CFRG
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

S. Fluhrer
Cisco Systems
S. Prorock
mesur.io
M. Celi
Brave
J. Gray
Entrust
K. Xagawa
TII
H. Kosuge
NTT

7 July 2025

# NTRU Key Encapsulation
# draft-fluhrer-cfrg-ntru-03

## Abstract

This draft document provides recommendations for the implementation of a post-quantum Key Encapsulation Mechanism (KEM) scheme based on the NTRU encryption scheme. The KEM is an existing cryptographic system; no new cryptography is defined herein. The well-defined and reviewed parameter sets for the scheme are defined and recommended. The test vectors are also provided.

## Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 January 2026.

## Copyright Notice

Table of Contents

1. Foreword . . . . . 3
2. Introduction . . . . . 3
3. Terminology . . . . . 4
3.1. Conventions and Definitions . . . . . 4
3.2. Notational Conventions . . . . . 4
4. Parameter Sets . . . . . 5
4.1. NTRU-HPS . . . . . 5
4.2. NTRU-HRSS . . . . . 6
5. Cryptographic Dependencies . . . . . 6
5.1. Polynomials . . . . . 6
5.1.1. Polynomial in NTRU . . . . . 6
5.1.2. Polynomial Addition . . . . . 8
5.1.3. Polynomial Subtraction . . . . . 8
5.1.4. Polynomial Multiplication . . . . . 9
5.1.5. Polynomial Inversion . . . . . 9
5.1.6. Polynomial Reduction . . . . . 9
5.1.7. Computing a Polynomial Modulo (x^(N-1))/(x-1) . . . . 10
5.1.8. Modulus Conversion . . . . . 10
5.2. Selecting Random Polynomials . . . . . 10
5.2.1. Sample a random ternary polynomial . . . . . 11
5.2.2. Sample a random balanced ternary polynomial . . . . . 11
5.2.3. Sample a random ternary plus polynomial . . . . . 11
6. Encoding Mechanisms . . . . . 12
6.1. Validating polynomials . . . . . 12
6.1.1. valid_iid . . . . . 12
6.1.2. valid_fixed_type . . . . . 12
6.2. Converting Between Polynomials and Byte Strings . . . . . 12
6.2.1. Serialize a polynomial base q . . . . . 12
6.2.2. Serialize a ternary polynomial . . . . . 13
7. NTRU KEM . . . . . 14
7.1. Scheme Overview . . . . . 14
7.2. Private and Public Key Generation . . . . . 14
7.3. Key Encapsulation . . . . . 16
7.4. Key Decapsulation . . . . . 17
8. NTRU Types . . . . . 18
8.1. NTRU-HPS . . . . . 18
8.1.1. Private and Public Key Generation . . . . . 18

8.1.2. Key Encapsulation . . . . . 19
8.1.3. Key Decapsulation . . . . . 19
8.2. NTRU-HRSS . . . . . 19
8.2.1. Private and Public Key Generation . . . . . 19
8.2.2. Key Encapsulation . . . . . 19
8.2.3. Key Decapsulation . . . . . 20
9. Test Vectors . . . . . 20
9.1. Test Vectors for ntruhps2048677 . . . . . 20
9.2. Test Vectors for ntruhps4096821 . . . . . 26
9.3. Test Vectors for ntruhps40961229 . . . . . 34
9.4. Test Vectors for ntruhrss701 . . . . . 43
9.5. Test Vectors for ntruhrss1373 . . . . . 51
10. Security Considerations . . . . . 63
10.1. Parameter set security . . . . . 63
10.2. Public key reuse . . . . . 63
11. IANA Considerations . . . . . 64
12. Open Questions . . . . . 64
13. References . . . . . 64
13.1. Normative References . . . . . 64
13.2. Informative References . . . . . 64
Appendix A. Acknowledgments . . . . . 65
Authors' Addresses . . . . . 65

## 1. Foreword

This document is based on the specification submitted to Round 3 of the NIST's Post Quantum Cryptography project [CDHH19], with the addition of HPS40961229 and HRSS1373 parameters. The original specification can be obtained at the following URL: https://ntru.org/ (https://ntru.org/)

## 2. Introduction

NTRU encryption scheme is a post-quantum public-key cryptosystem constructed on the principles of lattice-based cryptography, which provides encrypted and decrypted data. The basic concept of NTRU encryption was originally described in 1996 by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman [HPS98]. It has been developed by many researchers and has many variants.

