HPKE Publication, Kept Efficient
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

R. Barnes
Cisco
D. Connolly
Selkie Cryptography

2 March 2026

Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE
draft-ietf-hpke-pq-04

Abstract

Updating key exchange and public-key encryption protocols to resist attack by quantum computers is a high priority given the possibility of "harvest now, decrypt later" attacks. Hybrid Public Key Encryption (HPKE) is a widely-used public key encryption scheme based on combining a Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) scheme. In this document, we define KEM algorithms for HPKE based on both post-quantum KEMs and hybrid constructions of post-quantum KEMs with traditional KEMs, as well as a KDF based on SHA-3 that is suitable for use with these KEMs. When used with these algorithms, HPKE is resilient with respect to attacks by a quantum computer.

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://hpkewg.github.io/hpke-pq/draft-barnes-hpke-pq.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-hpke-pq/.

Discussion of this document takes place on the HPKE Publication, Kept Efficient mailing list (mailto:hpke@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/hpke. Subscribe at https://www.ietf.org/mailman/listinfo/hpke/.

Source for this draft and an issue tracker can be found at https://github.com/hpkewg/hpke-pq.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

A cryptographically relevant quantum computer may or may not exist as of this writing. The conventional wisdom, however, is that if one does not already, then it likely will within the lifetime of information that is cryptographically protected today. Such a computer would have the ability to infer decapsulation keys from encapsulation keys used for traditional KEMs, e.g., KEMs based on Diffie-Hellman over finite fields or elliptic curves. And it would be able to do this not just for data encrypted after the creation of the computer, but also for any information observed by the attacker previously, and stored for later decryption. This is the so-called "harvest now, decrypt later" attack.

It is thus a high priority for many organizations right now to migrate key exchange technologies to use "post-quantum" (PQ) algorithms, which are resistant to attack by a quantum computer [PQCE]. Since these PQ algorithms are relatively new, there is also interest in hybrid constructions combining PQ algorithms with traditional KEMs, so that if the PQ algorithm fails, then the traditional algorithm will still provide security, at least against classical attacks.

Hybrid Public Key Encryption (HPKE) is a widely-used public key encryption scheme based on combining a Key Encapsulation Mechanism (KEM), a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) scheme [HPKE]. It is the foundation of the Messaging Layer Security (MLS) protocol, the Oblivious HTTP protocol, and the TLS Encrypted ClientHello extension [RFC9420] [RFC9458] [TLS-ECH].

This document defines a collection of PQ and post-quantum/traditional (PQ/T) KEM algorithms for HPKE, which allows HPKE to provide post-quantum security, as discussed in Section 7:

* ML-KEM-512

* ML-KEM-768

* ML-KEM-1024

* X25519 + ML-KEM-768

* P-256 + ML-KEM-768

* P-384 + ML-KEM-1024

ML-KEM, X25519, and P-256/P-384 are defined in [FIPS203], [RFC7748], and [FIPS186], respectively.

This selection of KEM algorithms was chosen to provide a reasonably consolidated set of algorithms (in the interest of broad interoperability), while still allowing HPKE users flexibility along a few axes:

* Pure PQ vs. PQ/T hybrid

* CFRG-defined vs. NIST-defined elliptic curves

* Different security levels (NIST category 3 vs. category 5)

We also define HPKE KDF algorithms based on the SHA-3 family of hash functions. SHA-3 is used internally to ML-KEM, and so it could be convenient for HPKE users using the KEM algorithms in this document to rely solely on SHA-3.

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 generally use the terminology defined in the HPKE specification [HPKE].

There are two meanings of "hybrid" in this document. In the context of "hybrid public key encryption", it refers to the combination of an asymmetric KEM operation and a symmetric AEAD operation. In the context of "PQ/T hybrid", refers to the combination of PQ and traditional KEMs. For clarity, we always use "HPKE" for the former, and "PQ/T hybrid" for the latter.

3. ML-KEM

The NIST Module-Lattice-Based Key-Encapsulation Mechanism is defined in [FIPS203]. In this section, we define how to implement the HPKE KEM interface using ML-KEM.

The HPKE DeriveKeyPair function uses the SHAKE256 KDF (see Section 5) to derive an ML-KEM decapsulation key in the 64-byte seed format, then uses the function ML-KEM.KeyGen_internal from [FIPS203] to compute the corresponding encapsulation key.

```
def expandDecapsKey(dk):
    d = dk[:32]
    z = dk[32:]
    (ek, expanded_dk) = ML-KEM.KeyGen_internal(d, z)
    return (expanded_dk, ek)

def DeriveKeyPair(ikm):
    dk = SHAKE256.LabeledDerive(ikm, "DeriveKeyPair", "", 64)
    (_expanded_dk, ek) = expandDecapsKey(dk)
    return (dk, ek)
```

As discussed in Section 4.4 of [HPKE], the value of suite_id used within LabeledDerive identifies the KEM in use:

* ML-KEM-512: KEM\x00\x40 (hex: 4b454d0040)

* ML-KEM-768: KEM\x00\x41 (hex: 4b454d0041)

* ML-KEM-1024: KEM\x00\x42 (hex: 4b454d0042)

The GenerateKeyPair function simply calls ML-KEM.KeyGen_internal with a pseudorandom dk value. As long as the bytes supplied by random meet the randomness requirements of [FIPS203], this corresponds to the ML-KEM.KeyGen function, with the distinction that the decapsulation key is returned in seed format rather than the expanded form returned by ML-KEM.KeyGen.

```
def GenerateKeyPair():
    dk = random(64)
    (_expanded_dk, ek) = expandDecapsKey(dk)
    return (dk, ek)
```

The SerializePublicKey, DeserializePublicKey, SerializePrivateKey, and DeserializePrivateKey functions are both the identity function, since the ML-KEM already uses fixed-length byte strings for public encapsulation keys. The length of the byte string is determined by the ML-KEM parameter set in use.

The Encap function corresponds to the function ML-KEM.Encaps in [FIPS203], where an ML-KEM encapsulation key check failure causes an HPKE EncapError.

The Decap function corresponds to the function ML-KEM.Decaps in [FIPS203], where any of an ML-KEM ciphertext check failure, decapsulation key check failure, or hash check failure causes an HPKE DecapError. To be explicit, we derive the expanded decapsulation key from the 64-byte seed format and invoke ML-KEM.Decaps with it:

```
def Decap(enc, skR):
    (expanded_dk, _ek) = expandDecapsKey(skR)
    return ML-KEM.Decaps(expanded_dk, enc)
```

The constants Nsecret and Nsk are always 32 and 64, respectively. The constants Nenc and Npk depend on the ML-KEM parameter set in use; they are specified in Table 2.

> | Note: While this document defines an HPKE KEM for ML-KEM-512 in the interest of completeness, implementors should generally prefer ML-KEM-768 or ML-KEM-1024, or the PQ/T hybrids described in Section 4. According to current cryptanalysis, ML-KEM-512 provides security compatible with a 128-bit security level (or NIST security category 1). Given the relative novelty of ML-

> | KEM, however, there is some concern that new cryptanalysis
> | might reduce the security level of ML-KEM-512. Use of ML-
> | KEM-768 or ML-KEM-1024 acts as a hedge against cryptanalysis of
> | ML-KEM that removes some bits of security but is not
> | catastrophic, at a modest performance penalty.

4. Hybrid KEMs with ECDH and ML-KEM

[CONCRETE] defines a collection of concrete PQ/T hybrid KEMs. These KEMs combine ML-KEM with a traditional ECDH group:

MLKEM768-P256: ML-KEM-768 and P-256
MLKEM768-X25519: ML-KEM-768 and X25519
MLKEM1024-P384: ML-KEM-1024 and P-384

These KEMs satisfy the KEM interface defined in [GENERIC]. This interface maps to the KEM interface in [HPKE] in the following way:

* The HPKE DeriveKeyPair function uses the SHAKE256 KDF (see Section 5) to derive a 32-byte seed for the hybrid KEM, then uses the function DeriveKeyPair from [GENERIC] to compute the key pair for the hybrid KEM. The input to this function SHOULD be at least 32 bytes long.

```
def DeriveKeyPair(ikm):
    seed = SHAKE256.LabeledDerive(ikm, "DeriveKeyPair", "", 32)
    return KEM.DeriveKeyPair(seed)
```

* The GenerateKeyPair, Encap, and Decap algorithms are identical.

* The SerializePublicKey, DeserializePublicKey, SerializePrivateKey, and DeserializePrivateKey algorithms are the identity, since encapsulation and decapsulation keys are already fixed-length byte strings.

* The constants map as follows:

  - Nsecret = Nss

  - Nenc = Nct

  - Npk = Nek

  - Nsk = Ndk

As discussed in [HPKE], the value of suite_id used within LabeledDerive identifies the KEM in use:

* MLKEM768-P256: KEM\x00\x50 (hex: 4b454d0050)

* MLKEM768-X25519: KEM\x64\x7a (hex: 4b454d647a)

* MLKEM1024-P384: KEM\x00\x51 (hex: 4b454d0051)

5. Single-Stage KDFs

This section defines HPKE KDFs for eXtendable Output Functions (XOF) based on Keccak. SHAKE is defined as part of the SHA-3 specification [FIPS202]. The related TurboSHAKE XOFs are defined in [I-D.irtf-cfrg-kangarootwelve].

The Derive() function for SHAKE is as follows, where <SIZE> is either 128 or 256:

```
def SHAKE<SIZE>.Derive(ikm, L):
    return SHAKE<SIZE>(M = ikm, d = 8*L)
```

The Derive() function for TurboSHAKE is as follows, where <SIZE> is either 128 or 256:

```
def TurboSHAKE<SIZE>.Derive(ikm, L):
    return TurboSHAKE<SIZE>(M = ikm, D = 0x1f, L)
```

The Nh values for the KDFs defined in this section are listed in Table 1.

Value	KDF	Nh	Two-Stage	Reference
0x0010	SHAKE128	32	N	RFC XXXX
0x0011	SHAKE256	64	N	RFC XXXX
0x0012	TurboSHAKE128	32	N	RFC XXXX
0x0013	TurboSHAKE256	64	N	RFC XXXX

Table 1: Single-Stage KDF IDs

[[RFC EDITOR: Please change "XXXX" above to the RFC number assigned to this document.]]

6. Selection of AEAD Algorithms

As discussed in Section 2.1 of [PQCE], the advent of quantum computers does not necessarily require changes in the AEAD algorithms used in HPKE. However, some compliance regimes call for the use of AEAD algorithms with longer key lengths, for example, the AES-256-GCM or ChaCha20Poly1305 algorithms registered for HPKE instead of AES-128-GCM.

7. Security Considerations

As discussed in the HPKE Security Considerations, HPKE is an IND-CCA2 secure public-key encryption scheme if the KEM it uses is IND-CCA secure. It follows that HPKE is IND-CCA2 secure against a quantum attacker if it uses a KEM that provides IND-CCA security against a quantum attacker, i.e., a PQ KEM. The KEM algorithms defined in this document provide this level of security. ML-KEM itself is IND-CCA secure, and the IND-CCA security of the hybrid constructions used in this document is established in [CONCRETE].

Another security property that is salient in some use cases is "key binding". In [CDM23], these notions are referred to with the shorthand X-BIND-P-Q. The most salient for protocol design provide assurances similar to those provided by transcript hashing in protocols like TLS:

LEAK-BIND-K-PK: If the sender and receiver have the same key (K, shared_secret above), then there is only one encapsulation key (PK, pk) that could have produced it, even if the decapsulation key is leaked to an attacker after the encryption has been done.

LEAK-BIND-K-CT: If the sender and receiver have the same key (K, shared_secret above), then there is only one KEM ciphertext (CT, enc) that could have produced it, even if the decapsulation key is leaked to an attacker after the encryption has been done.

DHKEM and ML-KEM meet these properties, as shown in [CDM23]. The hybrid KEMs used in this document also provide these properties, as discussed in [GENERIC].

7.1. PQ Hybrid vs. Pure PQ

Assuming that ML-KEM is secure, either the PQ/T hybrid KEMs defined in Section 4 or the pure PQ KEMs defined in Section 3 provide security against a quantum attacker. Hybrid KEMs can be used to provide security against a non-quantum attacker in the event of failures with regard to the PQ algorithm, including both implementation flaws as well as new cryptanalysis. See [GENERIC] for

further analysis of hybrid security properties.

7.2. Asymmetric-Key-Authenticated Modes of RFC9180

In the [RFC9180] version of HPKE, KEMs could optionally define the additional functions AuthEncap and AuthDecap. These functions allowed a sender to authenticate the message to the recipient without interaction.

The KEMs defined in this document do not support AuthEncap/AuthDecap and cannot be used to migrate uses of HPKE that rely on this mode. PSK-authenticated HPKE (Section 5.1.2 of [HPKE]) or digital signatures may be suitable alternatives.

8. IANA Considerations

This section requests that IANA perform three actions:

1. Update the entries in HPKE KEM Identifiers registry corresponding to ML-KEM algorithms.

2. Add entries to the HPKE KEM Identifiers registry for the PQ/T hybrid KEMs defined in this document.

3. Add entries to the HPKE KDF Identifiers registry for the SHA-3 KDFs defined in this document.

8.1. Updated ML-KEM KEM Entries

IANA is requested to replace the entries in the HPKE KEM Identifiers registry for values 0x0040, 0x0041, and 0x0042 with the following values:

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0040	ML-KEM-512	32	768	800	64	no	RFCXXXX
0x0041	ML-KEM-768	32	1088	1184	64	no	RFCXXXX
0x0042	ML-KEM-1024	32	1568	1568	64	no	RFCXXXX

Table 2: Updated ML-KEM entries for the HPKE KEM Identifiers table

The only change being made is to update the "Reference" column to refer to this document.

8.2. PQ/T Hybrid KEM Entries

IANA is requested to replace the entry for the value 0x647a and add two entries for values 0x0050 and 0x0051 with the following values:

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0050	MLKEM768-P256	32	1153	1249	32	no	RFCXXXX
0x0051	MLKEM1024-P384	32	1665	1665	32	no	RFCXXXX
0x647a	MLKEM768-X25519	32	1120	1216	32	no	RFCXXXX

Table 3: PQ/T hybrid entries for the HPKE KEM Identifiers table

8.3. SHA-3 KDF Entries

IANA is requested to add the values listed in Table 1 to the HPKE KDF Identifiers registry.

9. References

9.1. Normative References

[CONCRETE] Connolly, D. and R. Barnes, "Concrete Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-concrete-hybrid-kems-02, 6 November 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-concrete-hybrid-kems-02>.

[FIPS186] "Digital Signature Standard (DSS)", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.186-5, February 2023, <https://doi.org/10.6028/nist.fips.186-5>.

[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>.

[GENERIC] Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-09, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-09>.

[HPKE] Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-02, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-02>.

[I-D.irtf-cfrg-kangarootwelve] Viguier, B., Wong, D., Van Assche, G., Dang, Q., and J. Daemen, "KangarooTwelve and TurboSHAKE", Work in Progress, Internet-Draft, draft-irtf-cfrg-kangarootwelve-17, 21 February 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-kangarootwelve-17>.

[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>.

[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>.

9.2. Informative References

[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>.

[PQCE] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/rfc/rfc9180>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

[RFC9458] Thomson, M. and C. A. Wood, "Oblivious HTTP", RFC 9458, DOI 10.17487/RFC9458, January 2024, <https://www.rfc-editor.org/rfc/rfc9458>.

[TestVectors] "HPKE Test Vectors for Post-Quantum Algorithms", 2025, <https://github.com/hpkewg/hpke-pq/blob/main/test-vectors.json>.

[TLS-ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-25, 14 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-25>.

Appendix A. Test Vectors

Each section below contains test vectors for a single selection of HPKE algorithms and contains the following values:

1. Configuration information and private key material: This includes the mode, info string, HPKE ciphersuite identifiers (kem_id, kdf_id, aead_id), and all sender and recipient key material. For each role S or R, (sender and recipient, respectively) key pairs are generated as (skX, pkX) = DeriveKeyPair(ikmX). Each key pair (skX, pkX) is written in its serialized form, where skXm = SerializePrivateKey(skX) and pkXm = SerializePublicKey(pkX). For the PSK mode, the shared PSK and PSK identifier are also included.

2. Context creation intermediate values: This includes the KEM outputs enc and shared_secret used to create the context, as well as the context values key, base_nonce, and exporter_secret.

3. Encryption test vectors: A fixed plaintext message is encrypted using different sequence numbers and AAD values using the context computed in (2). Each test vector lists the sequence number and corresponding nonce computed with base_nonce, the plaintext message pt, AAD aad, and output ciphertext ct.

4. Export test vectors: Several exported values of the same length with differing context parameters are computed using the context computed in (2). Each test vector lists the exporter_context, output length L, and resulting export value.

These test vectors are also available in JSON format at [TestVectors].

A.1. ML-KEM-512, HKDF-SHA256, AES-128-GCM

A.1.1. Base Setup Information

```
mode: 0
kem_id: 64
kdf_id: 1
aead_id: 1
info: 3466363436353230366636653230363132303437373236353633363936313665
      3230353537323665
ikmE: f98936e15de97b6ac920c54f4009166401f882220b8ef2df485f9c077d728ced
ikmR: d7c1c923cee18d6a91cada4526e4d72809749b68ae19fd32fe6c4ec5f82fa947
      2e336e68c54181766e5a978ecdf20d81977b94253a3827f9d9126bc91532bbe5
pkRm: b6a325284237f5fb45261cba99882a94d296a8fc6bb1510ee287704b6757cd15
      638b0901c99b533248210f18325c5cbe34989c62495d3392997023bc0e7c08bf
      70ac50d973c35533aa890fceb80cac5b4f9b63c0bafa041a451fdc3b61cc82ab
      c252a732646e84561fc9233629143363c486d719c21e5a8e62ab4d5b0c17b00b
      d0004147bba55f9e865716a157adba8db1e3cc8394354a9157f03c702b9cc5a2
      1a6891aa500af84268605ad3401c2b939c7a0134b9f789aae15ef6d08ce86633
      c63a0508c262329a2794d05a7a8223a6464302855b9838a586aa57b267b043d0
      6c05600df6991d0da91e84493366e86c664a35ab3b32e75c2a5ea8a0ddb43bee
      aa1b433257049965daa2c5db268e4d092a20b84d9537af45e58b76d8752ce08c
      3e379e8769a5f2895d9f7b9bb53b1cb8b357d2c13aa7601c5f6ac858dc51b606
      732a5b60ea597ea8f342a3a36e8f685e6be6a5d0a62c278b146be384ee273e77
      3539f0c54a51757261210f6993247671b8a9224f12cb2793125dd189a9780a72
      d35cbe0eb8205a200bdb651f92a9487eeb4a6b4181d2d1160572586bf0bdd6a3
      5652b2074d2883b49610eefc68ab0ba3cf410068dc1724c72516faaafb919c65
      2b3be2f16a59e3642d616d92708028401bae3a287b6bad4f04aace7524e73205
      86aa1d39942e8c82b03982cc0dc80424f105078a40eb193b8825b451a928e810
      c9ceaa1d0c4cb0cf061bde80b674fb1ab43636f1c625cc3b22976609b3c854f5
      973cf23283fce2635194081dd3077ac353aa549b2b670bd0b98957f986d5561b
      2b9c9dcbec20c19aa83709462c046bff3348c5384238bb035f433a41219ce29c
      9ab99ba1a89c25cfd47dce7767a56542021a1de8901fca6b7da47615b3599ee1
      604a40a08f76335d54861c7b415a2620143aa9010aa16f0cc897363729abccb4
      cc9ca5e6b0429a3012f6039123217a5c7c6e0e99513c3615792258efd51e4518
      b176fa9b72941328e683a1721fcc518c8983a303a96645f6205dd8200bc45640
      78949521a6d1e765feeb02a01169be887ef54846dfbc282a92c268ccb23ff031
      828e0479fd757141b98d0829fccc7ef3c27cda544b3a777affa209d86b5e719d
skRm: fcc790d47249f00165299da5ea7e8fc878913ad9487ea6f437039dd605cb032e
      4ed9054818b70b38fa139651fa80187a0f390d71af83d0661c76fb182c9fbd0c
```

```
  enc: 3eeb580127af6c5270c93176c82d0ef2e36e168ec1b9b62825d0bbc57c705a163
       2a7d377c42adea1c15c6a16f489293e8eebadc5341283911feb28d9424a155a4c
       b7a036a7f7bb92fe63b9d628143cc1c3c9a5864da7047f0dc12472ef4efa79f96
       16b4d178fd7fef0c37df42d6545f70724e70d8507797a72be14463f8e03501ad9
       54c036fb227bb64d0361d08e1f96e610b2578bf9bfdc9a8b035e79ea1ed0f4891
       af7200b99bc73e02a30576501ca55dff84c06dcef42cf6f22befe0358cc420584
       1c4003bb5d02c9c00dd388281c0a1de51d2c172db2b871aa8799de0907ba1e87a
       7fbceec515650605f0e8a1ef1587e1d8cd0bfe8b435b45eee673f721520b546e0
       5d31a35951d386811d49aa31065fcc2b5f4ca60d4843d88bbc046e708f4870a71
       bbc48bb734ffda4a810fa2a7da7af8e17ade025f8ab72024f6e04eab7daec46cb
       e88b2db950d05ce24a20b8f95eb26b880d6ee35a68eb201a67d1c6905d1cbf079
       835ab673377b2861d3d9b4d3460626d10d9b9b0c98faf0de96300dd570bc0cc59
       acd577d5c0f5fec89a18e34b5f4f117ace43094f94dab617ff859c2e02cfeb86c
       fdedaf9c6fced37a977e23312731a2f3032fb82ce5244f1869c0247520734f629
       fe4799067553849b42922873db8d0d9fae664602aeca96258814a3dc0486cb97e
       967381a736537aa2604fce066fc0200bfba28ec983399a5ea91acb1054829ca6e
       1762adb170499e3a361e868f449c3a5aeef935ab594e733f9c4352e6fb565832e
       3b3e583902ad0d9181c9b6151021a2f04b14cc415bdaa2485f957763452a3f9fe
       524b6adceae0bb7cdf03d886157a32ef162707dc8a2f71b07eedde31ef112a19c
       f0d61134bfdf9143c8e2e0ba9ee57641d4a0643c41509dbf7d5a8c96c2c012fce
       dca100c5ad973a5f1b328a4b7e1f1b3f9126bb572703f9e3da53abdf14c49e32d
       ec3fde3bf4d59cf4e362d09395e3771eca527f9a8944b745ae9b6943cfa404e39
       343cd361586bae04c712b26e750a26c4fa868cda1252acfbe4d2aaef3738b85f2
       f8723f299bdbc5b8f65479ffdd328931afbcd522f
  shared_secret: 6209eeb3c3fdf8aeba0d285bf0098f4b748bd630f78990f138f9cd0
                 e8023a264
  key: 53400b5a4cc75259e3bdb222e1081f56
  base_nonce: e4f3c7a0c8f2512c6993dee2
  exporter_secret: d5a1a92f0f3e88334c14d93e3a999bfab39776e63ed635cb28b59
                   e958e563ada
```

