35ce3f82f10a2
                    b863f65467291d4b996c2f30af4c5469292782353970
                    e4549e180a94fdfb24a0636384e02b5a861252ec5a1a
                    cb3b0396bfdd241e3522a49f526fdf9a5647d7cd7cf2
                    7bfd3796f138616cc3a5d163071a63a83da2a8fbd7c0
                    f020565e46b3c6182fc21462abb7605f387ccaa15c5a
                    d115d428a8f75faf9577f754b4872cc55aa3f67683ac
                    6830636f25cf04c77e9f4dd5fa8af50d958361b98902
                    ee569f7c67efdd4b15aef42b7b018872346ae3d0d4f2
                    af556401d3142b85233cf6f6a118b60c9317edf49288
                    1d1f2b651e057f202f662a54f7044ffa61b781f8c35f
                    ff2e86267ff0b8525ac13e4bf4a12e
   decapsulation_key = 0808080808080808080808080808080808080808080808
                    0808080080808080808
   decapsulation_key_pq = 08f68b3e03568d1e99c5c2167cf41dba4a6077557
                      4d21a9c79414bf1fb67a547e91d5f36267ef061cf
                      681cbe41b9cb15c17ee52a3579a51c20397ba3bda
                      5ea72
   decapsulation_key_t = 76a574362e7f03f27cc6f4288e046d753df47649c0
                     07741468fc4d252745150b91c380caeaecaf12cb03
                     c320bd3463bd
   ciphertext = 4aaedad0befe99ae3e9d21c745135279dbafa79e9935f328ecb
                b3258c6dc66557da90d2ada312b9b5b113b47f1dab9de69f14e
                6421d336d525bd4098288854d6ea2e449af19d702cb5f22ce8d
                6da820b4cb76a2e5b93ab390706dbc7570a9dc6f103928db508
                227b37c32a00ca4b25623396ffbdbf95703203ebfef5b07a450
                591792fd0adbb1277655fbc908ba0952758b74610f8152d8e59
                bb74e2f76dcd29a530c01aa3ee35689d16ba790d3b84dc4eab5
                2d60388eaa807a06be5d86a473fb55eff6c70e73edc73f8b6c0
                ec7e6b472d5a3b82f1eb6ec508f1c12d58f42f870af9173da75
                55b080be6a53233c0a6954d7f5501b0c522c69bb5853c6147ec
                2cc74e5a333d641fa130a63373497f844c16113aa7a14d8edb0
                097137710730d03ab6950a4a61d6659991bc70b9703f2ee670e
                5bb1986a9471f9c211a0ec8b38405a487b6ea425b598478caca
                583e3b6f968b73a72d34a81af674009c8a9c294269869c6d695
                982d4ba517646cd045db6e33d89bc91724608d5c7ee67e24e06
                13ed0c1c00e4eef02122994d6197b7da3fcd3590d42365d6b13
                8f09e1c61eed7f73d630a96f5a392c3033cd02d823b8dde7d52
                e7444bdb91f76dbb4dd0c8c9c081dea1c81cfe138d15d06af32
                136668658b9118a065d4203911c1ed7a3ccf5f02355de1191ff
                db02de1d0b3c1585f0ab81aacd405ec25b62f116b9a951f57d7
                80a4156143cb813edad47d41408a89daa1edd5a0f4d4a80598a
```

```
                739f6ef0a16e8b502b9408603ce5615b632b1aa8d0940b7f040
                29b06ff019271f90452667c054813afdce2c5a10583913b37c0
                1800dbb8cb4c8f7fa182079a2ac609c5209e8f9727f4edd0825
                e8ddbbb696f3ab76621dbef8f6df51a34cb9179ad3cb6de31a4
                552206ed8089c69439fdf5137012158d33bc97cd8185e94c24c
                c7303fcc9e801df3fb3b8f4fe268bdc50137cc1eaa1723bed66
                6d0aae9e452e166a356d04c84c65d19f8ebddc51bba49c85866
                dce77a4f9193bf6b238f1ea886ffc44db55e0458391f9a252d1