NTRU Key Encapsulation Mechanism (KEM) described in this document is based on the mechanism submitted to the Round 3 of the NIST's Post Quantum Cryptography project [CDHH19]. NTRU should denote the couple of NTRU variants that the KEM relies on; NTRU consists of NTRU-HPS and NTRU-HRSS [HRSS17]. NTRU KEM is constructed using a generic transformation from a deterministic public key scheme (correct DPKE) into a KEM (which has tight proof of IND-CCA2 security in a classical and quantum model).

NTRU has a tight proof of IND-CCA2 security in the quantum accessible random oracle model (QROM) under a non-standard assumption stated by Saito, Xagawa, and Yamakawa [SXY18]. To achieve IND-CCA2 security, NTRU uses the SXY transformation [SXY18] and does not rely on the Fujisaki-Okamoto transformation [FO99], which is based on the re-encryption and comparison of the ciphertext during decryption.

The organization of this document is as follows:

* Section 2 is an introduction.

* Section 3 defines some notation used in this document.

* Section 5 describes the cryptographic dependencies of NTRU KEM.

* Section 6 gives serializing and deserializing procedures.

* Section 7 describes the common part in the HPS and HRSS types of the NTRU KEM scheme.

* Section 8 describes the specific procedures for each of the HPS and HRSS types

## 3. Terminology

### 3.1. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

### 3.2. Notational Conventions

The following functions, terminology, and notation are used throughout the document.

len(x) For any object x, we write len(x) to denote its length in bytes.

x || y For two byte arrays x and y, write x || y to denote their concatenation.

I2OSP(x, xLen) Converts a non-negative integer x into a byte array of specified length xLen as described in {{!RFC8017}}. Note that this function returns a byte array in big-endian byte order.

N and Q N and Q are part of the NTRU parameter set. They are coprime positive integers. The first defines the size of the polynomials (treated as zero-indexed arrays), and the latter refers to the modulus of coefficients.

R and S When computing polynomial operations in NTRU, it is

performed modulo either the polynomial R = x^N - 1 or polynomial S = (x^N - 1)/(x - 1) = (x^(N-1) + x^(N-2) + ... + 1).

mod n Where n is a non-negative integer, the qualified polynomial expression should be calculated under the constraints that their coefficients should be the reminder of n. This annotation can be mapped to the reduction described in Section 5.1.

mod (n, P) Where n is a non-negative integer and P is a polynomial, the qualified polynomial expression should be calculated under the constraints that the polynomial is the reminder of polynomial P, where the coefficients are also taken modulo n. This annotation can be mapped to the reductions described in Section 5.1. Please note that this is an NTRU-specific notation.

Inv_(M,n)(P) Inv_(M,n)(P) computes the multiplicative inverse of the polynomial P mod (n, M) where M is a polynomial and n is an integer. This operation is described in Section 5.1.5.

Phi_1 Phi_1 is the polynomial x - 1

Phi_N Phi_N is the polynomial x^(N-1) + x^(N-2) + ... + 1 = S

modPhiN(P) modPhiN(P) reduces with Phi_N where P is a polynomial. This operation is described in Section 5.1.7.

modPhi1PhiN(P) modPhi1PhiN(P) reduces with Phi_1Phi_N where P is a polynomial.

sample_iid sample_iid selects a random ternary polynomial. This operation is described in Section 5.2.1.

sample_iid_plus sample_iid_plus selects a random ternary plus polynomial. This operation is described in Section 5.2.3.

sample_fixed_type sample_fixed_type selects a random ternary polynomial with a specific weight; it has an equal number of 1s and -1s in its coefficients, as determined by the parameter set. This procedure is described in Section 5.2.2.

# 4. Parameter Sets

## 4.1. NTRU-HPS

We define four parameter sets on the NTRU-HPS algorithm.

| Parameter Set | Polynomial Size N | Modulus Q | Hash |
|---|---|---|---|
| ntruhps2048677 | 677 | 2048=2^11 | SHA3-256 |
| ntruhps4096821 | 821 | 4096=2^12 | SHA3-256 |
| ntruhps40961229 | 1229 | 4096=2^12 | SHA3-256 |

Table 1: NTRU-HPS parameter sets

| Parameter Set | Private key | Public key | Ciphertext C | Secret string K |
|---|---|---|---|---|
| ntruhps2048677 | 1,234 | 930 | 930 | 32 |
| ntruhps4096821 | 1,590 | 1,230 | 1,230 | 32 |
| ntruhps40961229 | 2,366 | 1,842 | 1,842 | 32 |