A.1.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: e4f3c7a0c8f2512c6993dee2
  ct: 9258af357e97f286bf7b5779f0514184651b4e95f6c02febe3d3cf45536738b0b5
      d6d1c1fa6ec8a2ed1ec3a14e107736510aa6febe6996b5eb192ed5a6a8c1860b74
      08992fcb30eb14cb

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: e4f3c7a0c8f2512c6993dee3
  ct: f2e232e9c8f2605f7b9bd7ef64d1c7e3048490125407a6140589ae6e661b164e2b
```

```
      0b091a46626d005fbe40f5eadcf27c21908678b4dd93c1106a8f82e3c819f13966
      a4c866393a060f4d

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d32
  nonce: e4f3c7a0c8f2512c6993dee0
  ct: 452d947cdd2ed93f3d86d8b364934f92a087b1c470ac4cd4563a2e6025c38d403e
      f53ac6cfd701ca8730bf1ff4dc22ba03fb00e854b16a1738cdcb50e5cbdf28c8a4
      052ee84106774cf5

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d33
  nonce: e4f3c7a0c8f2512c6993dee1
  ct: 86bdc6a806d65cddd129ce8694f6313ae432d058c4b5105ab024771c9ee4c8cc42
      88221395a595f0167d3ac03d57f892ad91cc5e5361c4cb223b6dc9048502b1b32d
      14bcae706e1fa3e0

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d34
  nonce: e4f3c7a0c8f2512c6993dee6
  ct: deffa03cc600fdabd4ebca77e977aaf77501de3e1f34dd226e39b645856b326877
      64dd8279d5bb3a3da671e47c96a1fa29bc6a16ac5f4670fc8a44588004ad542231
      8925c2a9e09567cb

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d35
  nonce: e4f3c7a0c8f2512c6993dee7
  ct: 8d2d61bfa7aef1e1c5e68e8e0ef8652e50dff3596861c6fdbd33b30263750c50b4
      d4618d2f991eecdbee91e8c3ba02a0eef24af2f2efc796f778929e20ab9e24ed1a
      0dde50c51551be60

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d36
  nonce: e4f3c7a0c8f2512c6993dee4
  ct: 067efd47f7cf23ae4c04af96d944619a2f2b4841cfddc2553a8ac5cc2ff5dc815f
      3722c3891f480a134918caabe77e8ba5e64c5d9595547feb9a5380dcd5b0f4aae0
      f7eaa68e389538dc
```

```
  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d37
  nonce: e4f3c7a0c8f2512c6993dee5
  ct: 94cd305a3eff8a2080d4b926d837e65ad2d759196ae5204fc9dbb8be74eead731b
      c7096ac98710ca1624cbb0cb0eb3e48011212fb210f5c5766a83b4e38fac735409
      586df6c789fbdc9a

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: e4f3c7a0c8f2512c6993deea
  ct: 0874b2642c04b2306fe4253aeef57498955e75bb3f928dbfa4288c97ba5daa892f
      72adb98c8d6ac3fcbc52dd2b448411642a09ff46fa571a21eefa94543a8267e08a
      f4f607520e4ac2a0

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: e4f3c7a0c8f2512c6993deeb
  ct: 1c73dedde212e78f40263e8b33d4c750f8f4c939985afa7d8872a9ce2cca3c7ee3
      7ef3d832f3b6cc9239e16afe0d5c9f7f99230300a539200c78448396363407181e
      5daa8a81e4cc1df5
```

A.1.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 7083d75d22e2bf9d1bf257aeb440a6d080573af13907d546d7a859
                  55dba938fd

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 03cfd35156cfd4f36eb3668eb0cbbaf4cecad2b9a8e75e007cd413
                  20aca69b70

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: cce09f985aaf4c51bfe46d5d56e264de5e2ab7902fd1329236c224
                  ece7221a57

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: d6e29269d55073f16a21066454a2b95f8f1baf87dd5ddd80db8b3d
                  1d81a732b6

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 74937ee222a6cf02015d7140a88ce33f6a7b53b93add2474e5b3f6
                  df1cc0d9f9
```

A.2. ML-KEM-768, HKDF-SHA256, AES-128-GCM

A.2.1. Base Setup Information

```
  mode: 0
  kem_id: 65
  kdf_id: 1
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 4b3d28ac17e3aadfe767671928e6c0d26c346d4c7dfcf1db0994d131fd76aaba
  ikmR: 353e522ee88da0097916c435377e3ffee4cd8288b910a79882f4ac87787cebe6
        ef7d126a2ef91b2c37f741af42851a08d24a756b225d86d534902829896e726b
  pkRm: 0665cd16340cd373c7a7290f9ce315ddb57b61778aebd15fae817be1622f5f13
        380cbbaa61f9749141133606802d69a62d979d1aa04dcd6b073bc4b96612a843
        5a6578f86a8aa763fc2abdfbf30d35a6aeb8919cf0b7cad876bb1bc410a72159
        bf927b9e8a0ef56463162a45479166a98336412c4eb8042a70965df419a62163
        bc70cb567a3344dd86b3a282a32bd57d9518b82245aa8c0c603d36a057f0bffb
        b39ca67c18b8ac06344a441d2a6027dc7f261804cb2b94e9557820f7518e8b9f
        97952b953903ef89ae49eb34e4c0a9bf54797ce1535ca8a84a94c55730a909fa
        a7cf467f1c72414a99a41a439e74499c51689f9ea7938fac45813749c42b7d6b
        a13acc447d31052ceb9730e86b046fb47c18935c55f22d88e8a8987b7c02d045
        2c3b56d492a7f6718c7ce0c7916a3f905818df6a3caac037ec49a964d965e147
```

```
        aea4a273e9fca7dd57af51638eac08bc77388aa4091ec9b12ab8929d72fabf7d
        eca2469b25862b197406c9f0e479c40c257c809656465f076914cd3a2195c262
        9880c323a97236da39795985ced810e420527e1418dcabb2b5f8944d4433ba17
        2b4100a7393a5263324b2f9008d90957e5cb0f9c7a924851121ec0808a8c4ea5
        3a9f853a6b2f4a1ba4496d40c746ee646317025d477127f897379ae8b6833180
        38a932902668f0147af7f05cc7b37c4c90b7525062d468bc1106529d39673ffb
        a1cad6c2e93c327d92ac44485e84c768b34743eee6781e45261025af650ab85d
        a3c0af7a66d616a5eafc3bf7b30ce94a4740412384966edd992beb8ba695dbc2
        25f52c72e64d1e6c40dbe1013b840f9fc61d72530e0396048e1980c99751423a
        25874518be123a6f89556c8c270a736d1cc45fa4a5a6ad142e570c4d8974caa0
        368f1501a8a3d72a39cbafd441532d612901b454dc523de86b97aac84350a703
        db44869f4ac3a0dc7533723a31d9166bd33b72e8caf2f13364cc1934047952b3
        70b0bc37664b772fa91e262b95ec40519dd46515b99284d193c4738f854b3d6b
        a56cc819badb8b61bc0b86a2e2039dd7995bac3e38143fc744a89b351b3ba6a9
        67019842b0099e02ae87ca7c5c929935ea27180a9f02849b34e7396149c6d6db
        40b4b69aef0c85f7725f7218b31795bc98829c512b689914a50c1c9e15489e54
        ea8c57b28c4a2142c1c72b88424a7b9ac7c4f612a0725daf095c8de7a0d2a92a
        c34c042fd223b3f7a937704c6e60bab4887b46635bc0084ce5d8862088563a19
        6522ca7fc6e917a5ca895424778c6624c237425f4b2c98d206defa82335638a4
        2abeb97b46f327312ce23140243433118079d0bdd95c5ae806761f9774948321
        c4f081c300451e5542195b0a07999f225b2e9b6a3b125336d3fc9fd0884ce0a1
        068de158fab229d73a865d550786542af6c54095b88f21ecb207da9c5dc74ca8
        8124ef4b76e6d46ce9ac12a4ecadfb322526d8b42f0aa8f2329783961cccfa1a
        d3c0430a8a262a211563360e68104a8e903337b03fb715a728db5e6b861656e7
        30a54a1a3f887c17b29050c4a9fefc70f7565ff1804a81b48b2239b0dd01c100
        3b980ab48919ac496e823b227900286b3f9cc92df81bcfe5b146355a94cc93ab
        64c0b6df38eccab8b16f84038256c344dd4449aae52821a49ed62df1767d1a4b
  skRm: e3408aae322a3628a4d641c2690d4eb212fd66f369782f2dd22fa293476c6995
        7716be20e83920cd26a7710110a34ac3d5da7d90efdc9759812f5cf1a47e85bf
  enc: f4c758bd517040c97d327a0d30de9770055583ac2fb90a91a6ec7cca4b464abbd
       78722db29b985607aea1bb4a79fc76fb784c4d10828e9bfd21495c3e94596c4b6
       26051f30c7028a29c716a2568997392b30179cfbe136fb06b741504dd8901a729
       1446a692c804859171245d12aa53e0f58b6643a3ba8490180161340f24dfbeb0a
       b865445ceaa235236ee0db44c119bfe942c7f83d381d7d65172008de0d684de2e
       87f21394a66bfcf88918832f299469f32fca0e7d5efac51d34b6a788c54922b3b
       4b7e8325f6306cf545380169773ebdc03fa06ce25aa1c71d307c08bef2016affd
       d6c293f3cbb0cdb92021692a8ebaef6b74cd6a2bb468da79cc9d08a0494bb88bb
       2ba0c88d4a3ee2af38762cd6c297c6b36ee18816546b375718876efa557ec600e
       7c4c6e44aaa3a1372c677dc638dc9742d90319ffc27ee99149c5c8a8185ecf600
       fdd8be897efea52bfbdc4ef53fff7301ee49a7a352b4890e31c2f44b459b9f7df
       4623b0be87f1cb9212de1beb19687f3fca6d13ca7f924c0471cf3d9b284e13db8
       e25e2fd88095ae020100cd9ad5aa5355b8aa90d31657355f80160b3e1e1282090
       8b3a85d321be6d68bebfc7335738b7122de60f4acbb924d3a610749577e8c0957
       4ac0160a3a2f37f9f8af0082082673347db7f2ec20f9d05e96e483411b4c2b18c
       c49a01ec65ae3a077ba18a7074e5bd14ce97b773687a2cc89b18d9f442d30eebd
       4925d1591aeba4a04c1a69a7cc6cf34e2581300a27b2bbe9c2fec61ed1b63e50f
       8704c2737de13f4a9e53e021c5a314d13951293c0a74cc4f098a458885fee8dcf
       879ee8fe91ebd2a2ca1ffaa9efd84a042b32e195165ae187d66b27e3cde4334bf
```

```
      f1eced50910c3ea026ae049df54ab30791f129caa89180c1b6939f8017ef980de
      3900bbb32e9bc2e1bc53595c438137c62afa349961772d12694fea979f0f4e70c
      8176b750eb9002483815984b6747d8d4f301eb0b76987d407b2261adecf580160
      d3185f49aecace7e82701a2eb70d20c43de1be39c1a26e4b5433e213abb748ed5
      e6fa088c5843c725336c650fbd73f2ee3f8800e9c07948bedec99f75673545425
      ab826dfe8a0636f422035bb56ef90b5dfab3592232a0b9a84b1bdd78b610a9c3a
      89ab3dddeaceae9bc5b5d89c930ca20039b65acceb1dba527b58fd6517a21ba90
      cfb38a2cec950c3f3b490fa4458fe5ccdf79fbd88ae0a84b02cf980aacd4107c2
      9bff7ac8c2fb9e8c131144d968a8b9f4c5bc75420f6cba590682170f2931c99b4
      1895d68ea474f74829fda255f80c7d4ae7b2b0dbd002684f01aa5a2bb17003817
      d29f27697778404bb9d07fc46eedea487f50490e9beaaa2be101b0d03ae9612e7
      574022c49166e1e0ce14187df4c75a134f12f60f74d41645584017404b3da7c7e
      2dec2eca554fb90eb5c958db7e6f5f19cacd27de4651c52358bb7be407261ae4f
      16559c9617cbcdea92133114b35c376e174165d56082b0e6e2ea347f4e26b9043
      75da1248a863766d95b2c5a2de36b47
  shared_secret: 4f808592f5b6325b866e7d90e48bead8ec36ae17247cf3a1370d46c
                 582dad42e
  key: 00fc412edb7a5adc4a2994869d1016ef
  base_nonce: 2a2bd95954150f73d200005e
  exporter_secret: 3d46ed98c5a563ceada359aee128d69c81704edeba9607700cfe2
                   bf13472db88
```

A.2.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d30
  nonce: 2a2bd95954150f73d200005e
  ct: 4793c6f4dc5824a0039d8faf2d84d359fd6cf423eaeee578bbb7830068ba34b576
      a6e3f4ba03c5c2c62f2b869224a1c5acf96083cd13bdc3623a47bde544171a72aa
      684b12a562196785

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d31
  nonce: 2a2bd95954150f73d200005f
  ct: 83591508b3952f4dd43aee00760fce5c3c32a24ddc5594c1a9a1c45efbf6c69f41
      d2747c814c25377276ef9243ac4a89de05e746986dec2adab645bed9bff1e2cf4d
      433aed524b9d7ba2

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d32
  nonce: 2a2bd95954150f73d200005c
  ct: 7da978b2f52ee2168a4b28bf06d54c52ee2fcddd330498df3f37ddffba42fa0013
```

```
      aff6435b996652b612bd0583de397b120dbfb4a5bd5a4ab1a5072dc387afbad7a8
      db5b2b6c09f35023

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 2a2bd95954150f73d200005d
  ct: a10ccad4b013513d61c12c201b31104b4dee33db7583cd778de7bf16ce3a6a7377
      f8d0e822b429f8b1d2b551df7c227d8b1b095fcbd7af402f8280a7a505fd19b67b
      0a1be1c0b52d2495

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 2a2bd95954150f73d200005a
  ct: 457c05f281cc70ccaf83ff9e30489a5d5de8db8c1f62a6b422499641c252b9ec7a
      fca606ea13352e58e9f9e9bd4b381aecb2f4f4c5326ecd7872e9ad11ab0238dcc4
      41025a27789e7c1c

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 2a2bd95954150f73d200005b
  ct: 1b27d3631d6122adaee538019b2cc82de10cb7fcc021519aab29edea9b6f54c5c2
      50fab1006aa071265723d3c4517d8582e802c6c681f662647fe7de21273690af60
      5b8ae0ce7dc23c8d

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 2a2bd95954150f73d2000058
  ct: a71c675d817dda0c4064767d8a801d886e8d531df83d76d0658f0ba30d12d00a2d
      d7983f9fbbef6747b7d5e2d9c7d5294b81fa7eec06faee98d426547f8f435ac6d3
      7430d083e20bca73

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 2a2bd95954150f73d2000059
  ct: dbb9abd6e85aae5442e99dddbca964bf34b7c5ad09b6242ea19edf8d5e75e8f6eb
      a1508aaae031cb2ca7e64685093c5bd2ba8cb65e8cbfe1d53e24b9e697dc87e38a
      536e4ab45161d451
```

```
  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: 2a2bd95954150f73d2000056
  ct: 33f984d337b1df832367c5e54219bbe7a6c6fed52872bf02da987b3ebfde2483b9
      56cba8d7cafd7d8479756ca8c34e76b4ec11494a314cfb7be0b78f6526d1bd1b7c
      d9727f8273b0e0e3

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: 2a2bd95954150f73d2000057
  ct: 8f08ff2d727ce8567b4fc78619522542524b91dd53a52ae105aec39f434e4acda9
      769ffe89dcbd80d6f12710b061f4ba9c2965fc2ceb75e766b646ae9f21be9e7f4e
      3c22f68613012975
```

A.2.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: f05383cf57bc5c9d639f1eda2355ea5764f46b1a2c98fca15b99f6
                  1d7b5a6549

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 19e39f4f822df99b7488119e62385c99085c4a496e17a465124269
                  27d4fec854

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: abb0cae7628db9d8d5576e03a67e9d96c210ecf55863e45fe39c06
                  70b4a23760

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 81f0b774cfcb1368afd39a6678717c157cb075480fa01d78a17442
                  b64fe4559f

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 3835150e99658061ff40490f846ca63c410a1ea55c3ffa613b6618
                  a8ea0d5a37
```