                c20ed1921ed378b1e246a490b6221ea73db863c9bd04090a557
                481a24fdd75b12799d042a0e4c929e5570d41d7f562e90a314d
                3044daceee81cffa37ab5cb1083559bb321948437d9a5caff45
                62302f22f77754f834379b72e461958cf62bec4f1bcee846501
                b08aba0a11ca10d41dfcb04267ecfa0372896ba35acf9983b96
                c20fa5a0b9b2a824af911a0678c0cb6110a2ce520ee10bf32ef
                d72b1487b48ed9689d02def24567bcfdb76cdb17d31f540e715
                424b2a37c5c6ee44eb951737e3718ee01b95a9eef71b7d73d7d
                101a3e53c9073d360fa5bb340a3e14a06cb875c66f22c6791fd
                3ad7f720069874c77d7ccac01f13d870acd3055f0fce01a8529
                e8c058e1fba29dc2387927be0c8e95de7c70fd945ddb289288b
                9d7d7aa5be60504ec16c8392984784715dad292c1887d7cbb28
                09dfd45431c820fb28085036d4c903da826c26a141645fdd183
                4f6ea5fa9d87023129cc6467b25902d9fdd441c7a60ffeb5280
                f97a05e28bbe4e8702b101ab501cf3a186519979dd7681363a8
                77dea4aa16fcedfa55893fd69e0f4cf7be703921805e0eb6047
                109808d174473ebeca08f795537a8621a5cb555f2b63e763d2e
                7cdebe9da4cac208f737d1c86732aee5bcc40b6b469e4c5a00b
                5f82494ac09626beeb21925719d07cb6bc65c2d00bf18f27040
                3db32f151818dd8a2c3f9712a02691fcd3f82e8a1c8f7c90c5d
                de688a3135448025c7cebc2046fedd6e920075eb2debb5804cc
                aed5b66955b4c4606d7d52bcbf9937e21a7bc2f35d4bd6f9898
                6127cbb6ce68f27b88a4d0b6c3e7f97216bf500af9ab3654c27
                8e95dee865750937662ead1d807388acc004cfb4f737c32c4ab
                8719e15473d128f5ae4b4ca4c0b3348d811c348e9d4fd64e743
                50f4eac0de6dc3ad94793e3ffeea1abf89ef586b13f93bbf176
                d5d6e99df043a118a183eee4d66069c18d24f5a27c1777b2e30
                501d64658c5bb490259b15ad7c1d07a5bc9a73f6fe1f9176a36
                22f207eb941be7c736bfaf356ab4280c29f9735cdc6d37f489c
                9dfe1fbbcb3a67206aa22d221214603d4a9bb9f32e93b01b759
                5cee7156d939a0b63df1d89d4a603594314127f7c751bc28215
                ed5963045ba3e186e429cb08165fec5fab493a7c890e29279a3
                265b9055cf605508f1681a3f904e68f85580d097533d64a56cf
                c76d712e42729b87f4c28353d317eb8c157e2a920e2f350b473
                87f86e8dc86a14e6e4cfbbc73f8c02d6fef675f6e74605203b6
                70fe50f33a7b8bc670cbb6d0ced5ada15cf8e436e0e1a55c9eb
                c67ce0a8fb93754
   shared_secret = 3fa279b00ab2798d2d70a2578ea2c76539cbea4bd86d1aa0
                   9e92bf0cc40e6626
```

```
   seed = 0909090909090909090909090909090909090909090909090909090
          9090909
   randomness = 6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d
                6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6d6
                d6d6d6d
   encapsulation_key = 831a957ee82bba8605154b0aab3c3d4b43b304050a95
                       8a78a4f983ea4505b041652b5c26c0a11b74881a9512
                       119a4678d53641ad16819b85901111530d0308ad6a0b
                       7b419ca6d001edb967ceea6faba594ce482a1a177ff8
                       f2b01453add28a96dfd2358ec6ca7cda8f2c1308f4b6