Table 2: Data Size in NTRU-HPS (Bytes)

## 4.2. NTRU-HRSS

We define two parameter sets on the NTRU-HRSS algorithm.

| Parameter Set | Polynomial Size N | Modulus Q | Hash |
|---|---|---|---|
| ntruhrss701 | 701 | 8192=2^13 | SHA3-256 |
| ntruhrss1373 | 1373 | 16384=2^14 | SHA3-256 |

Table 3: NTRU-HRSS parameter sets

| Parameter Set | Private key | Public key | Ciphertext C | Secret string K |
|---|---|---|---|---|
| ntruhrss701 | 1,450 | 1,138 | 1,138 | 32 |
| ntruhrss1373 | 2,983 | 2,401 | 2,401 | 32 |

Table 4: Data Size in NTRU-HRSS (Bytes)

# 5. Cryptographic Dependencies

## 5.1. Polynomials

### 5.1.1. Polynomial in NTRU

NTRU is based on polynomials; the core algorithm of NTRU is described and calculated using polynomial operations. The polynomials used in NTRU are similar to well-known algebra, but they have some restrictions and specific properties.

The coefficients of a polynomial used in NTRU are non-negative integers and computed modulo a constant factor. The modulus may be either 3 or the value Q, where the parameter Q is specified by the parameter set; NTRU uses both at times but assumes it is Q unless specified otherwise because Q is used in most cases. Computing modulus Q means that each coefficient ranges between 0 and Q-1. And since Q is specified in the power of 2, the integers Q/2 to Q-1 can be regarded as negative values expressed in two's complement of log_2(Q) -bits integer. The polynomial operation of addition and subtraction under these conditions are defined in Section 5.1.2 and Section 5.1.3.

The degree of a polynomial used in NTRU is less than N-1. It is due to the polynomial modulo called the reduction performed in the multiplication operation. The multiplication operation is described in Section 5.1.4 and the reduction is described in Section 5.1.6.

There's a special form of a polynomial used in NTRU called the ternary polynomial. It is a polynomial whose coefficients are only 0, 1, -1. Further explanation will be provided Section 5.1.1.1

A polynomial used in NTRU is generally represented like a_(N-1)x^(N-1) + a_(N-2)x^(N-2) + ... + a_2x^2 + a_1x + a_0 (where N is specified by the parameter set, x is an independent variable that doesn't take a specific value, and a_0 to a_(N-1) are their coefficients). In this case, we don't think of a polynomial as a function of x that we can evaluate; instead, it is a quantity in and of itself. So a polynomial can be conveniently represented as an array of the coefficient values { a_0, a_1, ..., a_(N-2), a_(N-1) }; it is an array of N small values with the exponent factor being implicit in the positions in the array. In all parameter sets, Q is less than 65536, hence each small value fits within a 16 bit value.

#### 5.1.1.1. Ternary Polynomials

Some of the polynomials that NTRU uses are 'ternary polynomials'. These are standard polynomials that have all their coefficients being either 0, 1, or -1. Actually, -1 will be Q-1 modulo Q and it will be 2 modulo 3. The standard operations (including polynomial multiplication and inversion) can be done the same. However, an implementation may decide to optimize some operations based on a specific polynomial being ternary.

#### 5.1.1.2. Ternary Plus Polynomials

The ternary plus polynomial is a kind of the ternary polynomial that satisfies the non-negative correlation property; the ternary plus polynomial has the property that the sum of each product of all pairs of the adjacent coefficients should be the non-negative value.

For example, the polynomial x^5 + x^4 + x^2 - x - 1 is a ternary plus polynomial because (c_5 * c_4) + (c_4 * c_3) + (c_3 * c_2) + (c_2 * c_1) + (c_1 * c_0) = 1*1 + 1*0 + 0*1 + 1*(-1) + (-1)*(-1) = 1 + 0 + 0 -1 + 1 = 1 >= 0.

In the implementation, the sum need to be computed modulo Q, so the modulus may need to be changed.

For above example polynomial, it is computed as (c_5 * c_4) + (c_4 * c_3) + (c_3 * c_2) + (c_2 * c_1) + (c_1 * c_0) mod Q = 1*1 + 1*0 + 0*1 + 1*(Q-1) + (Q-1)*(Q-1) mod Q = 1 + 0 + 0 + (Q-1) + 1 mod Q = 1 and the sum < Q/2, where the negative values are represented between Q/2 and Q-1, means the polynomial is a ternary plus polynomial.