A.3. ML-KEM-1024, HKDF-SHA384, AES-256-GCM

A.3.1. Base Setup Information

```
  mode: 0
  kem_id: 66
  kdf_id: 2
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 0152bf3799ed0803b9ac3e62695c51065fe2cd4a18ff655fb3efe7399c404e19
  ikmR: ece1c121b5cc978bdce5eb8d60e9ff101d65b94379898e800c37f79164a25d03
        264a357df7cd28214b11e171c94dea2338b736e7dbb6f00a0b1b280ae6ad1ba4
  pkRm: 94c27955cc5863380245cbb32d564f4d86579f130e96947391f382f993184396
        5a99db8724f08cd6128cfcd1c98be3733fc5b3171531f9060b9d90528770aff2
        dac0d37451beb30428161ef818b641273b62c4c83b0b84b75565fdb9433ea32e
        c4bac540e57c2c6422144511edd6b0623b5f5751c8d0954912dcceef46095201
        28f8f81ee77045860633ec597bc3d116a6251d30843a274945ffb70389f30587
        497898f82669b0baa3b17dae3167ece26040a24a20407547f49014a6a25732c4
        ef1259cbc78bb92c9e787668da8c53e9b4c189d451e9447c5053b0edf3964c66
        55ae919a00c49a09384d0a5cbf0e889e499255c7f9a71420768e5016fac579eb
        127b71e18df5ea4b7a53bca7d97ce9898ef59acf36a6237427ae06b80ad0a594
        c6f52003dcca5dd36efff979b3a67a2455917121414d27aeb4f1a627d45edafc
        1f064621d20c82299250a39570c2e4999429b71fb87681b693f5d330ee01c8e2
        531b4b4088adb3ab18c057f6e532e38a5b03d69f382c24e7140fe1876851f735
        e8442093226f56686cff4457141c68099cc942ac2956b06745881c29bc557158
        0d2e2c56b8946634b17a46882188e09949b49ffe29376192846bfb3177c7191c
        0137cdab79df179a6226456b883a3fb42768bb0ec7e5a808e1670582a6ad3928
        1e88afd9b0514ee50956d5178e5b9f4265292b5b5f28644ec2dccf2850c56715
        2e5dea88dc185a800559d545969be9c90fc366f441a1cc79bf95d0bafac1a4d4
        91c5eb169dc26b6a2193b9500120bdd1492546a79db13a2df56f66ac40ab5893
        7d9550b71aa5812038d284566932cd001a0af6a285c0540260bcc323528fb337
        a2768c840676536466b0ee24c42494a661b176e36a98c99c31190555d7951f4c
        e4ca342a70dc5a2896d4b35e3064f5a32556b85bfd807673c670c6840609932d
        f7c83504dcc56a036836f9b55c14a948928622013382c96f875ba69ec7363e47
        420c08adfeb4b894578f2ec8a966e341a6838521bb533a604e0dc92745b39231
        035b722907797a531833437054545ea7c857b29f728a158f475b2be3774615a7
        16b9799ef8091150afd3d0bef530498f849fa6b99033778945f9be8250334fbc
        79b6124c27e11bad9a7b7c1248fc5306a85c0d0aac8f71ac9e062500ae688ab7
        ea304c22123a8aca343c84248b9b19495885585730340132149b474c26d51c1f
        36f3789948adb18254424a73d7030f87e90fe98a93473a8e08b5070728adcd4c
        ab4d3049bd7ca5313158e35c4eb5832cc7d50cca6661f6a7aaf0f8800a6559b3
        32b13fa128d3371e0c2a42738a56385cbe64077f07c3386dd5c759186b4cd038
        7111a131dc35863371f6e389aba0888ff9a2e4999d18f9768ff74b6885a823ca
        53884759ff4ab630f46df7fb43ebc46c0d494b2a59987da2c4785944754b9487
        5283c0cc11fb4b6418bc457416cf73e762da709b200b0adf448ec5b94911905d
        98b407d58942f9c09dfeb22f1f8c016b31ba0308494fc44a4e85b200ca227cb3
        a94c319ca09a3446258be00857f22640d3206adf5878dff9ba20255da9caaaf0
```

```
        8725071b9218dc1e1a572cc89a11f00c3b3ca98a534471de38a1c9b618ded765
        47ccbf1fb538cf78ac4dd8a53898b9d0731111227e1807b06c639c111359c96c
        991ba709bb16139ed0c1fadacd3a9abb9247087f01aac5673b30a86861283728
        c0087e683a4c3b2ed0c645f7321521641bf823c2ea0263d1db9e56bbb485f715
        cfe0671902b5eab9ca2cc2277b36cb751cb471abb79e2410b73cb8ab14b4b472
        19ad59511ddb9572fc979a0306eecc50ef99a78c2b737d8143cc727632a0bb74
        4753929b87929352282666666692adf276b2d4b8def0475e7685617a4892f6994
        b90293e9a49d92dc5d427487647625b0a38d8616acd1e590ccdb0a7628796776
        5af9030cb56216b168a6fe21ae98578e08c0c3873526125322l6642f2017b09e
        7666df2c3ab7dc17d25b8f8b512b2e6ccd28778084b000d2e03139979bddb29c
        65d27a5be70dfd7a24d8d6149b604e715647072246384b3a2e42488a63124a41
        bef79672f3e103d2c302df819710e738cb252e04d37092d3bc5584abbdb76e70
        e6a59e50859cd6053cd4c44b71c7a23c0df90cafa8b116cbc831a5c4998048a8
        6912c8ba4c3dd1399a1fd014fda88e38712368772684c68880728930425b37b5
  skRm: c58f733ea1245a7a54723c30dbf0837acdd7e93c188692523b53b132b993a25a
        f933368a76bbcbf1212e1d34d7128e32c387dc9b04a7ceb0e2b40e1e5769c57d
  enc: f4a53a8db87e065bc2929f5d4e827ef6f6aed7c8f457e19dd8d0c1930e3e1bd2a
       e6183590d45a037d13f5fa7ff1d1d7ec9873d625fec2727c0a940a66fe5bd6501
       946f3bfb8f027da703e82ea1d86ac8089d7f6e359e9ac6ec95661be7958489d48
       e930e9eb9e77e842adc9774525dafbbb6675727cea9501aeb53a33fe08bdaa434
       18486d3391add4a6cb72bd6865f616e3b9ae4339871e6662f03500e05c0ed883f
       c3ab9ed8940a7a48037f37b8701dc2daa42469b88086732bca4b7ecfe412b5217
       defa3b0db1df8b7b003938535cfaf72e55ae08fb76687a5268dfc1e3b2d827bb6
       6f2d09a689b69b5d06cc51aeffd76479fce38e952af5fc0ed1e0195929ba7d117
       2d509d26b133ec3f415273de4c8acc302435ea4afbfa0cb3e1b669d0e968f3326
       da174b10de6e29adcb4970036dd17567b376ad97e0a94d3fe7cbff0daaa3ea698
       ce12ba7fdede4c51f88502dddcc5a62a146253464c8f60ecffbf4c1469435c18c
       3380cb226931804497b9e73f8a0ced189770b626239531b709f9fc9b299b1f3dd
       403cdebda088104adac23ede52b4d225b5140f34e3f7da50b8a671807be7c0c40
       8b1b7e665609bb2bf0680d942d33f99fa24d8f9c9d41ac6d056a5d59de974c0e1
       6dd89e2c9794dc4f2a23f12d4d1dcdcd799ea56a185c0453348016a4bf05c5dae
       b71aa8a911eab43d787a81656a4f9a36fac5304ef8949077636b96536dfced3e0
       05d8c30d053f06bc30bdf97251d842e1a4a1713521bdc43ae1d0af798c33d383e
       36e1049f7040ca35dcc25537b93411959103e0be8a3c16b68c499e8f7ed2f1837
       2e6a7d605e5efdaa79d06a78e9e8c1fb47afe30eaf6f1fafad31cf88b39e502b3
       ac5b183ad3e5fdf90306a8840bc45d44f3ef933482a2a3cb2ac5e5adba06585fe
       04b5f8260bc0139b7d9892acb3326748aef0d7337122830e39cee915149ce3e2d
       a5281cd7917930274e74ca46a5078019411dcf662ea4c6fc1647b62653eecbe61
       14b2b8c7c6dc4b6f210ec380d093c2674da248029895e2ce8481094ae40a56eb0
       107e5213556b5af4d1f45fc1d1417d58844d7a116c308c1c794e3f76efafffc37
       2719aca595f34a6a87eae2211e0d4ba6d6217528bbbd09675105c2358d48d7171
       1bfd64f42f66179ba845266709e0dbeb2f8f71febc684bf1217e0176406b2eac9
       ec257c5ab4e1711ba866420da0874895eec278bbed2aa7546a798d13510bb4992
       9455dcc27791a381d086ef37872d1ec7b3a621bf989667c6804be0dcf1f1d7806
       cb1e32db6bd6701089b119b745b7d15b8b4d0d421e1cfbd1adaee71586a2d2a6e
       289cec185b3ce1e139cb9272bfd145918a0e7768ece9169197106a3487cab68eb
       c99f49919d6906953dacfb7ab020045c36db21315004ae7b9632ef1310b657b35
       e6f6312329274eea7858c9aca3a3f93eea9e065e9d248b1b5476da95708ee65f1
```

```
      e8b3a7a03d95188f87c504626793b8a4b87e49bc1da085dac71342b351496e63e
      00650b1f9751cec64a60f6b7920b9f9eaec00b5788bc77e9a2861501c528be11c
      5d98f6c4e1d8dd3f809456a8963e7511da4438bd0eb8621c210d522a60deb8e0d
      9c00b7d354e16d7af2969d64174493f0205444cee5bfcf21ef34e09c93c794150
      6e77329723e203c4473c9ed861fdf4a20d96235f5615cdd9f5b6013bef71fd37b
      464677f1a802919115f5231602798710ef33495bbb16a0de68d3c0dfd2e1c4833
      789912ecd7cf41af474f76eb22ef670176ae9e5418eda91be4853de9c212a1463
      6fc7f804612707981a4097f746d137ff7af79aaf73b9d79b5c1243ec5ca02fbfc
      00c12b02bd59d28217c1181f7388332a1362272182d23aa6059a7493586581a5d
      f3452bd414bcc84599bf740de19a745f40953f87f156b568ba4039e4ecc15e11b
      9f21f6acc6cffb1da164c0a40323043fc126dec090ecb9054ca3ac1a245291925
      b531f6b08d8ea60becb8edbdd2d4ac4b3a6fd5282335737b5c7fea581e2842f7b
      3b56a694e0b2e909507690f2c452d6ec020fb309d12ec0f75117c8cfb10c8a3c3
      614321beafcf0459d523ee0ceb7e730e3b5d2b1b509e7e5310c07f9dd4eb5250e
      550ae084613791b87c107c4c875c6ae44a30eece84d4ba8d45754c7b5c63ba319
      3bc0c013c1619c2b82710fd958a92f99c549a3be20fdb7ce3c2f07dba9b917e81
      190589c8a0fe95a3
  shared_secret: a9f5e349635145bb8a06c0b50b027bef523c5868dd3477a8a92cb5d
                 eecc4113b
  key: 57928282570ac8e002ebc79908293d65faabdb3ef58149edb33083cc2f38a55b
  base_nonce: 107259b6ac73abb151fb98a8
  exporter_secret: 9d4faf56b5319ad7a66492576d15522e30d948ed11ed3543daf77
                   4c0466b698ce699de9671ef34f9e23a741b7efc5074
```

A.3.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d30
  nonce: 107259b6ac73abb151fb98a8
  ct: 433d24cb45dba60451bfcdd3fcc9033a55cbcf128f6068a09cc617dee516d02bd1
      b15d8bb9f8acc788b29086566124414183c07dfe160d135213dc21b34e7320a19e
      54d979b2ba3f2d66

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d31
  nonce: 107259b6ac73abb151fb98a9
  ct: 7256a951ca1a6c0ec0ee5e2a9b9289ddd576aed1e18adbf722258ce16cc7c07296
      6f9ce35084c1fdbcf0d9d5efa56506856f4fbd424225dd26307a97514766e837c6
      b93581a34df523e9

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d32
```

```
  nonce: 107259b6ac73abb151fb98aa
  ct: 2777b8237a8482d4dee738870d5c95b53e901834c2dc1221f2816344cd40b0554b
      50257245f5b7a632c0464b4648ef77fd5f836e37b3a0c5a0c4ba9e4b4390007641
      aba8d2f74b274e93

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 107259b6ac73abb151fb98ab
  ct: a8979ccbb426a3ff16ccb5f32c339f7472bf735193cbdad4451b908650f7d8f669
      5fc954eefd653cdeef0b6c241bc0e95594d65448130839473fb9593144517eaa59
      fb3a13b823934d9b

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 107259b6ac73abb151fb98ac
  ct: afb23cfc3f728a9f6321f038191ccecbd69ab6d128bceed0f0e4fb6f976914da6e
      19b75d3a0466e50d1bda93ac629c5fdad92c1342a63a59148a1c5014f1f7e307fb
      6bf40ec0fc0764fc

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 107259b6ac73abb151fb98ad
  ct: c80e5a54a637bc14c008ca0cb181c4c92bb04327be2f5ce16d657fc4b8890c45b0
      30e00177b12ce374c6a99f8b6c89e0a7bc90625c33e3fb63e17859208e91974ab7
      051e56dda3cbc5bd

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 107259b6ac73abb151fb98ae
  ct: 4d7b7560977e436782735a2e5a12c22052550ad496728346e36ea3429aa0ea9448
      c3f2d931e97045d630240467a45a6d63a3d341138c398ca034664f46642f74964e
      a5d9cc224110ed8c

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 107259b6ac73abb151fb98af
  ct: 4586d93961d64b3c27508371352b3759f5807fffc7177c4fb5f4da48c614d2877c
      450ba6d68745b2abbbce13c4291b154e1e1f72810e8a353078b3520539e484d682
```

```
      7b2199ce0371f175

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 107259b6ac73abb151fb98a0
  ct: 1c908bd13f58346c54baf9b62cccef03ab01c1850f3756670ce13acdacada412f1
      c1af4e30c9912283e26e630c617e18a9d28b6758994a1f4f55863e0bb9f79facce
      e64fd4591808d7f6

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 107259b6ac73abb151fb98a1
  ct: 8544116dcac5e3aae933fbf65956f12e3f95ee2775ccacb6c7640fcfdc58029ac3
      297a5104152a64b94ce6634c6654fc936f9b2124cdcbaade506e00eef768b88db5
      ee68f39ba9c36f04
```

A.3.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: ef5dd95b6aceae5c9b29be381b4f374852125b5e6cdabc985ab0f6
                  b808b27eb4

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: d0f3ad6f13a67b3ddfe63c205d33d9061b65fb99d91441cc145463
                  1d7b6a9914

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: d39e047401b666247d7e7e4fe136302ad1e01a6a2a823193be9e20
                  5285a15a2f

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: f265416a47dabdee2b894aa5ff566f63f193e204e5819d506546b8
                  4a78f0354f

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: c9de4110b79f1d7d6940dbfa4021361b4220020ebcd71fe3633101
                  30fc887e69
```

A.4. MLKEM768-P256, HKDF-SHA256, AES-128-GCM

A.4.1. Base Setup Information

```
  mode: 0
  kem_id: 80
  kdf_id: 1
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 0ec0fee6a71457a9dac898a1c161bf1068e68de093f07754155bb8b8b378c17e
        d09ead96300cc402a6371b58928592dd93565834a19839e7dda048d8e04ff65c
        7b645f36738c370fbb2d684f59e16ea08aea04444762fdf3a70a114ecf0ba435
        c9a1e869578142b445398f49093bcca618f0ae5e810163b1503faf3eeaff0bdc
  ikmR: 5e28a96731c6665f07bb00811cd70f0d3d6c44666ca54cddbb7e5946053b6415
  pkRm: 4ae736fa988490bc81c4b9b253932c857357fdd015ebb52310d8bb75a7c4cb88
        7b1d5b763728c4a1b12bed869d63b583be163a946bc6f7e8bcb0c76ed9e40bf4
        b8683dd33edddacfdc8321bec86e98209241e4c6e1c3b842896c441171f00499
        35082701a50e22082071152c0376344a165508c3cd7e8432cfa62ccc5288eed8
        a1e940cc69442f9c0999bcf45d8ff8bd9d711dba37362d466dc0f32052b280c5
        5159e8f5bbb1728bf38c7fe0f9077fc8b2469198c664901df27a894c6b381acb
        967c696f43539fe784f2ea848b58673247015532b2937c958590a893064462b7
        35420714f0ba374b59b4f44b9f7aea5359cba0946531b9a2695e0a8be3a2a57b
        397b23db9de654b9465243cf05336b8a1c0e9a771e9a2f8603220542a5884839
        cb534fe2da5586b124736c6ebee8c445b95c95db9aa6ec752a012c1bba9296f6
        09b0c5cec9e989564261d17b183a0c13ad94b66dd40df06168058881b5f54c07
        a22d37a588f162352fb0011dbaaabdc13301c3361abc719f947078e583d90a76
        a9c050e01729a9f0ad7a9465edcb33003240eb5a0c39f449e932734c20ae573a
        23fb1cb87723aaa3caa81dd99f320c2424dcb0149bceaed949963b8246b49c3c
        16010a9527b5c8be14449eae371e8afc1959f0ae0bc8776714069f32c09e7106
        01138bf6794fc665a177837cc051a26a0856d040c37c5a0cab15bbd42a2ee191
        83edc0c6afba51c9716f82db70a9dbb5b16c177e990c910c851f163918b18449
        9872e2b55c73883de2552566bb483cd1a703d098954c1178218d75a6951b5918
        178289fc394217e2072e1245b0c5190590832f03078f9ac9a0fb10f8f0a5bbc4
        bf1a1ab8f0138b6a59bc57fc1a4448391a4a211fc16e5ff0c3ade90bc34504b1
        222d4b0c7e70b10e7574a41b510c21a634b2da02265698d180b71847bb79194f
        2b66541c28a333a0c18c022f2e9549e9a5cc6efba448eb800fcc94a783bee8d0
        a579d9a651c5c35887701253b9604884a673269293b4fb884f26bc99c9b200c8
        470ff200ae45a81ed9990a7c28155493bee1556446837efe07b5c636a4402a63
        8f556d0821415bfa057443c0f77b3bc8d3bedca81b08ab66b4e72081f8b94975
        30d3ebbc2ffc05b62b11f857a24a37b50d533528b42536d45198970d2f9b4a6e
        a9a5327c3a883b0cd160110b2662c75cc0e6a78a41166b341437f658b6ba0549
        315394b6fc4d12607d3d632161a6c8119576a52b88e4da35db4ccbadec835459
        2df74439d0709496c96b01713e4185064910563688a06e705766f4639583b5b2
        102ffeeb09d7780db4914de63b5317946cbdd24140baafde4a8267f617241ba7
        55f26f6438b86f503ecd5c12c7f64197331f0500394360901ee4be91db16c8b2
        01b7e492f52418f3304765d6c8d2a4679fcc832413367eb2820215852c917acc
        c72f76930865da112a8c0948c26e6120116c614af9ebc2cac89a7c864b4a1299
```

```
        d57a7895212e2f3514c615780f2368696711b3024441026522794bc1b2c09169
        18fa886f5b630077599d5f83ac90c618eec58646f3a9b408bd16470248c0c28c
        0a5a5b046a84b0056ac67af345b6c805c08fd900aeecbf1c0c4abae321b93739
        30e4bb53000b53cd709818607426e3d75b937705e48c4a0a5286653f9f4f79be
        04807101b696947999ab4fb348c748b3127f0b8caa3c9d641d7b5488e8dc762b
        8e4aa47e3e45864cd2eaa55d66ebaf2879aaf56ff888ccff46965204bdf84835
        e2
  skRm: 724eed44c3843d1f260f79b142ce633d602f7989a53ffc9fd4a68690c8e7baa5
  enc: 6eeebcc0acbd1805273308d61a4212e9254658f19d51d7b58783ec2750d1d521c
       0e428620915b0c12274182b3e02d449baae5794d437adae8466560f5c7404d0fc
       e35e752e1daee24709523e70cde70bb16831218d696a6e685d1f5948613a71401
       6f831946127268f7986d92c3c9207355ee62e3f692c69cc3c4421d826d666dd7a
       3fc574f79137bdc3a55673d8f9b761c8227c01e4bb9d076470d4185a8a2f59617
       16e761fc7cb514feda5a983cf7641e892f582abf7c76ec04ce7fb6cf8e4f69186
       b7dcb15193483c930f0e27bb814d985141b628eea98ce282c1f0314f272e52786
       9965ec619a529dd5d78f06d0264ac90bc8290968f525569dfa432068f3b425efd
       9485c2b657cd2c09a362c276ea48e3f4d7aab046e404d3a3ea39fefd1361c426f
       37bbe816696270146d216bd5f44fff3c6baf6094db1bf9d8f15e636cbc744cfe1
       f80a26e122e7c37d1ce23b21988bb4075985b073b11bd467a69a3a4fbd71e1c03
       af57d5fcff78c0378c2d17ecdb7ac01832ea9f3977345ea8808a9146da604f574
       09f1257f0d752cbc6d9766780a1732f6900857f108aa427f5262874707f651253
       eafcc992d222783c9e51843be8aa67ceea9e559670568cc3a58b9f491dcc07a5a
       a4715d10a4e444fedf423eef13e801af63cc8b0bd0596e25f048c0a4639f3ee19
       4fbaf203c7b6c48316f570fb3bd9b3b20e62608398af3bf74486855f304fb5dc4
       647616fec92834a6cf7e8c48a24916a24337b42c0ebb98aebec5531b93988112b
       b78f58113cf37208986c1389e51bb8e59bbaddc78033edda3889af70c2f7df2f9
       3ea43a278f55bf37f818d5c38a6d217b6e40b7f44ce6ab8c0cc574643768aba6d
       590fdfe9682cb056b0bfaccf92121c76940f8220fbf1a216595d0d6a9f4226ac3
       811c45aa95033dacf2ab6f7c75f8240af60b18e62396a320694f15485c29307a7
       5a6b09ac089b4e0785747a549a77184f31d18f867e1aa3886e0c03af8dc95e1e3
       bb103af2602fa6adbd375230ac15c7526c7836aef4dd58e617282ab4c27343f0c
       78af9c45c2dc0d91b64b6ba7c8015d9688ec6e078814011b7b6de74c3d4fdb1bd
       41432f9b277bdfd62c84b07b5f13d306fa2b2d98f6f1480f63d7e50a3e7e5f88e
       d1dae7c5ac0a5159c74447cd885217d66839b9842093aee5af90c68d99f7a4a34
       514116366e408f6ffcde79ab0c9415cf714d31de88552252643d630ca3ffa81e0
       cbe7ce3c847dfd41692c876ab79956ba2bad4a724cf5aa2d53390fcc8417373df
       d06cdcc69eefb5efc8acacee8026d5596dd09043bd406dec819c2faca2a1530fa
       63ea37b79e68a192a904c83aaf62237661ac1c9b6410f9c0dc46019e085a0d731
       9691edb9ac9675bc154f6db01ddd6c1a408ea15c36862264fae32f266dc86dca3
       a4baf3aba15199bd90113a3b104630df9ab23c9c0230ae718ddb83857cea87562
       a80ed42268c2029908d2fd55de6baa0773d0059cc4c866c8e9a63ee7285f732b2
       4fff5a34b7b38fdb668e265dbfb887b0474d0e8a0dfe351b682f657bcb310c9e7
       b31315f7fe53706ec9f62185cfa9c0fce11cbecd134b43acfd25e3959d914539a
       2501b3b9c8e9fec86b92a2b811fa9bc
  shared_secret: 26c25e807a24354387a7385bc374953539001fcb7eb99eb8d63ec7f
                 db8441f46
  key: cb79279f04960511e17368b7c83df0be
  base_nonce: 47cdcf9aec36fdf3730d94ce
```

```
  exporter_secret: 0443a178389fa1e426df5a129ef7431df2b7aca64d06c4a72a881
                   18fccf7058f
```