                       cd1596a14c326e51e527b1c3b2e99c8bb4a676306340
                       89a5b1469977b440ccfe2a49545716da34b55eb73d95
                       59a36d828ff936a71fe223abe7cb646b3b3955acd0e1
                       9ef2bb5d9e847cd3c7bcb18952e567b155e67c0b3994
                       8646ccc2547b43f1bf05451f90abb63bca0d0517bbc2
                       3aa6783552a915051222824f3739eba438ad1278e1a6
                       778505456fe86a8d280cd0f88dd52c06ffb28bfdd618
                       25d626f946c531e63364c6a4a5162bf5eb6628e8c017
                       40996573215b20ad80964ecbdca13ad2311a2046da84
                       c7cd2412faccc736f5998c5723c482120c2662244aa0
                       c5847dcbb7652907c36571ab3d4b93618973d2d066fb
                       1bba9b8587c9e017ac737c1cc40872e11e0ee55db5d4
                       bde221226df7822022b7eb0b80ca0428b6b0b94bc0bd
                       15a2873f3058425c0d7b2665c464499cba8a8163a088
                       01269712b76fe36a46c1250ba113f5596d782bc0315a
                       5dd45c2b77674238b59d0b0347498b1a11b5a7fa9486
                       4b14bf5fc20d762232b98b5b70797e411444df938dd5
                       2114575c3bc9b01f6812396ba69b6e89b33a304d3cf2
                       35d70582ed55ac9f043103b71b3b9845a7684057f794
                       00f954f4087b86481b9b80ce1d37972f438954d37a03
                       bb5b9a35277af5911d91b6611858460354a4945feb17
                       56a9d08e932887d02c32b6284e86829a6554a5916a64
                       2da448f97543fb159aa108661b30cd34d35c6c3358b8
                       88490dc17ff3e731239a69e4916e48993569989a2e55
                       575d29c9bfa501beb674a1fb5cbd5b4e4916bd389c29
                       96a761e123147f385f18fa81df417178c58a1826233b
                       8a9825c1bc3143069ea0404d468994669b95bb5ac27c
                       41849a8ce1352be857a2200970ef46aa2be28e5568b0
                       71012775f294fa6a8d2be12d6a8227ae719b47346b0e
                       b268afa43e8acb90a114a4a4b2ba7711122048333eea
                       a5a4141a4682a0220b5ec7369e2c64307d4173fa8071
                       5d69b3cd4835adb5072796891a6780b930540c5779f2
                       3b00f6b2964506c4d79a50b387080a5a1608a0973707
                       1f2432aca003bccfb56df1689433b4532ddba87d8078
                       428bc128a6609f35a917022936c4ae5085c040149620
                       904f1a1571ce42b98b335cc2814b25fb90f0c3991808
                       ab61154c12864922dc4acf75a74304174a68795f858d
```

```
                        4a8a3bd106bdcbfb3d87b6a6b4f93992b39ac2f131f7
                        8998e069b7da46c11b0a99d5b5255146412b15491e1b
                        8ec8d01e61161b54d9cf01ec2f84cba60d986d91229f
                        09c42400d5203c3c5164abbed8064f79d4cfa491c940
                        982b2dc2bba8493975227aa85145334b470e88900447
                        aa4e042fc0b06655f9668167aa93c0c8ab8018491821
                        516cb4085b1148d912c4668d1c72076c311142b80e7f
                        112c466c3e19f72418e03adbb0c8bbb885306294e704
                        35d4546f8c6095b3b591120c45b759c9a7d155328b1a
                        09b424aaa8b528484b48e689a8d54f86e383a8c25603