### 5.1.2. Polynomial Addition

When NTRU adds two polynomials, it does it by adding each element of the vector independently modulo Q.

For example, compute the addition of A = 7x + 6 and B = 5x + 4 where Q = 8, below:

```
A + B = (7+5 mod 8)x + (6+4  mod 8)
      = (12  mod 8)x + (10    mod 8)
      =          4 x +           2
```

### 5.1.3. Polynomial Subtraction

When NTRU subtracts two polynomials, it does it by subtracting each element of the vector independently modulo Q; that is, if the subtraction of two elements results in a negative value, it adds modulus Q to the difference.

For example, compute the subtraction of B = 7x + 3 from A = 5x + 4 where Q = 8, below:

```
A - B = (5-7 mod 8)x + (4-3 mod 8)
      = ( -2 mod 8)x + (1   mod 8)
      = (8-2 mod 8)x +          1
      =          6 x +          1
```

### 5.1.4. Polynomial Multiplication

When NTRU multiplies two polynomials, it does it by multiplying each pair of elements from each polynomial, and adding that result to the element indexed by the sum of the indicies. For example, (2x^2 + 3x + 5) * (4x + 8) = (2*4)x^3 + (2*8 + 3*4)x^2 + (3*8 + 4*5)x + 5*8 = 8x^3 + 28x^2 + 44x + 40.

As the coefficients must be within a specific range, they need to be computed modulo a constant factor (either 3 or the value Q; NTRU uses both at times, but Q is used in most cases). In the above example, assuming modulo Q=16, it would be (8 mod 16)x^3 + (28 mod 16)x^2 + (44 mod 16)x + (40 mod 16) = 8x^3 + 12x^2 + 12x + 8.

Then, it needs to make the reductions described in Section 5.1.6 to this multiplication. In the example above again, assuming N=3, the final result would be 8 + 12x^2 + 12x + 8 = 12x^2 + 12x + (16 mod 16) = 12x^2 + 12x.

These computation steps can be optimized but are not described here.

### 5.1.5. Polynomial Inversion

When NTUR ’intervas a polynomial’ X modulo a polynomial P, it finds a polynomial Y such that X * Y gives the polynomial c_Nx^N + c_(N-1)x^(N-1) + c_(N-2)x^(N-2) + ... + c_1x^1 + c_0 mod P = 0x^(N-1) + 0x^(N-2) + ... + 0x^2 + 0x^1 + 1 = 1, in other words, a polynomial where the constant term is 1, and all other terms are 0. Such Y is called the inverse of X (or, more precisely, the multiplicative inverse of X.)

There are some well-known algorithms to compute the inverse efficiency; for instance, extended Euclidean algorithm (see Section 4.5.2 of [K1981v2].)

Note that the inverse exists for most polynomials under the polynomial modulo Phi_N but does not always exist.

### 5.1.6. Polynomial Reduction

When NTRU multiplies two polynomials, it takes the multiplication modulo Phi_1*Phi_N = x^N - 1 (where the value of N is specified in the parameter set); that is, we subtract multiples of x^N-1 until the result is a polynomial of degree N-1 or less. An equivalent way of expressing this is to add the resulting coefficient to the term x^(i+N) to the coefficient to the term x^i (modulo the constant factor), and then discard all terms x^N and above.

Please find an example at Section 5.1.4

#### 5.1.7. Computing a Polynomial Modulo (x^(N-1))/(x-1)

At one point, we need to take a polynomial modulo Phi_N = x^(N-1)+x^(N-2)+...+1 = (x^(N-1))/(x-1). We refer to this operation as modPhiN. When the parameter polynomial can be assumed to be already reduced with Phi_N, it MAY be performed by taking the top coefficient and subtracting it from all the other coefficients.

For example, modPhiN(P), where P = 2x^3 + 3x^2 + 4x + 5 and N = 4, is computed as below:

```
modPhiN(P) = modPhiN(2x^3 + 3x^2 + 4x + 5)
           = 2x^3 + 3x^2 + 4x + 5 mod (x^3 + x^2 + x^1 + x + 1)
           = (3-2)x^2 + (4-2)x + (5-2)
           = x^2 + 2x + 3
```

#### 5.1.8. Modulus Conversion

NTRU sometimes needs to change the modulus of the polynomial coefficients to a different value. As described above, each of the coefficients is a non-negative circular integer, and values under modulo M in the range of [M/2, M-1] can be regarded as additive inverses, which are values in the range of [-M/2, -1]. Therefore, the conversion of the modulus needs to re-compute such effective negative values.