A.4.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 47cdcf9aec36fdf3730d94ce
  ct: 766437e462397ec6d4b78c755a6f41cce023100641c04102fe935b1495cba6aa31
      323a97af05190a024bd0718581d48c71ff69d06523f6127ffb8f0cffde5b0bc098
      6fba65bfbbd6c7ff

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: 47cdcf9aec36fdf3730d94cf
  ct: 30696da24a617458cbb0d8556d7fc64b98c726bc5144d941528af513795cb7c520
      b5a86d01b73c08dbb25b53b6b740f54808196834a6fc2e3202e17b14896a44adeb
      3bbf4f7d7343d3df

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d32
  nonce: 47cdcf9aec36fdf3730d94cc
  ct: 3912f1c1e2df141e9edfbaf1b756fcb119a4c5ca4a88cd9261755b6cf4c821bef6
      1dbbc397fe8bcd63198b9db409054a82c9434fdb7e737556cc9d40d5e959e6507d
      569035abfa67ee96

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 47cdcf9aec36fdf3730d94cd
  ct: 9b123ac5d114b85432b6f2d3a92f314ab1ccb9a73cf409a86bb97a3f4e027ca945
      15881013bd3c86d3bb14f73bea2756a9b79bd5258af8c1e75b19b0bce4bd15fe34
      cdbd2b984168916c

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 47cdcf9aec36fdf3730d94ca
  ct: 3801a0d46364299599313 17c4755bb7081f57c15b4b324154ed63b034bea15b6ae
      5a3c7fcf249a3b05ea9331234e845321b1679395ceb60700ac6bb6fbd4e3119333
```

```
      f6c0c5f405eee382

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 47cdcf9aec36fdf3730d94cb
  ct: 1f941775fee2bd01469b9ae3a95844b859ec092fb4486f6edc4a47de5d9fee156d
      fab5f15002d0071bb91add0d5ca8fd6679e1f3610a0f95c2467628f955ba4da12c
      9b63c1d94738e6ca

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 47cdcf9aec36fdf3730d94c8
  ct: 35c30460d446e1748d86bce7eea742c97f162d12f3da0efec3ce7822ddaf1b7a6a
      02852bbffebcd68066e206c15ef150ec5b57916adedb7f5223900c4650bb05b18a
      985843063fb448e2

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 47cdcf9aec36fdf3730d94c9
  ct: 224c4f11fbc2b784c793ab062754d042acb23bbf7f855b038e9245897e48adacbc
      257effbad74c879f32584a20d24020353f1973ae3464cfa409fe18feaa91c191ea
      0f2ed76df84655ae

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 47cdcf9aec36fdf3730d94c6
  ct: be5bafef8edc97e3882abfb5de2996478f074c5dced22d38abe4f12f50c50d9a6c
      6df50e5d661dd87803c66f4839faece63d878bd7dc3f3af2fb63d2049d944e3b0f
      ad01d95771d94831

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 47cdcf9aec36fdf3730d94c7
  ct: 79c9a1841add0336e2a18f7f19d74541cdcc4fa6ff6cacaf2f9a90d4d1595db277
      6ff989ac4cbce10eeac32c6b0e3cb35ba73d9d72091c55dff922862f180514ed57
      0a178738f960c8b3
```

A.4.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: b802e65aba5b55410741d61e2953e67596bdcb7c1914097f13d8ed
                  98e87e54d6

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 9a51c255f5dddc18a32357434443938129f2c1a488d997e44ebc3f
                  e015b62820

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 40aeccb100d739dc7c0b8964dc560b436c7ccb71b665323f59e1ea
                  a442406c36

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 9d2fd647be76ec1433b85cea7cb741a9e44d939995959f4076baa1
                  740222ec5d

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: e1f52ad203d47c81b30b11c2695284a225d2eaa562e6672c4262ae
                  36711fbacc
```

A.5. MLKEM768-X25519, HKDF-SHA256, ChaCha20Poly1305

A.5.1. Base Setup Information

```
  mode: 0
  kem_id: 25722
  kdf_id: 1
  aead_id: 3
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 2a1c0a3745fe8a48fb62034d300f54dfe1974a5b2e169e580a8789cb1cf5fd19
        0fc00f3fd899594e01a8b15334b9f3fa03d8de44da86e19f5776850fb689e6c8
  ikmR: b86e76a59fabfc87b30cd7b1f7aaa28a834eb64e7a261c197b9a842893fbce56
  pkRm: f5fb01a5db909ac907ecc9524de9b9eaf4997dac7d22c961267c964403825160
        5a105ba7216669a8a1208ecaaf3a706fa7a7c4d7492260ca88c42a19732869f3
        b4c383477cd51c1da5c13a400244ec4b5c25ba350ed1509731bf801a7cfc92c4
        9650269405931b05c584f8737252141d2a9d1b02ad1b05afc18083681818e2bc
        324fc0403bb96447959a0a4aa874481f6444cdaa5c6f7010c841b99170d9b575
        fb2da199c038e62672334048d33ed5d84c6193c5ad69b92310bd1359a662da65
        db688c33eb2f98f627f4b4600b4002611693a0e581aad6a5454a424af00cc44c
        6cb09a8100838cbabb16e39acf88d41733785f531a141961ad64588e87d5c252
```

```
        eb101934a56f38316984cd6ea3a635218d560b5e0df4aa77a58d70aaaa0b36b5
        3c783e6eb59b1fa5990db51402c03a55829775a45be2cbc3f3914f2d1869ff64
        643ae777d74a47966537b7315d06dc29812004daa7b9a406b12cdb744bfc5ba5
        ca602261785e38939c530d8cdc33020b4a2f77761e64985271ca1ea4a0b5f0a7
        51704e705a94fd238c0770c262946758d5a5cd1cb82931771c4376f7887a1e77
        bd7b772d39c991de6c00093c87e5880bb82a0ea101b00ddb81c15684eaeb5c72
        784e0b1979f2c991b602b25a727b1ef8925ac96d0f993badeb3602b181faa8b7
        dfd38ba32c420d1b02eff996c8954c5e732cc5149b9c35262e27c25d1979cbb8
        77735212d7bbb759f72e54155260950962d475a3d7a1f354c378038a5633b0a8
        698ba579a88a403cb3cba9b3e563d3c25cc89b143fcc16a9284655253ec7db8b
        2dbb7b3e3a6d49cb220ebbb18ea635d6b2016d0a2f4b775d659a5ad59b9e68cb
        b8bdf0b69aca1d5670520552574b812b66d23a67270d1163a250a54c37aa3aa8
        68b318185412f84b11b16ebfdc3509eb805bb4536d63a920e0921c3209678751
        f9d782368490de2693aaf8390d7a2a3d831fb48009a104422889891915aad657
        9950a91be324755d299a30f8baa8babe21081ce0e0cc7f8826174c6d71b44e5f
        6c1d15f250b63b930c0703b22cb9d1493e65918ae3137e4e91c6ea9a83b90606
        228698b83480c0a77f72a3c628f48621b4b7ff497e5c7307ebc7586495b1724b
        158311421a5ac8539651c0012dffbb01f9350e63104be9294e61ba9889e17691
        c9c572c4a9cc8759359b2b4f73bd19f97fc935895dba7e4fe43aa5b629edaa82
        5ce7c1ca430e006228c4649de0414fdf5a5a53eb27965cb5840644ce0ab5c0db
        ab89f048b6677b9d8b8f933ab4f14b296cf184b9eb660c14b0a8a8c5c7b371a2
        87a0a67354c9295646e36d4b13c65eb2bcb90728b0c71e9ff801ccbb13119b5c
        d6380fc193a5baf1998b231a59c3517b196263694fb9da3904e67fab95c251c0
        47ac698fa000a045e764a3598f0cd84b83e3ca5366cf6f6ba1b8fb38166bc165
        466e94e50c354546bd912b3d6c44e2e46fb6c244e5527b3948aecb8a1865ab90
        ac44a6bcc13606641831a836be96b00a403f8ddc8e88bb9a1ad774dd251861ba
        b6bfd180ae7c2c94107259e7b5bbf92ca836b496aab97794bf3e5797013b1605
        8c7d7c38c118034c39201fae92c79773361747ba2b8aac31a9afc7b53a36d74a
        e3415e3526c23f98bfc6584d1069019dd977c37e950ed90f14f52991b2b28d0b
        f571686619612d7bc8206650c1d2fc9072220e7f4d4f557f15b33dcf32e5c837
  skRm: 3ec47fa82dd5689d27c6190e724c74ec8f608df3331ce331929e37b829676630
  enc: 26759c7b22923ea5cc9c78e3e14c8fc62dcb0a66ce44460966978a7fe9685e0c6
       d22999d99a3f112c307a6d5b2e63591f41e8a3516ba62908376d664557206e696
       ae870305ff6ba08125266bc0765672beca90fd5c6dae0d3ddad1506065a9d4f29
       7e0c3e70bb441961df26d7a19d79d1ef7e2ac5e53b32a3c7b4e07f2af2ae65830
       a3e8d1cb2ac1932fc19ec5434303b62c9d010645cf95a475913da5d77a282b884
       02e4a77ab17b09559dce8a96c67a27bea8f653ceaca3d278b6ed150fe936dda28
       b1726665c946cab30363ef89eb878ffcc74caa277a5dab1994193a67967125ebd
       50986dc16997b8f7484d7d0e27c79ff4b68201c1b4102f5a73322fd3da96bf655
       d90c9b1e6305e01ab1b3449ea3f458b0e98e1f2d1632825c3b30018bb5eefbcc8
       0f767d0b9e7f9f731e1958083879ebcc1b5bb061e89302c444a85eeed169b10d2
       520fd47b6a111914f3bda2f31d04f250522ba951012a629fa2cd2192583cc9abd
       75d02b7a11fd18056c414b8f0e0936535bf9b637c7e614a1ae9b9e907fe9d1424
       3f13625ec92a97599eaa491b9da918b586e27d34c7279205dd76cf0ecdbf60b5a
       ea4cfb9dca41069f3e2fc8f371a7cf3b089ea469d8417bda3149159992399ccd5
       baf776a0f8966d4742cbedaeac131dde853cb1fbb7b869a4c01cea8a487a2e52e
       757bf4dfcec23995e5f088804d2cf99c82f087454144cc586845d7cf81249e7ad
       919ea1b06001ad13501da118ee19859595015b4b1872912dd2d4f5dd854f144ae
```

```
        07038bd8bb2b498f8edcb1c70c2102af768d508a1b4237238c0c6e34a9c819b0e
        bf28f49505d374095b2b58c7a810cf1e806cb3c79af3bc84c8b657787804e374d
        f2b49be6ac510d43024e65fd031540a7cd45c9348ad9f5511b969be6f9c4d849c
        1428f611225b0d9a3ae341669ba645baa877cdc34c39f5975f4991a77f86eca2c
        25ebee63a06928c1bbc9513f35547645e835544c1e4a8f33d7f29c1cfbde6425f
        a05aeff69f373aa8a281c92817cbe5be9305795354efc71a89462e87ce83919d6
        79dcbfded88f7fff9177f4b49e8a959d9aa78b63feb99fa56735df0f4fc253653
        a9177f767b307bb2a9e7e4d9042f22cc6c4f177db80efaebfef8a3baa6f142333
        5c830308c2496118263f0bd361d93f8b4e75a7cba94c2af72dd13ee8926524cfe
        9df14f79165a3498b9fd631cbb874d25b11315f9acb442512561cf7dc6098a088
        74fcc704cdd5e84e57811a49e78fbd56e5a8e767617321c295095595ea2b0f4aa
        ca30dd38749ab83532be1bdcf4c32a119e035558bb427dbdb806b4e15cea8df3c
        098728c2b5e40209c5138531db1b660777544e6a014477a7d1b93eb0f245fe9e7
        053997c10504ef692f21639c86d8926ddce6886d0c39eb7c59357ee54f8187101
        9593713f4a6df37bf7003358694cff59af9872ca02bf762e20499227dba2f5522
        03459dcc69780ef08d9bab4140d96e1c478f06b63b60c9bfb10d90e31d47570ea
        949ab8e9b99db6ec2f8a2a77dcb25cc36b733dfc09b8299a9d7b19e68c09ad827
        03f9b47d34d1a3cbafe42c73f57d0e
  shared_secret: 58200ed1f137bd95a921bb47f6aaecf2395b26f7fd24efd3a5ffae4
                 849e8dea3
  key: 131c2ebb469b909a40915914afd7ff5e638888ac7195dcaaaef8f9a84f0e4030
  base_nonce: 2b7a68f19e6cdbd43dda3c6d
  exporter_secret: c5362ef3c0008d0e573000c5c25a3f62a3bc7061cd41a384c86c2
                   7b37d945bbb
```

A.5.1.1. Encryptions

```
  sequence number: 0
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 2b7a68f19e6cdbd43dda3c6d
  ct: c5c591f99092d5e38df0a52699af249c66f8275a863423c076de8147a53e65cc58
      4041c963b77a7e59ea93841b1339b5efda8909b71f74bb0073ad62e899de310c15
      66dea2fd29eba377

  sequence number: 1
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: 2b7a68f19e6cdbd43dda3c6c
  ct: ce339b2b956509cf9a9d3d736e8529f4eb87f27483e0c647869bd1d32c6c95ab3f
      f3f151abb11f863e5ea7cb852dc0c92346b46ac340ab390f8d3b6bd85d5d2d11c7
      7499e006e36e3699

  sequence number: 2
  pt: 34323635363137353734373932303639373332303734373237353734363832633
      2303734373237353734363832303632363536313735373437343739
```

```
  aad: 436f756e742d32
  nonce: 2b7a68f19e6cdbd43dda3c6f
  ct: 94b291e1575d77fe9ff039079f597baaf6dee9985693ddd21f8d9176aa3405453b
      29c90aff3588a83688f82e86fce6489fa6fb6a50161cdf546c2a658d5e443ac1f5
      3def7d0d3a512583

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 2b7a68f19e6cdbd43dda3c6e
  ct: 823863656250abcce5b8f0c737aab253644b6ddfeb1070d1e5cd3d5cfac1ba3c92
      e384daa0a10003217ff5eb3fcfd54eb3598e6eba5bfac1ddf6f070ec2cdcfe376f
      e1b5e42f79ec477e

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 2b7a68f19e6cdbd43dda3c69
  ct: 31c9ffe256d0b90c425d0cd438cc93652319dff3716ed07e73a3aada21ca07d960
      6917d5b31cfbf5d3ab973492519586319df6dbe9bfdeee6fbdde80f677d44f9c08
      72cca8a230ae3ab2

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 2b7a68f19e6cdbd43dda3c68
  ct: 23aabe32ffdd4b8973a8f90f3f44f892691c2ac85caffc269faff453116e875d38
      462a48eab52d790f6a17ef2068e26334735c94dceb26b40b99dbb9d567bde3d840
      db06b0f04be3fcde

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 2b7a68f19e6cdbd43dda3c6b
  ct: 884b02a2998a88cf6d04904aa2ebaafff6bd8ac2a0fac7b68e27676ca6b0150165
      992565195f3b3fcd0678173ee2ae08c127208e93f981890f6b653b12f027477ff3
      d7c866ae5d3d74b0

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 2b7a68f19e6cdbd43dda3c6a
  ct: 0f9ad97aacf1a7e862c2720af04d14a44d416b0828f4e4b12ff21ff721876312f8
```

```
      a2508d76e92e5b1cfe3963da4cb598ce7c2ce03e49d0bcebc05e2529f62cf1aa57
      22b39c4c17bc84b8

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 2b7a68f19e6cdbd43dda3c65
  ct: 30cbcf8d2d4c7bf76abfde1ae15e24a24ecbc128bb0649b6dbc50e8102d46f8a8f
      d39e0a82e167dc1f064616a2eca74ee9660d8b4fa973cc2f20b5674a9c212f17b9
      f0f75a45590a3ade

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 2b7a68f19e6cdbd43dda3c64
  ct: f582d7aad5e83ea71a76b1b73a468f3170f0647ba3cc433a7e96733eb48f982f0e
      fab7466f417cdfe78c239aef5dfad026dd8dee092cc8899a38a143439d396db4c2
      8a7eca90469e97d7
```

A.5.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 5a78d37f40e078c17ef43fa40963f1ff7dcdee56e366da9099dc18
                  1c3eccaee5

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 19b8f5e1d7c02e44ad99d8332124b5c71fa9e81c5327ca485054f8
                  59e442bde5

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 60c955a15a48ea5f98cb86f54fb13b840c6fb9c676f72b2fb612c4
                  a096ddf796

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 0bd32702ab7d370d8e334998be6ae3e85c63aa9ee0aa46b8ea0414
                  b2951a1934

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: f77f100943595e59526fb9753401e57b86630f97ad99e6e9d73c8c
                  272a4ad2f0
```

A.6. MLKEM1024-P384, HKDF-SHA384, AES-256-GCM

A.6.1. Base Setup Information