                        707c3e174001ea2ac78ba008f81bed4a8963573eb06c
                        1f4f19091117a9f4211b107b2c4c05220ac2bcca6763
                        4b7cac8f51bb6a258b706c6cb07c5b8bd48b12877b74
                        3877c10b52d4363f03b21413365aee80c1f5f18380f5
                        b6afe5a2e911542af0022cb3c95d3a8b57b7c1fdb74f
                        3b51c6f2e8a4aab20918fc588928468d498ab7c749b5
                        4140ed26288bb804a9637482f56ce0a69706fc89ecdb
                        4cf3ab6a30f7c595a18076da50a8131d240049ac9996
                        30b0af01b8ad12350e132a7b9d81c3d5082b68e61f24
                        2a224a42553c3886e0261d115b8ae11705959c20c1c6
                        2611ba2c6b30622afa91a33a216c65539823621e84bb
                        897c2133c4c5fb01cde505a7d114466206a23fac8938
                        613fecb3c9609796df50caa701081ee76bf63893435a
                        8101e03f0c135824e9b488962f2356a15b0427c4e41f
                        2ba9be16056d79844b708c4140c3232915c06c83be4b
                        a83f9132b279d1bb8b0c9d5fd61f6af29252dc2401f1
                        7b830b5538723c046629cc913209cc9ebf24aee9083a
                        e883a98d04b27be8164801135f0cc37c2220295109f6
                        068201b721b549a15e0be0377089050bb02aaecefa9f
                        e5c3207eaa050436a60b2e64e53c71ee75186bab64a4
                        8919279b2b54453125fb735c0ca68e6292f6d9f4943a
                        06c086ea570fd604cc99b906e282a752e1681bea526b
                        a45e6c6d90edfcd90fb8a1c3a7b5d6d91cbf751fcf80
                        59d1ab34a422cd5ae881969f40e065
   decapsulation_key = 0909090909090909090909090909090909090909090909
                        09090909090909090909
   decapsulation_key_pq = e4c190b41d18fe33b5710819eb4a962a2a6af9cd2
                           663d9766a4896481dcfc8b89687089a9797cf2f69
                           d058df1f690441dbccf3faa91ead65b8d4dfadd6a
                           a4912
   decapsulation_key_t = 00ee28df5d8544c9ea9a79badcf995f43af90ef255
                          b64b6ca0c8d194528f71529193c88c09fc62a4b432
                          ef6314e1222c
   ciphertext = aacb765d071dd63516706b226b20856e386e89bc8225d8b9235
                ea9e796ba9ab270f7376f22b2a1433d533ddca26a95a68597ba
                80fab3af861fa45be6e1bb58e1564ef6159b9f7c3c30588020e
                fb44fa2b2769ab163fb969cdc80714075adc8d71433117ce682
                52c6dffbb5294b0977a1eecc27393a3f33c8f818b0ac1f229f8
```

2e1f50a7510b164402cc017df95be6715544ef5b0780208a673
77d5fc06e505a122d188d649074029634b69f9a62d2b6abc3e7
d28bfb80cdb09336bcba0fade46662a5e62f43fee55a3a01e9c
9cc86b2390de4bce484b04ccb0dfe644c66de375a0e4c082409
062a4d030a3c1fa919985016a3f30a8c37b064579b3223396e1
a20be912426d754a5b6e3313c78964b96d6bb55fdee97ca8855
3c31dce9229138fac659f0d12edfe8853383c4b30001bb24e52
16c2c437eac7c0bbaf68a03a44619b3bf9e009503631c98b2a8
1544780d3f376f09a0574f236772d59517918c6d8c2a7ed0a09
497393dfa23e178aeb7ac9ff92b3843da99fa6d4a6e9e6c2ed4
f2be3566104683a4965538356456614504f825eceb488e625f3
c9384106f50b9ce88b0f310ac30922298f53b1631159bfc069f
26de61b40577f6f42b517b76bc0dbe5781de35f1950b6309236