Such a conversion from modulus M_from to modulus M_to MAY be performed with the following steps: The operation is performed by mapping each coefficient v in the range of [M_from/2, M_from-1] to (M_to - (M_from modulo M_to) + v modulo M_to).

### 5.2. Selecting Random Polynomials

When running NTRU, we sometimes need random polynomials with certain forms, which is called sampling.

We need to do this both when generating keys and when encrypting a message. It MUST rely on a cryptographically secure random number generator (RNG) to select these values.

#### 5.2.1. Sample a random ternary polynomial

This function (referred to as sample_iid below) selects a random ternary polynomial of degree N-2, that is, one where all the coefficients are either 0, 1, or -1. Since the coefficients need to be generated modulo 3, the coefficient values of -1, which is the additive inverse of 1 under modulo 3, are mapped to 2.

Such a polynomial MAY be obtained with the following steps: The operation is performed by calling the RNG N-1 times to generate N-1 bytes, and then taking each byte modulo 3 (and setting the last coefficient to be 0.) While this operation is not precisely uniform, it is close enough for the purposes of NTRU.

#### 5.2.2. Sample a random balanced ternary polynomial

This function (hereafter referred to as sample_fixed_type) selects a random ternary polynomial of degree N-2 with a specific weight; it consists of Q/16-1 coefficients which are 1, Q/16-1 coefficients are -1, and the remainder are 0. Since the coefficients must be generated modulo 3, the coefficient value of -1, the additive inverse of 1 under modulo 3, is mapped to 2.

Such a polynomial MAY be obtained with the following steps: This operation is performed by generating N-1 random values, tagging Q/16-1 of the values as 1, Q/16-1 of the values as -1, and the rest tagged as 0. Then, you can sort (in constant time) the random values; the resulting tags are in the required random order. You then scan through the list and assign the coefficients to the values of the tags.

#### 5.2.3. Sample a random ternary plus polynomial

This function (referred to as sample_iid_plus below) selects a random ternary plus polynomial of degree N-2, that is, one where all the coefficients are either 0, 1, or -1 with the non-negative correlation property. Since the coefficients need to be generated modulo 3, the coefficient values of -1, which is the additive inverse of 1 under modulo 3, are mapped to 2.

Such a polynomial MAY be obtained with the following steps:

1. Call sample_iid to sample a base ternary polynomial V_3
2. Let V be V_3 changed modulus from 3 to Q
3. Compute T = the sum of the products of each pair of adjacent coefficients of V; v_(N-1)v_(N-2) + v_(N-2)v_(N-3) + v_(N-3)v_(N-4) + ... + v_2v_1 + v_1v_0 where v_n is the coefficient of x^n in the polynomial V

4. If T is a negative value, then multiply the even coefficients of V_3 by -1. That is, for i = 0, 2, 4, 6, ..., N-3: v_3[i] = -v_3[i].
5. Output a sampled ternary plus polynomial with the value of V_3

# 6. Encoding Mechanisms

## 6.1. Validating polynomials

We also need to validate polynomials generated during decapsulation; that is, whether they were possible outputs of the sample_iid or sample_fixed_type procedures.

### 6.1.1. valid_iid

This verifies that R is a possible output of the sample_iid procedure; that is, that the coefficients of the polynomial R consist only of 0, 1, and -1, and that the last coefficient is 0.

### 6.1.2. valid_fixed_type

This verifies that M is a possible output of the sample_fixed_type procedure; that is, that the coefficients of the polynomial R consist only of 0, 1, and -1, that the last coefficient is 0, and that there are precisely Q/16-1 1 values and Q/16-2 Q-1 values.

## 6.2. Converting Between Polynomials and Byte Strings

NTRU needs to convert polynomials into byte strings and vice versa, both to export public keys and ciphertexts, as well as being able to hash those polynomials. We refer to this process as serialization and deserialization.

### 6.2.1. Serialize a polynomial base q

This function (referred to as pack_Rq0 below) converts a polynomial into a byte string.