```
  mode: 0
  kem_id: 81
  kdf_id: 2
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: bd1207854ec0963347d5218f900783d6ca0ff62c5e2181ca5a932e2d6d8d96cc
        9b092a9d709468d10f7e8ec8d9eccd7e7a647d351133e2a2f4b438154d1dd708
        50af7f7841c1dbd0699feb9852d99c08
  ikmR: 0fce198c0c1ccfca5cd1ca8bc495b06696cbb8c733e708ead4531b2b294c38d2
  pkRm: 72e98103195375869acaecafed5a70808b0ec7603139ba6ecba9c6335510f088
        12fa2c3ed429b707c16509576c9268c2017ac3ca616ad8f32f78932d91974459
        d103b7255f3b41c4c19ab024921a3f114b6eb56e829688eb97592653a1849123
        45c4a5fab78645440e1459b1f6e24f93735148f2b6ab86a1c2054aa56abed73b
        3f0795b39a22cd73d254365c6c387ac9333b570d07a9688024353b553a5801ae
        0893bce24b0f7bb02914444cc88fba120e671aa8a120c8baca2f241003d1fb86
        0a259fb0ec6ab60a9b44d104f4312c51c02c53c685ba67242054cdefe97d1507
        2c15380a1e5b18a3ca423f82167e9b9583fabbced09a3eea90b31b3c15022b62
        c46b43e3675052ad1582c5a5c6746b287565c007989c399ff9774389774a9700
        316254c02669c9b3ae5101c73a9bbe0e601038aa7933092f8164c5ad2319d4b2
        72a3362b45bb86b739ce3c4ccc410a67c309ce5d131f1d4c11e648855e1974b4
        c51e0cbb9585e4bb55119428e4ce0a908b07c455ed0561cc65ab4fc0bfff8a9d
        8235772f417d95dc294ca54d8e015b694bb479223ab28ab06ee74683a9182969
        9a98acb19cc9803877401889b63c110b55a55f19103fb5bb0dcfe66b75520b2f
        b94b48a7b2968508f7bb8e4ec11f153ccfcf2a474eb833911c08a2f316678153
        d2a68bdae3527dec949dc732692054fd359f1fd467968359996acc1f58bcf074
        19f1b6354cf74339b64533dabd499423c164bbb95741d80aab6f5514a90a5b73
        46330bd0aa8d34a27f363609132cc3b4a74a04139dd1b71d531e9c351960f107
        06f5be286cac7728648516283adabf6b12a75b069350bcb0504a3c29d7cffbf6
        c76919913a8622c7a121f6a757b6b14a17c9a63b6a432c8773d5e04ff5846605
        9b6c5d543f031c372a00702f5c6fd78c8966e93d90d29fe22a5c55f8900e1a1b
        f34881a317412ffa6393f9c48c680ec52c74ca986313e5326f13574211a4cf26
        a3e1e426d6d6266dfba85c153abefc2da223853863237832a0181c7fe1703c07
        b63cfcf57b476353a435ba24ca05505b311dcaa861eb7dc8eaa44511afeb839d
        f4c70de66512e799aca1947f6a0b207ac18c3ca5054b3762981c2c0156809098
        6fb4f91b6d211c70514ccb21cd94923a741196e3826f2659cf5047abcfd83e0a
        23906166a949c9c6cea892537b95db2c0fe38c888db9256a43384b826d40c09b
        f88149bef83b0aba2b68e1374bd6aa86f334e8a69f0b42774ad2bccf218fc865
        7b03303ba893a518a063cb27a94d84c25a414ccb71843f25bf3db89db82530d0
        522dbc239ed9f0c1ec606168e40692b1301b666141e04ce7a6665a294ffdf61d
        64a6b1adb68987e2a4694a7d3a7cbae6b296e9d55bb3bc00d9b4bb379760fa49
        99e43ac1e4383b7ae17cfdbc9b956caded4199019571f36194c56b1b95d74fa6
        a0c64a941cc4771670715c65921307c4967f14aa9f0260d3a17f16a04aeca152
        3758190ac08ec3da464ffcbdc2e95ab334a05ff88b07eb9c1a2cc62a10a26785
```

```
        a3d6266839e5a049246390682877b074711a55478885dd968ff481ad4b44389f
        85b45dfa7f5224c96d93c470f7a506dc1de37a375a50635cf420e0e039877033
        c6ca6fd4eba113155c08316df5a0507c14130d9ac546a03179e700f721b3521a
        68e215999ad37c096a6988c514bca72887ec5ed4d4163fec18eb906a72e36c9a
        fc993a3b487793284e31418d8001e18431a36668ef750bc3842780d40249da91
        66526a1114348e153033b64189da3fe12c8aea9c31652917a8211651b0182d46
        132203952b38645e1ba401460c72b6c0cea2561d1b2392329e65b0ad37b04c35
        f38ee297a515337bf694c99a572444d4930f52c0082b913e190a4193c25dba19
        dc027d8c79468401480a5c628c041ccf2553466294c91aa671ec8a79d465876b
        75e3a381dbea82a13139be6135b14a4d42199098588dcd0c24139b3c2397767e
        e18a7bc17f8d62612884c53efab3867b8af6184d6c9a55c91bc54a7610f628a2
        de86b98ee8c561cc4b334a7455aa7e67682128a7adac93c47666ac167462b71b
        a33c21ba5e17a4b856a292ac06bb2980e9fb4200a22e7ba40dda73868b546966
        2cb099523eba0158e160a1c82361d9a6b55d931874a3376ef87792a972368636
        8ee415ac2431fb0814190539714fab40143818c3385239108837886da809618a
        04c6d17df540ce46f755cdb12b168e87d1cbbefd1185cf82951caf3aee8888a2
        8e1d5b7fa5da17ae1368fb2e06d4bd14f4c0aa24c7bcae7233e5cb55418c0471
        a5f56c4b21832e60c2f351d8362f616568f207fedfe2ea5cd6a2def2f79d3ff5
        e7
  skRm: dbdae0423ba0e5db3d6322601b8dc302d3051d4677142079c7bdf441f4c448dd
  enc: 6f422a46a6828949f974f0a88de8325984272267a95255b5a807c38ce27defd18
       2334463d20cbf0f1ff1014719dee8ecd6d9a3affa01f91f2218195405d65acef9
       167c930954a60acb7e48ac6519098e444d7ccd383fa0840f6bc5a9d775172cc69
       b720777f8808bf8eb89f77bd5ed8c27352f8d5107fabbd75a6c862cfc9c64a9c7
       109ec7beeb458ac5b8b2193cc85c8897983a12925f6ec72f4ad4464db48ed1576
       c74d0635f4096c3ddb66883708805fcc5292186c570663ab3d2a73f7f2ed0b2f5
       de77ee5437208f2ee481ff7451d158ccd6820efc9d54842e2e96ce7489d801ce6
       e2a8bb6ed3108fba63232f5aab57181adcd4c3fa60f9cdcf9cb8c88374de47ab4
       5c9f5d40af1b9bcf695c033c9017a3c6b6b5bfdd73b59334e82d66e766b394ff8
       5f298ce1b69097da08f6f7f68118c1bc5a0c4d77669280b9e8525ac998ac06e94
       0c12a76427a787afb78719178acb627cd989b51b3b77d3536697271b3f951930a
       ae5f1c23401f0fa4b6e617bcd07e88e1dc1ea04df1bf7de3a5162b36aff6f34ed
       2e776cecb7e0d51bfbe50b2a0782a77476c455196bff38a84732dfd588c2cbe63
       6d604275b4b1abcb0b8a2deb465c0630ecc7548e4ad7f1f1713db17722896f9e3
       784c8a0924e06a729a78ed3681bfb467505e5812cb7fcca5a6f7962d067a843a6
       8bdbffd1d3e40f12e103c4c67688e947c41c57fff528d9e0f49dbcb2f1fc3fbb6
       0dd89121d2cdcb34609c12f5034f7000be89f78be256fda8ac29c492b536088a9
       efa7e61441526b73c2727f49baba7da735ffcd41959badf05a9af6521c2966005
       8fe8914c61b0b613b3e813b7ec46b193b454b494696b0f95d138551ad02a5ab80
       ac5da861ebc5a3c7b8b46989f0bb7fe763c40b0f44708bd7622321e846ec6c894
       6dfbd7e1aa80a57483280e7b516cb3cf97c33f0ab7adc06214b74c685eacfb085
       7095fa2a532e1ac8176e43f97ff8ebbe654f1e8156e83eb23be79ae2d9f03777d
       08afed866114854566c3cc516fdbc293a40a3d1cab4b090fa7e9d1b4cda6ac10b
       e727d6880510743754829196cc22a7f9e4ca0e669ff0fe470a229793ef3f39208
       c0fd3a90206b8e465a7292e65f24668fef75971553699aa500e4dde7f9c61163a
       ba398519db6942f46cb872318bd09c77c671cdbff693e1275dbfae4404be73b5b
       6154d0eb095bb279d8de7f85bcb3f3f8b025e3e811fe2cf2f97d86d53d3009993
       f550a3283c35db0a99b906218c8b260627e8cbef3448654530f7a0987df54bd56
```

```
      7614844e5fe1f3601c5243f147d898cc3790734ab62be5e0a3e13c7f03a6098fc
      42f4ae0055ffddf12fd68cd04ed1d908517385d8a323a2f8c777c04e8afb4978b
      eab00464b1cc2670e3d6810e923a5628a382f2ca7232708617fb4fa15b5a29c76
      da406e32e7f108d3d4db31be640b621a22b1055104bba2b899f2a479bad73e0c7
      99657e629c72a1a6363346bb49b39ccf1cfd0f69f22bfb52aa748e7920d9eeb6c
      cddb0483107ec2daca4c482441ce9bf730df1f5d507b107e76ca61ec05e9d090c
      98273cbeaa7212bc54a49ae2d13fb9d25d2b0f463acc84c737f8b91eb8a5ff977
      1539192c5c75aa8d599e205fc661519b9b69970ebc3b55755611ca618aa0260d8
      1bb15773ca4ef38d5d6ecfbb511b658d5196691190eb22e014e41a8caebf0a833
      57547f8a13c8cbb71478ef5a6578d551536402614a9b58944e188ec7a1f103916
      c01535cb3c3829134bbc7417580b9b25bef2d0d864f532e1cc83f13a9396bd971
      1e9e1bdd8f2caea2190efafd52c0e3a386ddfd88aabd2a88dd130c3012aeb41b5
      e88fb744ee65768aedace0e957bfc99793995788142602fe327f1b2559dbaf5e1
      6a2397199156f4cccf6b83e7d6e18ef7cd5dc25d48b03716ed3650385e83ea784
      4f759d131d8ca470339f92d34828126c77d57d8281eb247eca8ead23f66697e6e
      0a106388b510bd694156b29310070662470e0c3b1c479804bb85f8c3867117502
      f135b80ffd3a74411ea5ff02b7c8206b0302d61affc80862f6ca07cbb7a682f87
      287a294d579175b7b5bfcd9fe5edcd920818d282b3c1a445fc5843239f58be42c
      ad99ddf10d5e53664e627922a51d75b77934c4083391a3437be813214f269d24b
      e0f8fde3a956b1e224a3e08aba0efe8a77b0a134160940b3f5879b6f9734845ee
      e24ae7e350dc8ef90435fdf3b145fe16e1aba8b7358c62846712a324d3d1b9f51
      e1ba5045126369a38bd1e2bba241467a2a4730ffd21cfaade48b17a470c3a5269
      a5c236edeacef9e4335b7b7b558ea45d9e0179010ab17c26c16b4cd9f6bd466f5
      3bc0be8ad23abe9
  shared_secret: cb959223131df11c3a3dc1da2ff8670249cb41be2d0b399a3706d3a
                 23b158bc7
  key: 6f5b0a62d262c2cc2026a8f38b3879abea8042823ca193573e7154953d22dd64
  base_nonce: b057357da81f0102a835a35d
  exporter_secret: 8865b4be7a2544efeeb3cceb2d0e010adde42cda0fd0b7d4c2230
                   dad1f9c095a87b0ec6ff60bd5d76a1266d75ecac133
```

A.6.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: b057357da81f0102a835a35d
  ct: 4c2683632b3d5fc13457a54620085e49e300f1bd03408ad7c6821df4ec8168c2ea
      bbf935541fdeb235e97ae537d1280471735063a5b922746c19d14b5a2830f38fd7
      a8804c057d9bea2b

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: b057357da81f0102a835a35c
  ct: 89a0a3bccddf1ab32b3a68a2d4db71795c2e3299ff01d060f06d551f7ae2a5364b
```

```
      9e0a752438b9d6e1a7aa0a7096d07cbcc2723de387272e60cd39fa54eb5d43e169
      9e267652179f1659

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d32
  nonce: b057357da81f0102a835a35f
  ct: ff5b4c863ce641a675fd701700e42c1cd84fe5dd943bf342ce758012a16229944d
      dfac1b8c8fb70b55c0fa952f7e7974a4eb657cba0c8b9f715187432d88295168bb
      a9e0ebdf6ffde48e

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: b057357da81f0102a835a35e
  ct: 71d49e78762144ebb826874909a6424ca6fe4aec272fe8e01274af84ea4ad8c36f
      a01715f166ac9693e7a836f1f828b1119423357f824fc9aca9f8d68e2e1520ac56
      2b0febc552e808e6

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: b057357da81f0102a835a359
  ct: 041cbf5fe60ca05e1315c04e408075a0fe75cd06fe6f3f5ed5e9da1b069e6dfd8b
      88d9e94fbc4ac7899e56a99758bd823c351ae4dd4dfc50437e1c3e7da6266d8608
      8a4a298c1780cef6

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: b057357da81f0102a835a358
  ct: 91364b6a6694800502f74f167b20de99fc8ca4d94de6444ed33ba48a88115ba4a0
      463bc4f7bfb7ca2e58038a64ef834edb689bf1aff3a51a4ffb43f0593e0ae0815e
      7bad7f5a304e2253

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: b057357da81f0102a835a35b
  ct: 0b1ce0e66e9b8e873a94961c7e3d2dc5257b7d3f858558fd74272b0b7d6f01c78d
      7af5072eddaa5b060927bc734c6b42276804b7a71e2bb8802eff1a993dbebb320a
      89b63abdaa29b818
```

```
  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437363832303632363536
      31373537343739
  aad: 436f756e742d37
  nonce: b057357da81f0102a835a35a
  ct: 91c8ad3df0eb8efdc33b5956b13717d59ca714d5e32b26f7000ae77208d72e3425
      eed82ac39deb182e494382193c80f3a34d45d6faeb93851995438d83e26b666b8d
      740d845b1e00be84

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437363832303632363536
      31373537343739
  aad: 436f756e742d38
  nonce: b057357da81f0102a835a355
  ct: 1e3905368352af376ccb7e252ca1b2eb14d2a255956153892dc3c645b067b4c242
      d2c69bdad6de0cf3355ef09bb0b1b4b34f4e536ae1bf5c4a805882bafac53ffaf2
      82eca98850aba17a

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437363832303632363536
      31373537343739
  aad: 436f756e742d39
  nonce: b057357da81f0102a835a354
  ct: d468a6cbf85f220684c594727c84da1dc9c27bf9a1851e221f9874a12e579515ba
      ce2c07325f33b793e0916fd91124318cd3fdbbee98d4b1d15dd8d8348a6be16600
      3066e1c6cb12ad0b
```

A.6.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: bc1c15452944a0d0db9195d24334d6862d68a3d7b18d35c756978c
                  d649a6ac31

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 3e2fa8b88788690e13a139707c4fd764847bdd4d0d1902d64fa7fb
                  c12c151ddc

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 5b97aec03e9d3b352945bd83ae054a35989d671edab320d8b8f167
                  c6e3a43843

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 25eaff2825a9c2e57e18513f054041afe22ff7160b30e8730106c5
                  787ea7662e

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 82b5f6f11791dd39d81b7e7396e8f7c3d9a9a8341ea43f7cdbfbb2
                  75a95dca5d
```

A.7. DHKEM(P-256, HKDF-SHA256), SHAKE256, AES-128-GCM

A.7.1. Base Setup Information

```
  mode: 0
  kem_id: 16
  kdf_id: 16
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 65c72db26bf7f1f50d18a1fda71905653b88d6f361e365b1c35fc2a7bdc40cc0
  ikmR: c6eedf3e84fca93ef3434208f038538f182693825a803f8a3e5469890d893090
  pkRm: 04b965ae2a0c28be5e8d8e44d4f47f337bff11d62b40d184cc09fd3d15613c9d
        ee8895a226b1f63869b35507094789abae1d61cd323107b76e902d8a81413c2f
        70
  skRm: 5822d76fd4586619a9cb6c0c8f823e0544d89ef1de0e6cbb21206800708bd1ec
  enc: 04fd736e604d5c501b8348cb2e2a4468252ee669ad5d0889c4b9a63367c88f201
       a20938fbe98538be37bc44284185c6c8e8f579cc6a3bc3d3b397b6d083004c44f
  shared_secret: 2c3139230d3c69f7f653149b4b036355920bcfd5805705a7640be64
                 fd9b11ec9
  key: 104d43e2b37b5d843fdf137d36c765e9
  base_nonce: b320e8cab81d613258b5686e
  exporter_secret: a30bc8dac89fd0211eebb68d1e765672d41039ef10df93a56ca9d
                   15755c65b2a
```

A.7.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: b320e8cab81d613258b5686e
  ct: 593668f9ca772ac7332d676a71fc9736c3699cc0f8cf51ec6c2d6eeaa0b3a0daab
      2774cf703ac11eb2b89e75a12aca75c86b218c9d95fa3f1155c429537cea322c5a
      fd75e8af2be46687

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: b320e8cab81d613258b5686f
  ct: d395181fa659e7996e199b7633c661d4e9ee7d9769658d74dec855345daafedc1c
      2007d53c6cb3d0904206cdefe207dafe07d68ffc0ce3c2f31d289b2456908c3e41
      062c1c7bfd00dbe6

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d32
  nonce: b320e8cab81d613258b5686c
  ct: df57f9209852c0e467c5d27d2670da7046d12a2480d85356f321e1eea067fef3d4
      015a97666c7207a04c5bcf69a86dee0d62d1cedf0b217108c432131cc46cb54cbf
```

```
      32b55f5c18dce76b

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d33
  nonce: b320e8cab81d613258b5686d
  ct: 3791919f57eef136a8582b567fbec1ddd4b885225d534848ba4d0f6f99d1707587
      429450466c5a9f95905b752159b1b9924d53c40a22a4370bdbb2df612fbcb2c8a0
      c4e4256fe9166418

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d34
  nonce: b320e8cab81d613258b5686a
  ct: 55f5dacb7a45ee03c397ad3f9e63717ffc0ff0c96fe3a391f072732255f0e02ee5
      f538feb9614fd46cb6d2a5e82249374d30e1e94cb62edff892d8f32b6fd8234fd6
      f628dc95b374add0

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d35
  nonce: b320e8cab81d613258b5686b
  ct: 36de6f1c317cb22edf80d8c98f639029e3d5d153eb10179368ec2b5a6000c980af
      84763569d3336fb08e3fe889787b9c70d438a9abcb53da89c2dcf2f9646c7121e7
      5f5a72cbac02c2db

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d36
  nonce: b320e8cab81d613258b56868
  ct: 3c139df8b416303544f068c9c5f7f2e6ae611a9de2a273eb9abd52ac06c6337d68
      1a8d1e097d4b806e81a6b8ae6901293b3ab3b632268523ceb801febef378287cd5
      840fd1f46976b551

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393739
  aad: 436f756e742d37
  nonce: b320e8cab81d613258b56869
  ct: 40b53d28cf519078e5c0120b2684b485a2f1317393c0fff02169bdee118c0abfa5
      c939f1d53de4684e7035653b1aa4bf28afb7ed39f4c6bc2e8c31c9e7ad1327de01
      36525beaa6d96339

  sequence number: 8
```

```
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: b320e8cab81d613258b56866
  ct: 9f385a36a195bf529b53b422c8305122a91198ea46799af237bf5d2c5d405e4398
      ecd361eb36d2d181e064135c4ddc43a3e479f02b25ef9d9b79aa08a3575748ebb8
      d17ea050731adc85

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: b320e8cab81d613258b56867
  ct: 4bc25005814c4dac1d6a75620d52cca8809a7a62ac67d77d81e20ed55ba7401f69
      05c794c5c4d591588b1d83644f1ffac18cab8607e9848c1f856f7cb2701e6d982c
      acb8ff0ac207f6ca
```