d8b0cc8f53430726c084c01af7d670c27b34d77086324a849d2
60ca00a4f2faa4e1cc65f34680e3b96993c1ed13a93d2107e5b
b757085e55c27a2a9830db6f3ded55916a18b074673e3f97fe3
7db600c75897a1e6bb1c4cb3874e25793493cca4194b97103d8
f75a1510452e2401bd27982db0269df85fba994f0b011e405b7
10e655a007f6e73f14c3191438a39c96f8304e237f7ae3c7e7a
b239f8b313e7c1b9d757bd87dd19ecb91e1db5cc3e827490f8f
1be70fa51eecfbc4e42a84f4ec8680b8f6b25d247e131ceef22
758d9a34314aa681fd0a9de4139f9931acbe7ebbcd2bf576e9e
87d2ea9287e96f4e54098eb263d48024aeabdf056739450139b
159c3885c8c05caba47038e044155792dad58acff4eb601a82e
ddb6dcb351f00522218fbc5979d6c7f3bab9d3cb407540c10cd
593e856d91e543eadd0696808698bfae3c14baf2d43c5af4f8d
a9c9b8e7c3ddc88b8f5761576c039fa381da89e58966f5bbe00
b6d8549f8f3b611f8dc736aca21bb3e2666953c96b43b037026
125bde594273d2cc409ef3d3ab1882ae4ee1b745f186136046b
57df284cc2ccf05c42b9eb6ccb402b26cf218a423803ad8d9f9
089cb27bc0d7e3c1c9b21d6cdd8c3fa672b7b1d9eabe8be1ddf
59b34fa7394296f727e48f85cef69ae1eddd76e085232f141cd
9809d5ffbbb8c43f571aaa8ea2f51350289d37db5b66b0ff5ab
5c14e05756369ba307be2f25c63b64768ee5ecc5d2060425674
164eab8daa03da7348034cd7a88cf3ad6131acab875ab9f3a5c
d6cb66c99297abd477c699e30675cf5d51c1baa8c1900633e4a
cdd6214968c3134af30125d5afeb8bb37e0d9cd6dd92d5399c4
c319a35c83eb66c91ce90b2c4813063d420b06cd3c91355c744
e5f854b7907696953a9af76ea8fa6ff4ceedb46106303a5e59e
00c3824d66083e93f27a0a7caee64fead39528c716b0b984009
95038ec40bb880635dd2b143426ff52d0412a1a911928f6ac98
ba8d38bd4099f9e01265a1debc25ae47780d0a5d51db0c641f9
52dbd85498a40db10a8051f48b537cde45a29da4cca985631f2
445be724ee4039baae8ac7cb3d0527402e0a7c8bf60e26f537a
ae00b7f8236466bf131dfec2e3c3a09f12a45c77d8b1eff124e
33bde64b02864b73464331a654b2bfb3d6e5c9796e120df8502
015047089257f549b8d79af8d05b0f18acc0141a352e6d07119
532c4eafdbe826e13ad11a7ff57e542ef398b155ed325d23920

```
                6c71cb1ee052be6a7d63efedeb5f0f32c88492f330b2e20303d
                55337723457c1c9b72ca110f628ab3751c99e467b977a32c4cd
                c5904a53aad0ec46e2f4dea22c14493fa5a35ec9eefcf8134f1
                ecf2424eeaae71509279b59114056ec4f0e19268e098d5285aa
                a05dbc56669fdd7abddc7ecfb62e357abe51b507cbf2bab79a8
                f447e81632d185d989f2cd67fb83323f6f5f59eefc63359d166
                8a4cb86b77faaad7aa487b7b1726418fa872869b0279c545880
                75a59f7952aba6836748c28fa0419a3fe3e9e9e0bc38cf09317
                92e6cbc6c9f8c87f5d5ee6924048a871dea160c961093cb257c
                1e1c3c4f7ee0f37304caba13d3eb6f03539c7b92a2eab2f4ac9
                bc96ea7eced9db4885ef5a79517bd153037c7a5b719a2e71721
                e95e8635464576e833114ded11f2304b549ed682dd8e1ff40f9
                3e5dfa49ce9b19e
   shared_secret = 3722070676e89cc0c97613a0207dbd89222219920caf5e9a
                   8c6aa9d1e1a42bd5
```

Acknowledgments

Thanks to Chris Wood and Britta Hale for contributions to early versions of this document. Thanks to Filippo Valsorda for the ASCII art labels for the non-X-Wing hybrid KEMs. Thanks to Mike Ounsworth, Bas Westerbaan, and Chris Patton for independent validation of the test vectors.

Authors' Addresses

Deirdre Connolly
SandboxAQ
Email: durumcrustulum@gmail.com

Richard Barnes
Cisco
Email: rlb@ipv.sx