This function takes the first N-1 coefficients (each a value between 0 and q-1), and expresses each as a log_2(Q) bit bitstring as a little-endian integer. All N-1 coefficients are of length log_2(Q). Then, it concatenates those N-1 bit strings into a long bit string; the result is that bit string parsed into bytes (with any trailing bits in the last byte being set to 0).

The inverse function (called) unpack_Rq0 converts that byte string back into a polynomial.

It takes the byte string, parses it into N-1 consecutive log_2(Q) bit strings, takes each such bit string as a little-endian integer, and sets the corresponding coefficient of the polynomial to that integer. Since all bit strings are of equal length, this can be done efficiently. Then, it adds all those N-1 coefficients together and sets the N-th coefficient to the negation of that sum modulo Q.

A close reading of the above algorithms will note that the pack_Rq0 doesn't actually depend on the last coefficient. This is because this code assumes that the polynomial is a multiple of the polynomial x-1; the unpack_Rq0 code uses that assumption to reconstruct that last coefficient.

This assumption is true within NTRU because pack_Rq0 will be called only for polynomials that are a multiple of the polynomial G; we always sample G values that have an equal number of 1 and -1 coefficients (with the rest 0), and any such a polynomial will always be a multiple of x-1.

#### 6.2.2. Serialize a ternary polynomial

This function (referred to as pack_S3 below) converts a ternary polynomial into a byte string. It works by taking the coefficients in groups of 5 and packing each such group into a byte.

This function takes the N-1 coefficients in sets of 5; it converts the five coefficients c0, c1, c2, c3, and c4 into the values 0, 1, or 2. Then, it sums up the coefficients as c0 + 3*c1 + 9*c2 + 27*c3 + 81*c4 and then stores that value as the next byte in the byte string.

If the last set of 5 is incomplete (which will happen if N-1 is not a multiple of 5), then the higher missing coefficients are assumed to be zero.

Now, if the polynomial happens not to be ternary, then it doesn't matter what byte we store; we need to store some value, and this code still needs to be constant time. The reason we don't care is this happens only on decryption failure (someone handed us an invalid ciphertext); in that case, the value of the hash will end up being ignored. Of course, no matter what the coefficient is, this still needs to be done in constant time.

The output of this function will be used only for hashing; hence, there is no need for an inverse function.

# 7. NTRU KEM

## 7.1. Scheme Overview

NTRU KEM solves the problem where two systems (we'll call them Alice and Bob) wish to establish a common secret string that they can use to derive keys to protect future communication. They share a communication path that is authenticated (that is, the problem of detecting changes to messages between Alice and Bob is solved by something else), but that communication path may be monitored. What NTRU KEM tries to achieve is to ensure that someone monitoring the communication path cannot rederive the common secret string (and hence cannot derive the communication keys).

To do this, Alice and Bob follow this three-step process.

* Step 1: Alice follows the 'Private and Public Key Generation' procedure; this creates a private key (which Alice keeps to herself) and a public key, which she sends to Bob. Alternatively, she may decide to reuse a previously generated keypair.

* Step 2: Bob receives Alice's public key, and follows the 'Key Encapsulation' procedure; this creates a secret string (which Bob keeps to himself) and a ciphertext, which he sends to Alice

* Step 3: Alice receives Bob's ciphertext, and follows the 'Key Decapsulation' procedure; this creates a secret string (which Alice keeps to herself). Alice can then either destroy her private key, or keep it around for next time.

The secret strings that Alice and Bob generate are the same, and can be used for creating symmetric keys or other key-shared material used to protect future communications.

## 7.2. Private and Public Key Generation

This generates both a private_key and a public_key. The private_key should be kept securely stored, and the public_key should be made public to the communication partner.

The brief procedure to generate a public/private keypair is given below:

1. Select two 'short' polynomials F and G.
    * A 'short' polynomial means that each coefficient of the polynomial must be either 0, 1, or -1 here.

    * -1 could be Q-1 or 2 in the implementation. Please remember that the additive inverse of 1 is Q-1 under modulus Q, and it is 2 under modulus 3.
    * The polynomial F is a part of the private key.
2. Multiply each coefficient of G by 3.
3. Compute H = Inv_(S,Q)(F) * G mod(Q, Phi1*PhiN)
    * The polynomial H is the public key.
4. Compute H_inv = Inv_(S,Q)(H)
    * The polynomial H_inv is a part of the private key.
5. Compute F_inv = Inv_(S,3)(F)
    * The polynomial F_inv is a part of the private key.
6. Generate a random 32 byte value s randomly

Note that it is possible to improve performance by modifying the calculation process.