A.7.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: e445830750c592c6ed3170d16fc1ef1298812285bb8a6cd06646b8
                  d5e854feb7

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 832ed1c00b4111f4d18526171750361c178a1fd819f545e9be73a4
                  51313852ff

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: dbbbde553ce79f1847abee84cd5c598b9b0a2d4d130174d8e272de
                  22936ef6dd

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: f59e918684d7abbd5efd6a1328fb5a22d798a4b76ca01ddb82e299
                  21f012c973

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 1583ea91298b3b4f7f0440d7bfc83743d919941734e1d3da1a3901
                  e1df3f4f95
```

A.8. DHKEM(P-384, HKDF-SHA384), Unknown KDF, AES-256-GCM

A.8.1. Base Setup Information

```
  mode: 0
  kem_id: 17
  kdf_id: 17
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: df490f3d80254f2485bc8abd4225c0834ab1982ce844a6b4a3390bbe9f348b0a
        82ca464297bfccfa8b2ceaac6b43e6bc
  ikmR: 1569d065e398456987a4a76e7117d97767cc8aecef8efebaa3ad5aee78d44f5f
        ab347ee19307e6804ff32d8b15a3fbe1
  pkRm: 0412c5d064adef237657fa743d1722d505af30635b96b977887eb3d1a821190f
        3d425109dd2e452aa795421301622fe12abdb92e934778be5fc86cbe07c65762
        4d9844f16e51cc1745b74d0fdfffeff23289340a812f002b2527e607133074d2
        18
  skRm: 8871021324f8190e50abe26cff62404778585a56d8712ff28afd99605e898d08
        b580b7c8f18fb166b28b1a6584662b96
  enc: 0427d6d80a6394078f3b8f8cb86b0c38e1996895672415b313a8ebbfe9adff897
       d8eec659efe200b5608a43140059fdb3f6ab0179c5cd110adcf2e5caad5a027a7
       eb86b18d2ade59de94bab544f06222f49ab09d8d68debac3cb67ecce8bbcad9e
  shared_secret: 8207f0a43f67bf912e327f0893e5a3b14314c38eaa8604229de4c03
                 3c6589e3bbe28b513aac127e85b4830c63daf572f
  key: 3ac9e7e6bcbc65ae622fa26565263221985bdaf6277dcee0c883759ac297cc1a
  base_nonce: 3e5d5affb035edaa9a181e27
  exporter_secret: 2cb29d9cd269212ebe4453fee3c3382f0ad11a3236a330ff91fd0
                   62fa2ea2f2ff02a8e3136ce38b2c053b11f05996965e33e636880
                   296accc652cd39349cb736
```

A.8.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 3e5d5affb035edaa9a181e27
  ct: 01b56453319ac535a38bc1a82ea4236f670f431cfd51e908e23e088eaa1b199e37
      c898661a288f24750f87d1b1d8e16b38fd3ee9159eda205336ccde14a2e6d38e99
      40441c5d86d5151d

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: 3e5d5affb035edaa9a181e26
  ct: 956d4226ec8c7b3a8985c5b03363fc44f2dcd12ec7e6b8f46377e45eaba99256cb
      a06431299046738 90b236ee192e99ff8ba104655dd4a52d106f3474106416ff33b
      864befec30bdb0c0

  sequence number: 2
```

```
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d32
  nonce: 3e5d5affb035edaa9a181e25
  ct: ccb136489b3ce513e2280b6235cf740daa62997494abd526634c130f7c12bf589f
      aa43f70c02d0d6ec02f0192eb2a65a4d5531facff2f0d212c04cd5b7f43b4fb2ff
      72727f55d6b5fd11

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d33
  nonce: 3e5d5affb035edaa9a181e24
  ct: 580748bd478c4c88672c327c8b713ffa7cfa1c7a758eae328c693eb776f7c6433e
      e74a780f5af8c90df83b6ada2b3938ac82cf835e00a4209e978aad6f420f47b6ee
      43142dfef7346e1f

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d34
  nonce: 3e5d5affb035edaa9a181e23
  ct: 2b6cb5dfd22e656c50c9800b46b5d6e1920327fee06acb2754f6c694cc9ab3531b
      05cb98267902e772a8491686948b7a65103f328ae7d3f47af7ea57c0c5900acbbe
      74907f45db29dc6f

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d35
  nonce: 3e5d5affb035edaa9a181e22
  ct: a24127c3441e759d4fcb67c259905fc7bf7f97df089ab8e3581a9bb645df868cec
      8aa4c0cfbc3353fc4e06fd692d7622d83ea19ba4a4aea9ad69efb8e5052e7f8c46
      ce60beabc96eea0a

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d36
  nonce: 3e5d5affb035edaa9a181e21
  ct: 3fcc157f457131eece66b090d3d337da9ce2db7c92e638a095b07d0c673747c33e
      0281aeffd6ce74c36402f2168a00293abae163d3af049fe4457879aa2cec1c5981
      48811e8ff89cc5c8

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d37
```

```
  nonce: 3e5d5affb035edaa9a181e20
  ct: 95049bdd0afd478adaccdbfc6a32af9dea96c526ebcc5def2211ff2d2af2e1e2b5
      4f21c821cd30252101c8ab11f4bb221dbfd034b1c7e67e0c8b34126023fe6610c2
      8594a4fc96046954

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: 3e5d5affb035edaa9a181e2f
  ct: 57e02657267287ba37d582ea3c654d845f9dfdf1731807a0e52d37814b08268e98
      95f81836766238ce47f9690b9f5ed99e475cdd19ce130b3f626bf010a14063b658
      02b1a576179b6c6a

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: 3e5d5affb035edaa9a181e2e
  ct: 1fa83c4ea77ee131919daf10ad2b889bedde85cf433478a56dce8f85efd8b414fc
      76cb62bcc573a89dc14bc611f413ce4efb1b1f4161e041254508def59ce2d87894
      6f347919a79cfdec
```

A.8.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 874efb72c977692c78f6052d686b44c6d1592547988e969d9f09c6
                  46ac537b33

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: c573d286aa300d3e85f0fdde1df31dc35328b4b3a973f12b28f4df
                  7196444d3f

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 1f8f367cb8df3931c51ece78c8ecd337cd044679edd9146548af74
                  522704e696

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: da682a54fb0481f0796436bfdcef0c989feb64b46967201aec453d
                  f1a9e3cb4e

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 3a18e24424a4ed12172d96f53593318398d71d3b49daba1ad138d1
                  f8e4eacb86
```

A.9. DHKEM(X25519, HKDF-SHA256), Unknown KDF, ChaCha20Poly1305

A.9.1. Base Setup Information

```
  mode: 0
  kem_id: 32
  kdf_id: 18
  aead_id: 3
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 6a83220f8a55194c8d8621531a1af58a3e67a9d4ad6ffaa1f04ca52f5af6dc1a
  ikmR: 97b023835635fbaeca0d748871b9a420865212e74fbef3d942c331e147149560
  pkRm: 6210488914aa067e2019db9af7f70964601e9e64af54cd3b219253e622e99062
  skRm: 85765ddffb3d34268e05ac28213b6fbef25ae7a43fcc8c03cd6e52977fcd5ee3
  enc: 2ab42ac5e099dacf517d69fcd7e6df0c5a6a9e79e765f5c0c33e1437f9638e0f
  shared_secret: fcce4708329c0abad769b20a916009149486bc62798ab52210820b3
                 353d86182
  key: e12d5464fb07e0b41b917fbb8a28d02026c6233660e94046d64e9a9ab1d9f137
  base_nonce: 01de599541be16789d9431b5
  exporter_secret: 737ce6aebdc271c9c348894ab8e6ba401c273a2822349e7b18cb6
                   0de5f601df4
```

A.9.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373436383263
  aad: 436f756e742d30
  nonce: 01de599541be16789d9431b5
  ct: 5829095764d917cf36a75a6fb3801f3659b6b5910891efbf0754cb9f79eec14a18
      d171c9722a55d0781042fb2e2314071ef1befa5e6986d9eb485a1b68d4a0889543
      f0e337d4b2f86592

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373436383263
  aad: 436f756e742d31
  nonce: 01de599541be16789d9431b4
  ct: 4b522c648ba01f8da28a4589b820cf93df6c48170fe99ffc6ecb9406d2bcba3aa5
      dfd01e411faf8bc5e8dde23d7dd00052df058a153bc3a64fd5dbe36f178fb9f8e1
      47daa0af1ff6cd9c

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373436383263
  aad: 436f756e742d32
  nonce: 01de599541be16789d9431b7
  ct: 635157fd31c210c86f000d89b454e110953820cacc8331d8b093797cdb2335b15e
      595f7837f6c6c9ea7b48811856eaf4eb7023f7179a1c22b2980f570ea3f1164d19
      fcf87bb7078ce2fe

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373436383263
  aad: 436f756e742d33
  nonce: 01de599541be16789d9431b6
  ct: dc783bdc54830dbcc7305359446a06913ba396c170898c34483b11da1183599479
      d2e41b3ebb4fe55dd2203ab6472ef9c4c3f5c6d8edf66c8b846a23bab60702e0c1
      52e88ebadf2292d3

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373436383263
  aad: 436f756e742d34
  nonce: 01de599541be16789d9431b1
  ct: d7683d570715b84e656480e2baac9d9c9b413445af7457b0b6c3baeef3bf83e547
      0433db5d046c64fe1d1231e463d6257929f816bcbb25a02960865e866daacecfa7
      746541f460131d1f

  sequence number: 5
```

```
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d35
  nonce: 01de599541be16789d9431b0
  ct: c5fcbc1c85817e757519b9cb260b3b05de710233c6f873c01b53eed14799a2b73f
      3d19d6570b1730d2007d3e03e01fd4c82617a8d01688a6e633e6f96411f1194fed
      c43896cb29b4b3ee

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d36
  nonce: 01de599541be16789d9431b3
  ct: 7337b2e35d9db06099d88c8a5395505ae9ba20b6aee030eeff14fabef1529bb903
      9ff583f9e7e3292c1b3d1d206725740f33b73e156200fd8bcef259a818978e6580
      04b05c375fee9c83

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d37
  nonce: 01de599541be16789d9431b2
  ct: 8fbb1e0ea0ad2c9922cb9ddc2a2216f92204323e24618a0273c81f2cac1c13833c
      5410675e6c4794eaa3dc54612ad7062dcde553021a01d6f8f5414861548480 0d09
      14bd65fce7a61216

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d38
  nonce: 01de599541be16789d9431bd
  ct: a4a9be8152bb3bb106ac2a02dd85ff7ad46eba0f5ed2bf7e4deb19c1172a35f034
      4030aef3480d139d3d0e9bb62081adde10515c72572334962f8efb1013666b9205
      3a9a227d5c79c7ee

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437393
  aad: 436f756e742d39
  nonce: 01de599541be16789d9431bc
  ct: 60ca29cc4f805548b0a28175769d5d2f998e00e8448813ea016c7f1c74fb60e56b
      3827089c06bcaf2b734f1b91ab83a91698ec2d39f1b375ba1dd40f23dd0234f5d3
      a403d064b445552b
```

A.9.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 6a370b998427c699725e43fe9f16a15994c465408d0c8429ba0145
                  9862690620

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: a8a0c9d3e4faf4dbcee304c8eb956990f2c4171ba696f5f7b822e4
                  41dfd05970

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 00a908abe9e7d6198dd5dc32ff3c6e8b5a56922782ea5b07bc2157
                  6d9b59425c

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 5c55ae2e7054b8c78860c81a333dc2ee346557d3c6bef811e92683
                  73c09d06f0

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 583001f477fc4bb168eeb04c434bb5576456571c8153eb5880b15f
                  baa5a40a1f
```

A.10. DHKEM(X448, HKDF-SHA512), Unknown KDF, ChaCha20Poly1305

A.10.1. Base Setup Information

```
  mode: 0
  kem_id: 33
  kdf_id: 19
  aead_id: 3
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: d967d4102fabf6108bae6474d9ffb0f8fd63e87721fc0e67eebd79e4d6e3d28a
        8c179c6b2febcf9568595075df86a4ed736be8b5ff80da79
  ikmR: 4d93c28aef376727c67c68a1404b8399d046c612619d45468ed2ee12b35f5de1
        f1d2afe8684a38262ba1327490c7299ecfa151ac949266d9
  pkRm: b0e5983da0fb66a0a9040d34c8487901040984f883562cf6ed6f694b821b7a0e
        a672947ec72c6e6893aeffa1a9f824e82a4908483101ebc1
  skRm: c0fbcb8b2960a8e4a16fe190baf53790e513498bbe508dec614e5e4bb28cf41c
        780b20aa83afa3e4aac57202682934c75b8a977000d441aa
  enc: 3e201b8e44d713687fa3f765ed454edb77bd1b28b5567e313a4eed994ef47a01b
       b8bfee283ebaacb38c34af69b0643c9ffd225dd2ff6074c
  shared_secret: 7835f33012c6964b7dbd420c296be335a4e2b854347495137fdc246
                 6faea4694ebd09bcbdcdf5afa640591ab68a1901bf83beabeffd138
                 45644022e6de31f672
  key: 5011ed9b69ad3a302a4862b32971c84c98c594b528008afd9978a93f4373244b
  base_nonce: 5d2300c7f1815ead278bf6b6
  exporter_secret: 1d04bc333f5a92e9924ab38d51087c088adb9cecd2df81092cda7
                   f14b27d1057debf405dc9fe7a99ff3b9bbafab2483455b5136c02
                   9e57db307909653866e994
```

A.10.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 5d2300c7f1815ead278bf6b6
  ct: 04f8624dbc6e4c8661dc60b3e32f3b7202d31e4c10fb290eb866999e5f62f14df8
      00a071d5845d06b2af96ba0f03752c8392bd9a7bbe85ebc44c431e66c64dfcda91
      d1aa4004eee68325

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: 5d2300c7f1815ead278bf6b7
  ct: e453d2b5121288bdc9dd5d9b41585b1e16b5d7bf3c2f7d7fcb5d07b0f6a54ca94a
      da06ba34267f2f0f624f01025eefd423a597e0c526d7e9d7547441f7bc4df03ef5
      52a1b045468a4b51

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
```

```
  aad: 436f756e742d32
  nonce: 5d2300c7f1815ead278bf6b4
  ct: 842bdd3f3f7ab70b2858aa92cf4f7ae48168f4aa40a640087db9920fa629851242
      84a0267c467dfb27a584b25adc2415fbcf6990d8bb2e957d9253c3ae5932d7180b
      95b714728d249aca

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 5d2300c7f1815ead278bf6b5
  ct: 768e872c20d36fb7bd467c9910df9634ac6d638defe74a78fddcc63ebfe9b8a5bb
      79b80429ebb23ea144298526f15a60cd74595e72d218ce7d07ef4fef2b93767da8
      992ab03ffd8f8e39

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 5d2300c7f1815ead278bf6b2
  ct: 6af3907be4924887e90119a3cb504ebe0316d0ba8a9dc3e4ad9643bd1247c38453
      e79ecd09e374969a5b8fd206ee4d7b60996ba2485ad658cf49429f162dfdb9ef90
      5c9c84650ed3535f

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 5d2300c7f1815ead278bf6b3
  ct: 6a511ec7e0bccf1cb4256d386315bc383e546d35356f0badb71c2a8896e3d50c53
      908008f7a38f6da18ff5bbb6c3de4f8df4721b08d3b39c128c9bb41e912e1d434c
      49ef06a7f1867b4d

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 5d2300c7f1815ead278bf6b0
  ct: 030f4e13241293ff180ca7ae985d375d047d6c27025836b11eb21b51e6f360980e
      0cdf42807dad09541c0075bc5509aa13d9750258b4fcf81bb906e5833d3b46142a
      95b6f2ae11c99303

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 5d2300c7f1815ead278bf6b1
  ct: e8b5b2768caf86d7dc5f3401bd358662d3b03da561d6120b694e96cdcf43baf013
```

```
      6a67b91d3ebfac3acd676482484ca68a8d86220a6e9debeb18c6c4014862d32007
      010bebd69dcce771

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d38
  nonce: 5d2300c7f1815ead278bf6be
  ct: accb83d462dec7b21dac9d45b74328dfee5b9f58a21704b3d9e5d260fd4310d718
      13a8486a28e4e10dc2a10607be645c510e5b873a1129445a1f3af7d197965d92b4
      74723ed7124d1eda

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536311373537343739
  aad: 436f756e742d39
  nonce: 5d2300c7f1815ead278bf6bf
  ct: daf0a18a61938312c702b1e4f7d526df197c19909975b5d223e8266221511c4e64
      2597d0505180333055d7d887a4f63eb6c567c1211c2d8a042cba146ee8ae610353
      fe92676e20a601bb
```

A.10.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: ad4afad4f20d4d7f19b9aaffeebfa95f9d59fc167dbefe01c3a3e9
                  3b097d9a7a

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: 934a365b300922e19e8358803bd259ac0300d87c28f0e3f265be92
                  df1b0decc7

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: e079096bc542fc891bf9ae9a31fb1c6d8f3092bb253223e11b56ae
                  dff252bbd6

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: c74fbe98feec042b432606d4d021494b6b6ac0977e0ceeada578fd
                  a8edd97740

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 257de4e327f03248c71b623084e86c15ad067efd8e0e58c43cacc6
                  4f36bbc8de
```

A.11. MLKEM768-P256, SHAKE256, AES-256-GCM

A.11.1. Base Setup Information

```
  mode: 0
  kem_id: 80
  kdf_id: 16
  aead_id: 2
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 0244aa79fe4ea903b915a291c90fc30c43ae27794cbf4edb4c7285500273ee74
        83841d6dca12848d453853486ce317889443efbcfb44a0a91fbaecb22e25a2f8
        f61a81224a3ca716e57e85c59426773095e357d0abb11048863d900517eed2dd
        bec062a420d0e6deee4642f61c1a02ab709defcf4871b153fad642f5384d87e1
  ikmR: b40a79eb27e10e2c7b5811a36f1d4275810e17117b308fd85ab9c2b3dba7a961
  pkRm: 4f47aaa026b3efbc7b7df892893b5a6c1a2d72d63db3e49d672ca64a7192d837
        96c369369038cb319a34b76555441ca43025adfea869e113a81d9a59b4734866
        1a150b316b585151eb1556a98134ef33bf3fc49b14a56758a235bcb21cbefb61
        362441db13084f037e8ab866de852743c8cebcb5cf7c16167c6c2e4c47b44264
        97b53b6324aac69e411d73b17077b1cb4f8a151c462c68e0065cf3856d57c936
        7021fa7c5b01a6bd27e2502d0765940c6061b6278a53ca5c775dfcc143ff92b2
        98dc9b352b191147a7f1f10543f5b991ab80c47caf3ad9c46336a5ff24cac815
        8737f58467a5815c0b50d76419a04479a642c0e0db2b7ba528c203ccf7eb5d2a
        aab660e22c282c045c03a072c9cff64cb3da91ca6092720be0c34302d0ed946b
        4ff444c1b5afdcf65a8279bbda7909c081879a84613fb69489157c2a36aa5f87
        4247579304e6613d8b161519bbf1436caff825a2b33b708c10c989882ed3ca35
        d144e1992898c86e417bcae0495cfa396d5e348e92b9342700b76a06707404b4
        1240200bc43f3a87065efc1db8f44255c986bb3b1dbcf075aa91869405b07c92
        a10a3b424aba8c53c748ffe83b4446af3ea2755ea34b52534e61122f9a37b0cc
        a347fb5621e77880e259823b4c7d9b77b56079cd759b6943d0b1a0b25f88a76d
        28c0051bea9f48e0678e00747d1890b56c09687454ac64ba498775766811b943
        cff486bc12d70eb8e115cb21b6501350671a3f2269534cf2b12218caeb3c1089
        a28d79f2a54d8a28c802c388c21b30ba6bdb86afcb1543c4f6a9d8ec5255969c
        9616bf6e5a5efa37c0c591cac8a4635fcaaa65726252479c9fc94defab407cd8
        c1eafa654c2aa8594364c05c9aacb4aa47c59aa5109190913385229c6e3450fe
        99b66c93307aecc5ac2760852534f40073f4c121bf1056f5403cef2912382538
        31e72dfba5a29a9515693bc7e2d19be8d540b412751575ccac6334377982214b
        31a8705c29da4fa20ba62ecabe50ca78a4b47bb3b2acd20485f9547f6d0b433e
        eaa8c06c36fd6cb2f367b2dd7018196670fef0b8897bab5d004d53328222b260
        34214b8a7002d782621e1b65e3d3c15d786390b9a9ada13a581b7e5bb5a48e37
        671b949ef0f91b4e9b44e769cbbde1a11768541d8134d9760fff38714823b286
        93a94bf2284825cd95ec0938030a76a31a4cd0764410238a9c4042f376a0014e
        5a035736ec5f9604a8698b3309fc7b32eb07784cb4e938c5b4b66570c0941b1b
        5ebc981c477b032226cba324508a920f3f167e71123821f98b318843f3b96144
        e76078fa589342449a6509e2739d320c415c38489e9c962881bf844ab70632a0
        b578cfe91c7a9e5a868270aeaf3481e23634db0b4360a1bb7051b482711d47d7
        8c4f78aefc66b3a5142b63b607eac42fc779580447a272961953f8b2c9384584
        5261039440009101cecb39a7d560301461bdc05f12622bb4047939f299f2415b
```