Steps 3 and 4 compute the multiplicative inverses, but they tend to consume many cycles. Introducing medium variable V_0 and V_1 reduces one inverse computation:

1. Compute V_0 = G * F
2. Compute V_1 = Inv_(S,Q)(V_0)
3. Compute H = V_1 * G * G
4. Compute H_inv = V_1 * F * F

The recommended strict procedure to generate a public/private keypair is defined below:

1. Generate a random polynomial F_3 and G_3 using the sample_fg procedure
    * The sample_fg procedure varies depending on NTRU Type, NTRU-HPS and NTRU-HRSS, and it is described in their respective subsections in Section 8
2. Let F and G be F_3 and G_3 changed modulus from 3 to Q
3. Multiply each coefficient of G by 3
4. Compute V_0 = modPhiN(G * F mod Q)
5. Compute V_1 = Inv_(S,Q)(V_0)
6. Compute H = modPhi1PhiN(V_1 * G * G mod Q)
7. Compute H_inv = modPhi1PhiN(V_1 * F * F mod Q)
8. Compute F_(inv,3) = Inv_(S,3)(F_3)
9. Output a public key with the value H
10. Output a private key with a set of the values (F_3, F_(inv,3), H_inv)
11. Dispose of any other intermediate values securely

These keys should be serialized as below:

* public_key = pack_Rq0(H)

* private_key = pack_S3(F_3) || pack_S3(F_(inv,3)) || pack_Sq(H_inv)

### 7.3. Key Encapsulation

This takes a public key H, and generates both a ciphertext C as well as a secret string K. The ciphertext C should be sent to the holder of the private key; the string K should be used as the secret.

The brief procedure is as follows:

1. Select two 'short' polynomials R_shared and M_shared
    * Please refer to the Private and Key Generation section for the definition of 'short' polynomials.
2. Compute K as the hash value of concatenated octets (R_shared || M_shared)
    * R_shared and M_shared here refer to serialized ones
    * The hash function is defined in the parameter set
    * The octet string K is the secret string.
3. Compute C = R_shared * H + M_shared mod (Q, R)
    * The polynomial C is the ciphertext.

The set of R_shared and M_shared is a secret key shared with NTRU encryption scheme. In the NTRU KEM scheme, it takes a hash value of this shared key to enhance strength against security attacks. It ensures the same value on both sides of the key share.

The recommended strict procedure of the key encapsulation is defined below:

1. Generate a random polynomial R_(shared,3) and M_(shared,3) using the sample_rm procedure
    * The sample_rm procedure varies depending on NTRU Variant, NTRU-HPS and NTRU-HRSS, and it is described in their respective subsections in Section 8
2. Set packed_rm = pack_S3(R_(shared,3)) || pack_S3(M_(shared,3))
3. Compute K = Hash(packed_rm) where Hash is the hash function defined in the parameter set
4. Output a secret string with the value of K
5. Let R_shared and M_shared be R_(shared,3) and M_(shared,3) changed modulus from 3 to Q
6. Compute C = modPhi1PhiN(R_shared * H + M_shared mod Q)
7. Output a ciphertext with the value C

Related to this procedure, the polynomials should be deserialized and serialized as below:

* H = unpack_Rq0(public_key)
* ciphertext = pack_Rq0(C)

### 7.4. Key Decapsulation

This takes a private key (F, F_inv, H_inv) and a ciphertext C, and produces a secret string K. If the ciphertext is the same as what was produced by the key encapsulation procedure, then this will generate the same secret string K.

The brief procedure to decapsulate an encapsulated key C and to obtain a secret string K is given below:

1. Compute A = C * F mod (Q, R)
2. Compute M_(shared,3) = A * F_inv mod (3, S)
    * Note that some of the coefficients may be 'negative' (that is, in the range Q/2 to Q-1); those need to be treated as negative values for this next step.
3. Compute R_shared = (C - M_shared) * H_inv mod (Q, S)
4. Set Success = ValidM(M_shared) AND ValidR(R_shared)
5. Compute K1 as the hash value of concatenated octets (R_shared || M_shared)
    * R_shared and M_shared here refer to serialized ones
    * The hash function is defined in the parameter set
    * The octet string K is the secret string.
6. Compute K2 as the hash value of concatenated octets (s || C)
7. If Success, return K=K1; otherwise, return K=K2