```
        abfab970a0838732abc4147daf7a2ae22b45ee0caefd637f4e54841ee3a6f0a2
        766cb5b5a40c22a18107c8b4099b265ae5546bef147e89c25c36c32f5c0683d0
        34953f376ad6401d5d94619895053cb9ab83fa3613298161b06f8cfa18b1a4a0
        771463a31fd2ceec77d9e56402e0c4c048b7091f98139a4772b35f9bb6e03dec
        0410246cef4221fa388efa76394d8eb9d72a9038cc0fc5716a72f117c421c664
        07bf613ecb85375e48c358a800d5ad03165eb2e9acaa4ec1389808b774349ca7
        9d
  skRm: fd4cdf57f4026868a90103ae657fcbe866e08267f8cfda0e6be6b9b111b9e3c1
  enc: c81d88196d7c3d5dcf095d60af7d1ab970b4cd3cc0a13bbb712ef12ae2e2d82f6
       5dc23a662247da8ca8fb4f5d8ce28dbc2c18eb838508648a958f58f3d7fbc8bef
       c53e2b5ebcb594031a173ee949b3e571c509b2cfbf7eb3339cd78d12b2502d933
       ddc22c25890e7e770ca012eee3364664231c28a4653024bea814403b4d2128c7c
       142bf181f79237a256a993ceef1b2facd56cb42bbe1ba1f2bf1e96923dce2d323
       a398b67f820b93153d68ba7b529c9975243073436798c313397c348bc4962febd
       08b96b15233ec0256e49951af7fcfac15a5ffcaa7d27d7a919f3c5011688d93d6
       bf690ca67674ab36adf2fe4f566226152820e9a4cf521a5da6adf1078b84be06c
       54979d818c231fcfe9b0da2b5650c8b75020b3f8ce372ef63f1811b4cfd011819
       fafdb6ff9137b198fe59bcf869843270913969aa7b0e354d66f0fff76c4770474
       574ce2c4d21a5d70fdec93103bdd313f60add4ca76c1bf9f06ff615ad589488f3
       c0bf37f8ceb2ad96d36c1bf93e9109407cf1072d18b14c359053a25619a4888ed
       d6dfbbeedd3403c854be9ede572a3f66a4b76d30fb34078c316e73cfa9c8b8890
       ffdb57517ff860b4936f0d6b48024610e65c72869024d67ec84d4165d2987c245
       935f7ee213dc09d050c04984089ee7895087afcd577db6f0e2376241134e4f8f0
       31d559e3eeca3fa81c8a5677784f7721cca90bddd8c2413b0c8c82eee3212741e
       7aa71f74a39bb9eefddd11a011e34ab2070e0dd188095174a31e83ab6af8315ca
       1bf3ef0e84954c81be534133b53f09d6c315b729a0025fcbcfbe97fb9d447747b
       58fcbbf40e5075a87e56a1644b66dcabf5020dc3720ab56514e03b3eaa5ff82db
       e6e1e9b2e0cc974add9ea46ecf946d4d8ee704535abd41ab499550b92850d19d2
       a05e8be91777e066e5a6e8f17484cce0295ee80635e05b8a5625a9cd507344fc2
       3550e47d45570c308f7d5ee2ac7201991c669a993cfb90cd227b245000f9bb699
       417ee1bb5a85234cf4390728a196d418914e70fabfea3860884e8a7a28d364b2f
       83e4aa404ac7c62704eeb474b78ef8095ba6aa168b5439e3b7a19aec8b5c10148
       b4aaf92637213ef83395ee3209bff22ba2331d23f6f32349b8a10bf62f3116e30
       fd0a90638ccbf64b2d258ff769c4cf8ea621787024cac5de498c2d91476057f7c
       579a572e9125b3b90410de2b976e106436474458e1adebb956cb9e1261acbbba3
       7346ddbafc248cae0df70cfb8bdba4fe7f116397012b15a7a10b1ace8b8f19cf6
       07f9f64e071703056632d435366da8e9912fe76320d950026281a6691e10c4917
       4c764838251cd312b0e19088ab71536f331999bee92c0ecf7af0b1ac2e9e07311
       fcb5ca968917895d8d99a1c3e23919d47b964f49afe02dc2368d5a08125183731
       142acf2fdcca3c17db267fbb68691cfc5d87a117dd4b9ec04b816f24b2fb2aea2
       43c02f0d4e47e26ae14b21d0a8099ee453847b46114b430b17506c0e8bc2f488d
       d5467acfec5dec1c3dce8c27f20b2a60493da8beab7ff43491e6fbb57f077aef6
       c2e07c1144ce4962456ecb4e538498c0897cfa73c3f75ebf2ba5c23a903e2d3eb
       df981eee22480cbab5ae6e2e85b5e86
  shared_secret: 4b87ac4d2e1d4b111ab7f69875a112d4734fe02938fa0d25976e002
                 828a8bd3b
  key: 0b0298c6396745fb30f5e3df0e60c390c0a1a3e52090893871fc24adb02976e7
  base_nonce: a5c6e6fe2671b3c4d7e6e8c7
```

```
  exporter_secret: d5c597cb1c2a92d81aacb171635149b7f45a08a57b25407136cd2
                   2be1ecd6bcb
```

A.11.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: a5c6e6fe2671b3c4d7e6e8c7
  ct: 8ee605b372d7005d22227f45a5e45f55d99868ef45eeae12ef9d64134c39f4146f
      82d831cac8c33cf836acba6a3d514a40c6bb4025da8087b78a2d390bc09df77abe
      cb2d1ea0705f5bca

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: a5c6e6fe2671b3c4d7e6e8c6
  ct: ed7d8659bf03480c69fb6830fc7d7aacd5cda0aa89ae41471465ed02cf1cd80639
      81c3efd194488e7cc329c0099ec24493cf5a98a113e27b5d647efea017911ee9ff
      bdd9d5b2c3fa1fc4

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d32
  nonce: a5c6e6fe2671b3c4d7e6e8c5
  ct: e74d0775b5ff8617878acdbb66bb10ae2772bfce4dd479f1de453e0c61290e789f
      64b922c929bdd8e2d5075b9096f5c6e51c8eaa8d58836ba7d2dc4e1627f28a880f
      8e52fde939bda2ff

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: a5c6e6fe2671b3c4d7e6e8c4
  ct: c7c5f892dbeab151ebb881b0d7f95488e932be694951279278f67aec75e30b819f
      ecc6f0bb2dc1a46b03c5aebddfb28d6b578205e82924a2fb34a9b451f8f5c1e468
      4857a87a3ca12c20

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: a5c6e6fe2671b3c4d7e6e8c3
  ct: 05d1af9cedfbe14bea56de2b88aed1f7e74428b53adfd16de491aaba2335ce70c1
      f098b20cb75ead03b9f1c9d91ab65c30392078180e5b343de9d1dbbd1766e0fec1
```

```
      076bfc9bf349c609

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: a5c6e6fe2671b3c4d7e6e8c2
  ct: 0b9fb804a6752969175cd0c248e99be8014a55b240a69928fd54a63990b978d9f2
      f9e78cfed58d0a93597c1f6fa71b4bdebf60eec4774d3522dc4ea4d7ce3c083970
      3cdef4a2c5f925d9

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: a5c6e6fe2671b3c4d7e6e8c1
  ct: 8dbb0f4dcc61cbdaa98238134854e5ef6affacfee94bae77770f4707d47fb3697f
      aeb808b4be20b1b50c675b6e07376ff5dc3a71e03781a0910487a4d0127ae0aa67
      f3aa983d8695bdfc

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: a5c6e6fe2671b3c4d7e6e8c0
  ct: 2a0d0b16345481f5bad77f9cbf8a6b7872a1445636dbc10e0619ba790ad0986207
      31c1d5bcd9954105a17d27286a33f20bc8596504ed4b78f4adb93601fcc6e4ceb3
      38f0d5e57869f1d5

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: a5c6e6fe2671b3c4d7e6e8cf
  ct: be88cefe91010d561100be0b2f5e9b6275165a104d69bb1499b7be7ba658811194
      81eb3b695d6d47f514a03941459b446df015dba69805aa9b4f6431db617310fd7c
      cea881bdfa2fd91c

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: a5c6e6fe2671b3c4d7e6e8ce
  ct: 3ea42762c3d079eb0481588975eb66947b1aeb0774a4bd678ee9faded56d586eea
      29dadaec38a259f93d4b03640231ca974c4caa40786019d799683029f515fc348d
      0cf6683d34fc56b4
```

A.11.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: a2976da31f76e88396507981fd69b3ad575f8da4cab101d16dba51
                  fc31670f28

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: dbfadc2fa4f7c297a8107bd3a188af560a808b22c1f862663e6429
                  233ba9804d

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: f71846724bdf4120966126aa08d3c1e5d52985ef9bb98f0d31555d
                  919a0c5a9a

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: 5fac32598d3e80f6ce9be0405012dd5a6c2d046ac7f2ba4ea40d89
                  cb0ffb2715

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: b2a008ab3acd18fe02714053734a715f6ec97569985c9fdf9f76c8
                  c96a018706
```

A.12. MLKEM768-X25519, Unknown KDF, ChaCha20Poly1305

A.12.1. Base Setup Information

```
  mode: 0
  kem_id: 25722
  kdf_id: 17
  aead_id: 3
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: 67d925853f974ffeb36a867ba8b370c455c77fa386e0b667d6dea0fa0bcd9446
        a7a24daaf163ec2c0979a75f6b776a4e08ba8e89aa9fb4f604e95a9acddc4091
  ikmR: 9b3988687f65935430cf740cc30c36cd480d3dbd24867815addad49ea0dc050d
  pkRm: e6b1689ff28e68c7536cfc35a8d4b63bac50777871b8b82358ea75d8339817f0
        4e0e0b2fb25c9d0cecb3d1d8b23100982b867df40889d45bb27f5738d876c5c9
        48b2831c5d72587b2031391d957edf1167705c611cb9be9de54a56462a814662
        468330a382150cb15970882271d1182394675057c833b382f9e9cba4756cb903
        afe17ba6ca90a3cb086a3335b0fef76edea612d0aa8e784ab03b9829fc160a58
        e16d1d8ab545aa35f2b410c3d9b38e931bc0e65b66e841ed331e1381655c2a1d
        64219259f75993c675ec919c4a812e8a922a7e854c496323ca27275dc0730981
        aba4018f7d323cfb61cce066bffd3982b8ba609b5bb7991ba5138b9ed1ab3dd6
```

```
        24361ebba9f93aa4f062a7bf9125d86906cf302e5d31200d4aad983792c3d2bb
        2f62767623c84c490be48c1f194c4f6ad601d7eccec886aee1371db88a29edb5
        1f99235e7c9571dcc13082fa64c77bc689e1663dba0016170e1d3864f3f831a1
        e1c1a539549342b6b4e391f1845756a90448c5380ba81f34e9b67422adafaace
        b8d80c89d38053259721b17cc716362857c805b1bdec5caa0f1ca615172f3320
        737e5b6855fbbd20639deeec497c203a2ef51c5aac18ee883fb51195394a0c6d
        0ccee4054cb7a36d25c4695573cb4c31b4760c0d86cc80318a05862813c9e18f
        d2097097d30286f481e194048fb0c8ff3b24fa72ca6de6adfa0a8d11f8820db4
        38f24c6783b3005929bee9216fc7696350b461a03b6e895b07816c2c91e160ac
        79c528bc9fd9c31520b6ca5ebc410f716856101bea73bccc7a066d1c380c9543
        ea48ba1c013b33e988db43762b995002c0b7daa26c4b42062a7b9cd9a5a2b4a3
        a827362fdc2363025c23a3b484292a4b1524856db23c851ac23b75afbd736478
        ac892345355238206e068d9296457a8543934314283c71435c92a37bb3839b24
        789a07f4e4a77787ad98f404c6777afaa575acacc97905570fb8764b28838c00
        3b04b3967bb29f0745446879532347009155 5dbea5afc5c9969a38af17394f2d
        423834faa688e10356c785b27368b5c581047c50f233691742463dc6bfc1538f
        6f2584aaabb87f1914e3aa049cc8c94b99393df69840fa3ec7ab11ad684c49d8
        4161a541a5997fc865a0098c3475680362b82ab07a15fb8194e6aa5e6da59543
        545eb0c9a8b301c373a1809d994b8a3927aa4c3a5e639ea303967bf375e3ac10
        0d693161f99628c4c1147c657c721de5e50287f1578bc5ad11cc37304c17ba38
        4cb7d360ddc891b9a225aaf89f5eca6c5f67cc554376fab6119fe378a35a6080
        396d90fc6da2330e231649ce8b4e60f131486411634489530 98a70691640a7c5
        51e44e76d18f3c80c2b67c0dfa24962ef8732c78236996a65732c62350c1f837
        6d313b74aab09459246f08e375843abe316bb12508181da565bf4a5640bc23b6
        4a2a2a7755d61c0acf2cb2fe903c9308769d8304ef88aea4aabfae8239aa001f
        cd04acbe500d689042f6ec628208b5489c81fa409f2dea3fb6d9233390344704
        7eaaa25abcb2c51ca88f0feb1925d5355e468d7fa97ca7f00d92598ef95a44b8
        9976f705a9c8c01c3008aba8939dff23971fb760df7996756aaf6d551ee0483e
        f5f8e3078295e69f29f6119a1863d5e830548c6b615ef53d5033c9b669a0e470
        b73cac8e3e03cbad4d319c971fd811afd25c7dbe164b8d5ef96b29552d70aa56
  skRm: 8f908710ee25a3aa6fd3ed80eb5bf102963547bf4fe36d86f772432ac383e6e9
  enc: 83cc3ee720f72a3d37c2870f84ef83e4206b82366b63371116566096f9e7f8fc0
       1e0ff2694f8dc8c25e1772bb6c1b68627985ca551cdcf1e4cea286755bef42b02
       63e0e09104ca438c87ef0550920445d0d80f964a4335dc4a47cfe3a5cc0e771c6
       23c55d898804d48fe3add931920ea17a5a0637b00ef2a058db56dc74b2721b0d8
       161bdb0e5377934722cdfa06d0f762ea4b7008c79c09be858e2a92195629ed54d
       82bc872608fa0f2dea3a1785b328b584485a772c50b0f1e9d99569834fe9c16e6
       4fa7fc7c772135ad632fe0f9a0025de13432dab939c8fdf3b88f47f77c63732c8
       433e852a2d64be590daf7b4de0066a053366a2a2c142ebfedb03176d1d941814e
       9959c4b5bcb91b513c8aaa023c50b4ccd74861a98f52151dce3e554e9f8f1c9c2
       e6ec10b70dacf92ebf6ccefca7f16109b991c6141dea0321eeac896bcb9cb57af
       c93c388c81d2854a6b6c670d5bd0adc7858da5855e5c9d5d0600404d0807e7bae
       fd114b15e65f885ff771501c2049880e0515850efcc6f134804b89d25cf102c72
       3513666b15ec5e5e2541281cf87643f0ddf836a01b25073aa85644607848305e5
       1f2a38f4df0102855a6589ce63bb19170d8c207a554b6a375656a3ae127d89716
       3bf63aef7c59543c771c16ec22bf9b270c5e34c3252afb09759e675e5052ae20b
       2a59230e26f0ec957b51416658a460bfd8cdfd92c39145b588c8a7af63f7d4952
       ba4de335c94805752879275c5d8b259d731eaf55b0ed8405d4c613c0cdf3b1050
```

```
      bbab611bddfa86651888c745a475565b55356c81acb7331b36c56b3370bfa591b
      948156b4fd822cec54a4cb02dc9cfe6dfa9909b739190e2d5632f8cc7940252bc
      db6eb1ab8fda81dc1697c974b6c2aabab691082bbe2fb0a35b32a5cd0f6a88ee4
      dfb89ffb5b5548d60ab8ed3c091d99a9e5d2505e65a42c4e35eb88577ea3a5707
      abc131813f9ce39c4f8224f5716cebfc7e0a1469ee429964fcc59a5a33bc76573
      bd2ddb37a516c16cd69506ccdaef340236b8befdf716357aa1a2622fa9b76572f
      dea7731808ce2a6473e9592ff65beef439b0bfea17a5e610e9e4c4ea2e0b32fe2
      b06150c75fda5f164e957290e2b2e435bc02d38928928aeac8a3c47b9dbbf9e0f
      eaa5084a071798fa8a51c304fe0fd4f23ba00f0b159368efe087cf44d6dd40c9f
      eb9f0dec27df2e6408c0e8b447edfdda4ff1e32b84df37e2e6e72027cbfd556a7
      d0eda5c9a17da48fce948308992f8d43690574f0e85f094222f9c277221c5b76c
      46365c6b7071a8c1aa1373d96b02e60f80d5898b0f1b1b79dac591ead6496a438
      d35ee5a1f38d6934beb780ec1f320a0d5ea3607f8c956a834751f990f46bf178a
      af492aaa6e8b6b3da9af858e9a8f9a031baa0525d097aaa10f876797fbb3e5baa
      0aad9d959d45b3d8954bce43adea5eb62f5ff20d97cf57564438543b0df9a60f5
      87d1730aaac22e23e4ca71c2fd8e211948560acadb8023e1f00606798b51bad9f
      49cba74fc0c911610e09b9885e97f5489c885f1570081debb1dbc4deb442fdd67
      33869d9e3e1fb43ba62bb7e2656e0b
  shared_secret: d9994083f7879bfd2333bab88dad36c0473eb67daeabb4f7d4e4dca
                 56c63ddb4
  key: fde2cb86e35b2adbc0730e09b87aff8e71703975b90512c9d5b9816bc26b2719
  base_nonce: cebe8333792f645648e6188e
  exporter_secret: ce13bbb4db2f720aa4fa0778afadacc0a7c03f2658548119c3584
                   998bc672c29e455a5fe5d82f8f12b974af8fab4dfffe048495ff0
                   d02851a8d6be4105e4d039
```

A.12.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: cebe8333792f645648e6188e
  ct: d56982e7b1b43cabf8210a30a3a427b880260c89989cb4dddbe13c8bff9f345c79
      dce1ce8f4ebed134a0c8edc66b5485f3c535e46335fccb41cb87273b2ddc690701
      38e56c08480c1857

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: cebe8333792f645648e6188f
  ct: b13fba7cd35d08236ba2f87bcc6f6e7ff64cdae73f57532d4e4a0a8de9f77c7fce
      7bdc75d3d75e0c3d0433a598ecec66384ef6c01f3efd9b3228d302b428aec58b8b
      2dc968a807686dda

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
```

```
      3037343732373537343638323036323635363137353734363
    aad: 436f756e742d32
    nonce: cebe8333792f645648e6188c
    ct: b72272fcfad2bd2862ce98487122ca81c8053eb318ced45290abfeda4ee6fd4db6
        05569060e404ea958c70a6323754e93b9c77a584c32853bd59742171153864608b
        7e475fac27564088

    sequence number: 3
    pt: 343236353631373537343739323036393733323037343732373537343638326332
        3037343732373537343638323036323635363137353734363832303632363536
    aad: 436f756e742d33
    nonce: cebe8333792f645648e6188d
    ct: 1d838380c36deda36c67ee375fc924df5d0f2aa2f9a99c7f22e2d22518b467ca4a
        c9d48d9ef1dd9771a96fc543f5d727ec32f8a5ac1788126d2e22641efb5ff23c62
        6e788a0ae38b1499

    sequence number: 4
    pt: 343236353631373537343739323036393733323037343732373537343638326332
        3037343732373537343638323036323635363137353734363832303632363536
    aad: 436f756e742d34
    nonce: cebe8333792f645648e6188a
    ct: 224710a4ef7715ff68a08e1098e44303ba550f2eaf474bc9043496fb6657f4b442
        7c130bbb8e3ae21eb77377b35586a8cd3d7ca9ef5c3ea0a729eb7ebe5bc09d3e3a
        6a49dd0cf4bba124

    sequence number: 5
    pt: 343236353631373537343739323036393733323037343732373537343638326332
        3037343732373537343638323036323635363137353734363832303632363536
    aad: 436f756e742d35
    nonce: cebe8333792f645648e6188b
    ct: 9a467be44adde9742e106a7edabae3f28aa861430b373ba7f49e9cbdd33f7615ff
        d03cc715a3c8f7232d28050c966ef829609afc9c62733c95615379f9de2cc9911d
        10043db071dd6339

    sequence number: 6
    pt: 343236353631373537343739323036393733323037343732373537343638326332
        3037343732373537343638323036323635363137353734363832303632363536
    aad: 436f756e742d36
    nonce: cebe8333792f645648e61888
    ct: a0473d7b63f7d5303af2eb4b7fd5bf3b58b48ed3c7dbefaadcd40355a6c312642e
        32e7a25009fad968d67740e50761e500f551954649419132a585d0cd3b83426dae
        4c56ba87e27953c7

    sequence number: 7
    pt: 343236353631373537343739323036393733323037343732373537343638326332
        3037343732373537343638323036323635363137353734363832303632363536
    aad: 436f756e742d37
    nonce: cebe8333792f645648e61889
```

```
  ct: 4911885268000f22ccb9c517bfea3e0f4195ef41d7548d15f0f356120384a186e5
      d219fb0d06a8a77dc73be85e40bd3df9f4d79a72adaaf439ac5fa3734d721da9c7
      fffb8b5d940e4a15

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: cebe8333792f645648e61886
  ct: 03cc03b80cb610ff99087a962f806dd8e839d26590970a76cac25b4ef9b62642ef
      ef3507f57d0ce91b3ebe40ec2ba3e141893afbb78706f7234142a04d830008fd4d
      18c62003d3d4663b

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: cebe8333792f645648e61887
  ct: 41f311f10928dee0af2a91a0bb90d9ebf77b383e4a12a5cf36d11d6c1135518513
      239432748aa21483127f7c16dacc183a8fc42584a771b719bbb5d1aa90857f58ff
      6bd8c91fe4e55d8d
```

A.12.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 51aa31c5abe8b1785a8abe0ecc54870f4290839084259e12bd44ca
                  c46e09dedb

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: f5514fb3f03ba111219e5df93e2212d1d612b11d23caa4ae4eb0d5
                  a5aaaa209b

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: b184436c8c4bd6aaa0ddfca28a500a1d6314ed4be4ddaa4c92d9e4
                  6725e857de

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: c315a582d94eda563d5bdda139fadac0bfd9475e4a57ee92d5bef1
                  5946c71ae7

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 43b55c27838a27e2710ed2b8f00b77878ca78ef5753c97d377ed78
                  3082b7d11f
```

A.13. ML-KEM-1024, Unknown KDF, AES-128-GCM

A.13.1. Base Setup Information

```
  mode: 0
  kem_id: 66
  kdf_id: 19
  aead_id: 1
  info: 3466363436353230366636653230363132303437373236353633363936313665
        3230353537323665
  ikmE: ab765f59234788d2c785d7fc0cbb82873d73bfa6b8fc95cdefff6959a52bb9c1
  ikmR: cfcd8c6d1798c45453ff275bd58e27c8222725354068fd85f00227521cfe275b
        cd7525205c2b7809fc2eb5c201416a100769b4bb4a64490e821494dba747c87f
  pkRm: bb2a7548e97f525ac760e5bdca8ac33cba130c045f12182fe2e3949c0546e544
        a633173e1e39bd7a926078db70b1072fdbc4023138afc8f0240c80b5994492c5
        348475e1cfa4a2ac77a6a2f7d740ee26add739a05958c8bd844f3f69313d76ba
        acb00ba74b39b87b2938a5771acc71a8ca44c964c0d92a6c9bb4670f25a597d1
        559b9125018b337e5a807e2a65f4d1b8bf821aa10008ae87c96e294a00311cea
        b09d259abf56a48507037ea957254e63ae137345ee3a8d335191d14874f27b64
        d3b87cbd19562381c21a74013a1b21a915b543690a282b3aedb8a187757e2770
        3944cb91f0e240f915a91cf8590ac92b7876c6a0fc0577a59e8a4399c6b3a89b
        e267b9a9ca69608e52067a5638b4953949adb2c713a95a7c372b4ea1b7791b12
        7f23b917502ae9e26d5e568e910824afea6833bc48fc42c05273c9fc693b051a
        69f50883545b275db909f1fa12936aa06448983b039db28c91f96969e538a8a2
        1a7b0349532fcbb4c920ae459b09c37527285515f5eb38a3114f473b2b7a1097
        d21615522232952bb4de87b625e92cad260aa1fba7b380cc14437073805769e8
        bb8142c707a2a957194b0e7435d84506e305082b89a9161b20e00a537c56900b
        bba8534c373d20b14b10b214e73ba7e698780890d301871ed44868339c28464a
        f1d046502ca871e97d9286802bfb8207b27ff8150d8632b8b3420f5bb908a628
        391c25519667c52846396b9860b0670412bb48d095aa85b21db19ccf63822760
        b7377bab3e1f09a3a39b69f3e40b1088793738ce43a56dccc27efe483f27b322
        cd753d0ac77780a770e06ac5369407f3eb3a517420bf549645901f26305f9c09
        7dd13440383965c28c3304bc13840c3f1b28ab3b2a053ba3746c4cc4fdf41b83
        d908b480cbafa8bb514b41db07b5b7990583dcbf9817592674c674351260646a
        09b6778f2bb393e9824b087de700750c102dfed1cda2da75321097d9d4ad8f59
        a56bd127938261b7f38a08664d7eeb1de1fb2981721b14b107fa989d23d5bd46
        31763c10b1d615811b997d18fccc74a151482c2576274955b5370ba782fdd670
        fb7a6581cba079310ac55118c34a40ce7b0827d61458b63e9951879b237d84f3
        348fe5a44c3b654a5c4389cbb75fb5a1fce0c0b6861fc51883e0e01b7d118084
        17cecaa91f1af6a1ad029b11706f19e7be4e04809620591d4a9d2ef52209241f
        ff429bfef1c35ee56e57fbc733a893e3f66ae6b4cc73d33389971491f05f89f4
        ae583c92eadb0af0372a18c466ba5c5565ca8f957682a150b2ec27266b209a47
        6b8eddb00376d4c484957bfd0c67a1d81d69000e6b805aa68424990a0c63369e
        6b03754c1b1d79b71c84d22993e335c6ab28ac974451e9676e04243419105d10
        35217188c7481af33ab03fc67d7ab4c9a9f675e173205e2b21a9747f65a079ab
        605962545b510b9c83b5c47ae41b026869e1a90eeee0b701cc5ddb482a5627c8
        045b0e798aac032b692ba484c1909c042883b8f4227e187c2e226687059af88c
        44480994e15c48dd15603304716966a0f7f2373ca9b302a83f42223c12ec31e5
```

```
        bc95ee738f9210a1571c7fc5db1be783c0319b9a7850ab849538384218f8d41c
        82959a0cecb3084b8567437c491959f879a153c1aca0d01a324b95fdc1852a1b
        47e9414f52f4470b8bb41729b1fcb9011e3408fe83cdd4346ee62a31c5404dd1
        4724ab61b817eb081e58ac76ca2386b92a08b959c285a8d1333a431c7b82569d
        7f1c6705e3b84de9a0555712ef33521c2773a651c079ab9071170a0d15ab8d4c
        59646b0b5c8ac78a6b35398356b8baa9cccc7735b25a91878f3cabcac1f2651e
        a860d49b4cbf63aac3d57c2f268d1d17542114b7b97abc6c5b42f6f4a907fb93
        27431e93790f1ee696ff4186179450e2662b0e2047f4c389d505067ea7481d5b
        535b96825df52e22127ce77c54dc5892669c98e2aaba5e46a9da9b9a6690cda7
        e3542806707ca16c2c40954b0ccf59943ceaa628ce526d77619bd1111d159300
        e6d3b6ba88a76a2797e1b8c5db6b161cdb3db0f6a84da1a18042b75ee7c56128
        b6ffc4adbda53143f09d210c5a30c5677ed349f8b3ac19c1bc00b6594e345137
        e8236aa4926b719f7a8ac9ea463d4c9bcd695754c40c2616753c0327b3139828
        296da004486635a36a194fc5622c428cb057851cf89ced5e2c7533328708d0f5
  skRm: 545f8a47869bbe8231bfa14de61aaa71aaafde79ab6281e3f42e0a28a8868f8f
        bd405f148b0137bbc46603919e5ac1e768d1e6bb9ac4a9abc05edc5b5a5be726
  enc: 0cb6a215dab3c53cacb28f943fb791897083a76ac9e7b4d4a0a561ab3bec02669
       abdecb44c4be773610dcabbc5de3381acbecd79ab6542e92132a4a7960c6cf9be
       1140d59ebbce2d1fd7d662eaafb69b09afb392dd81e9c7f4aa85be187b202ddd0
       5d2dfd91d98b9229ea1074038ae53ac25fd0bd0ce494985bc2e9ca4e25c98e8de
       5e1773351d4150404f946e6f6217a98ae895741755b527663a958cdf27fa7c9dc
       bf0dc877eaeecbe417f07bb644825fc3473ae6b6d8ea68513078f75b35a3c5c62
       90035b8825d9b8b1dfc443cd85e207882e1106f38532d9dea044c982002f4ea57
       38b242d4ed0096e6f7f92859c03b39223b98125e66975a6145efd49e56e3bd54e
       f3cda59a26a50841826b6140653fbfc9a0fb6dba2a0c8fd3211ef98643a3b5712
       13be54a03763c73bcf5582d83df836e5d9276adc02b15dfd2f920b889e3fd07a2
       93b2eb4af3999028ace4168f4ac51cf9d68aab0f9566d2a2a05e128fc9d06e55d
       c7b3506a99cd56ba359f3751656d543b701d0c3cb70c85fdd4f39f2505a911acd
       48866c8016491472f468f646df5202321d82f9b950b24f8fa8755830d73c37d84
       d6bdf820498052792d3a91592a29aa0633556c7a8c9e7207beb07ed396d7af4a8
       26ed88058f868780fe67d137893840b706545a28ffd596c0eb07c04c401297c41
       0f500f589b663133d22904a4497a0bd1284e9a7a781ea2a76ad63c131e2c60eeb
       b0c544a7d9eb904399beaf75538eb884e4321d91ecdd543c3bd922e5a41c8e444
       bd037591d3c02d84940f8e67c2828bea775bf517864f8413404db8d157ae86ad1
       96f919d048408c73721c55430129a00229e19e3cbaabdf7b001c70ec1064a5b5c
       e434c149132c6bc4cf48ba740a98cc8e4695d5d223e32348a8bd24e0555c4de1a
       888b81c7915276eb9ee3c522d9ac92b357ff83e31ac35de66d308fc0a5cb3b7fe
       4683757ca8586c0bd56b7be4989936391657bc74705c1501084965ed9298b2fac
       b7dea91a90f195cd15151788bed3b7bd39b606f95274f930169a5a592e134f5c3
       60d54325ef34e925271561f280cd70fe2175b130d88d3bd1bb18db1c3483a8c5b
       5ff14672688278f4b46ab4a81ffc829294af5bed297f613c5bddf5165d38806d3
       1a27940acfb2f0ae5e856f1faa850fd3d384d711993be92f9e478f3c82fb7b68e
       2eddc51608bb0fbe8b1d71015c9730da8a0b45c29ff7d28b19958bcf3a1dae0b2
       90fe144445f211f11645784240210ce6b40333648118631c347ec483ec072969c
       6a2cecae1c298b216f988e002810d70e37f7a8044cb1298f1547c92731985e1f3
       b5445c8ba57d3a96cede572bc3e754cd7c6f47ad416b444426664046a4b5743e6
       b15ad37c9d042b388b73970813bb694a015f511fd6f9063ec3726a28060f8462c
       7f1baed77e22fb2a4c2a2a66f08f8925d32f3fc8096cc27ae91bbfddcd63c27c7
```

```
      1a4261a7507fa912c9dd466d8e1e09662789076f3d1dbb626a4d6a72538f1208b
      9bacc8b20f74e7f8862e7c7481ddda4c387821301959679a7bca986c72ed32ca9
      342f9c726877d94bcace8096e7d6815476c4b624665ba5151d347a6de5544c764
      757191ddd3b0c8c00db5c9fd3fdb07800b6ea6afd3ac13f375bd2c662408224af
      a4efeda238f2ee48c73365aa8d934783d9a55a9cdd247194d1f812e67c05aab76
      0493328f6ea85419963b10016ee2c461e6b14031f35f075a0bb573ff349435c31
      7940a4e4ab098fdd94f74eccd558a924bcde3a8c5c22d025f61fc4d85f4515e51
      21c74bf5ffa5c7b20dbb4252b5c2a5e1cc2b99c37e735f9026d93a6e9873bec98
      0b4ab14c1e549b39dd1d3d3a7092aa87bbe4f314e29ac982f4e5d20f8a0b6d2d9
      a724aa90bc1d606366353ae643d5a1a556cb8cfb6f0897f88c5f8741b87dc9f6e
      a5ed6ef9a25a53875cf9ae9a932ccc3d352b25761a1d21ccc5b24b4a7182e43d5
      50d0b4167072f7b2d67fec4dc01ba92d5070b6f0c2182a9c904b54a3ac4656f7d
      81e6966ee59abd31e2640abefb946cad125266bdd441e9ab856a568c602c8553c
      ef6678147b409c6dec27d91bd3c68ec3d22f94e482fe2f4decc88ca45fda1edef
      4da862e6914ff26f6f96faf5b1b5945c2fcc37c965c0ceb763c7f4f70a89e7f73
      254075516e4e34eb24af4a10b2f22d515e7a4a9965cfd2ea02b4d4a436f61f97c
      948472e5dbb33b00
  shared_secret: 6d3d3174abc633f10cc9ee967988926586d6174a53d4f83c4d1c1a1
                 add2ffb04
  key: 572706a57022ab98af4f4ce1b8de4242
  base_nonce: 9bc56885fe63e193ff62b41c
  exporter_secret: bf9a89c68d9d7a6116e833ee5e95ef8ad25d586b5f4faf304604f
                   27fe174c3cd6f87ba8d50e4791ea1c2a8f1780a0a01b3075db65b
                   28d1cfe7f0dd87a806044a
```

A.13.1.1. Encryptions

```
  sequence number: 0
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d30
  nonce: 9bc56885fe63e193ff62b41c
  ct: 3f491e91c4f0b61d710c51f5a4cbf06ec2aa1171894418b660345b22ccdd7b8be4
      314e90caadc4554eb3d0ccef61c231f98547d8a16bca8f8f1556d619a85fb089ba
      c81a24b17203421e

  sequence number: 1
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d31
  nonce: 9bc56885fe63e193ff62b41d
  ct: c32d4336f4e00e45dbcce8cc3a2958e50ce7c307c7b3389b7749c0ff13107b01d4
      1d98c39ee1b762ed49e43d9bf43a3eda9461306ee687188d509d9aaded972b9633
      22c816006fdca3eb

  sequence number: 2
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
```

```
  aad: 436f756e742d32
  nonce: 9bc56885fe63e193ff62b41e
  ct: 270a87f92b9d037b4fb23436a632c7bab284a0b9a9b9d4b3142e010c02f7748fe9
      96cd862157cb2c8c1c3c5502596c6fdf972c4a76bb73816c4778ead2692e71731e
      01f29696c7500021

  sequence number: 3
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d33
  nonce: 9bc56885fe63e193ff62b41f
  ct: d0b35bb0220deba5cde7a7f0bf8f74089bf5d48c9ebc0c59fc5ad6a5a8f86a2122
      6fddf9ff86181016d7e859d731ebdf9b39b59064efd62caf709dcd6724b99f379d
      d388df85ef60b367

  sequence number: 4
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d34
  nonce: 9bc56885fe63e193ff62b418
  ct: 61138622949b91ea650873986a57b74dec984935e7d8639457cdd52b75afdbc53a
      6d77221da0cfc3494e10743d0ec01203570857f453c345a418314427972cacdbb9
      5ea8b59aefdcdbb0

  sequence number: 5
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d35
  nonce: 9bc56885fe63e193ff62b419
  ct: a57362283100bf431a005b780c35359478a6b1e4669fcd5a79f00176ddfa36d9be
      c2a9ac920ba65e7e3980afb6c00660c768aa10306017b8ba8a96c5d11183f5c91f
      5e66fce25f80d3bb

  sequence number: 6
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d36
  nonce: 9bc56885fe63e193ff62b41a
  ct: cdfd3ad51e6b8a47c1b5722ef8c0e2e2e56ceb0ab6ba81b87f08bf269844c319c0
      75fee643cbf5941013006d4ada82ea2fc4277d014d3c9a1728151681b0a07fb54f
      f98d8d643d5def7e

  sequence number: 7
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d37
  nonce: 9bc56885fe63e193ff62b41b
  ct: dcd3c344c0ad475cc2c43496bc5d4f10c940dbbf9f3b0b07d240922c540bedf099
```

```
      e7f128067a31992dc8e2c6edeb5d658ded8e941a27b64e5b549edf23f19fd46479
      67f9ac56767f1193

  sequence number: 8
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d38
  nonce: 9bc56885fe63e193ff62b414
  ct: dd17d4b09d56035b5ba3d7447f1583a04542fb7565ffeb2a27b882638ad4f533d5
      4636a7c67d055257e4b05b2a130ab48ba6d7e62aaebc370fe04c1db499e60cbc2a
      de0a579a746a9203

  sequence number: 9
  pt: 343236353631373537343739323036393733323037343732373537343638326332
      303734373237353734363832303632363536313735373437343739
  aad: 436f756e742d39
  nonce: 9bc56885fe63e193ff62b415
  ct: 39636c1bc61e2e833f5b883231edf9440bc29b25ccbb03d603adfce62ebaa3b0a8
      286c2343f0639a31af08d1df279e03a7fe3f2bf25e84915b7b11e461d2153a04f5
      99730a25edc991ed
```

A.13.1.2. Exported Values

```
  exporter_context: 70736575646f72616e646f6d30
  L: 32
  exported_value: 3e7d4943487b9b2a6e56040a271a5fe79b73791f49e9bd18df78ba
                  06a3da7dcf

  exporter_context: 70736575646f72616e646f6d31
  L: 32
  exported_value: ce8934e777b1e850be6a4490a159121a10b1f0b469f817ffe49651
                  9b2d9b4a22

  exporter_context: 70736575646f72616e646f6d32
  L: 32
  exported_value: 383bc2c8cb930be3e5f5c494685e10e45c085a394bf0fef654a56b
                  9f37b45afc

  exporter_context: 70736575646f72616e646f6d33
  L: 32
  exported_value: ae9a1cf28962975edd876488c5d33319e61608b58fcc0d43c6b695
                  a8e4f6c197

  exporter_context: 70736575646f72616e646f6d34
  L: 32
  exported_value: 43c609f55bdfe1e837c523ef35a0be0e9dfa6c6653c58456bffec4
                  5a31c8dea8
```

Authors' Addresses

Richard Barnes
Cisco
Email: rlb@ipv.sx

Deirdre Connolly
Selkie Cryptography
Email: durumcrustulum@gmail.com