At the step 1, please note that A = C * F where C = R_shared * Inv(F) * G + M_shared; this results in C * F = R_shared * G + M_shared * F. Since all the polynomials R_shared, G, M_shared, and F are short polynomials, the resulting coefficients are not large (that is, always less than Q/2 in absolute value), and so the fact that we computed everything modulo Q can be ignored. In the step 2, taking all the coefficients modulo 3 (taking into account the negative coefficients); because all the coefficients of G are multiples of 3 (and so is R_shared * G), those drop out, and the only M_shared * F (with each coefficient taken modulo 3) must be left as the reminder. Then, multiplying that polynomial by F_inv will recover M_shared. It must be equal to the original.

The set of R_shared and M_shared, which are a secret key shared with the NTRU encryption scheme, is equal on both sides, so taking a hash value of them produces a copy of the secret string K.

The recommended strict procedure of the key decapsulation is defined below:

1. Let F be F_3 changed modulus from 3 to Q
2. Compute V_1 = C * F
3. Let V_(1,3) be V_1 changed modulus from (Q, R) to (3, S)

4. Compute M_(0,3) = modPhiN(V_(1,3) * F_(inv,3) mod 3)
   * M_(0,3) is a part of the shared key identified with M_(shared,3)
5. Compute m_1 = Lift(M_(0,3))
   * The Lift procedure varies depending on NTRU Type, NTRU-HPS and NTRU-HRSS, and it is described in their respective subsections in Section 8
6. Compute R_shared = modPhiN((C - M_1) * H_inv mod Q)
7. Let R_(shared,3) be R_shared changed modulus from Q to 3
8. Set Success = ValidM(M_(shared,3)) AND ValidR(R_(shared,3))
   * The ValidR procedure and ValidM procedure vary depending on NTRU Type, NTRU-HPS and NTRU-HRSS, and it is described in their respective subsections in Section 8
9. Set packed_rm = pack_S3(R_(shared,3)) || pack_S3(M_(shared,3))
10. Compute K1 = Hash(packed_rm) where Hash is the hash function defined in the parameter set
11. Compute K2 = Hash(s || C) where Hash is the hash function defined in the parameter set
12. If Success, output a secret string with the value of K=K1; otherwise, return K=K2

Related to this procedure, the polynomials should be deserialized and serialized as below:

* C = unpack_Rq0(ciphertext)
* F_3 = unpack_S3(F_(3,serialized))
* F_(inv,3) = unpack_S3(F_(inv,3,serialized))
* H_(inv,3) = unpack_Sq(H_(inv,3,serialized))

# 8. NTRU Types

The NTRU-HPS and NTRU-HRSS algorithms are very similar, and the common aspects are described in Section 7. This section describes the type-specific ones.

## 8.1. NTRU-HPS

### 8.1.1. Private and Public Key Generation

The sample_fg procedure of the HPS type is defined as follows:

* Generate a random polynomial F_3 using the sample_iid procedure
* Generate a random polynomial G_3 using the sample_fixed_type procedure
* Output the sampled polynomials with a set of the values (F_3, G_3)

#### 8.1.2. Key Encapsulation

The sample_rm procedure of the HPS type is described as follows:

* Generate a random polynomial R_(shared,3) using the sample_iid procedure
* Generate a random polynomial M_(shared,3) using the sample_fixed_type procedure
* Output the sampled polynomials with a set of the values (R_(shared,3), M_(shared,3))

#### 8.1.3. Key Decapsulation

In the HPS type, the ValidR procedure is equivalent to valid_iid procedure, and the ValidM procedure is equivalent to valid_fixed_type procedure.

The Lift(M_3) procedure of the HPS type is an identity function, input is a polynomial parameter M_3, and it is described as follows:

* Let M be M_3 changed modulus from 3 to Q
* Output an injected polynomial with the value of M

### 8.2. NTRU-HRSS

#### 8.2.1. Private and Public Key Generation

The sample_fg procedure of the HRSS type is defined as follows:

* Generate a random polynomial F_3 using the sample_iid_plus procedure
* Generate a random polynomial G_(0,3) using the sample_iid_plus procedure
* Let G_0 be G_(0,3) changed modulus from 3 to Q
* Compute G = Phi_1 * G_0
* Let G_3 be G changed modulus from Q to 3
* Output the sampled polynomials with a set of the values (F_3, G_3)

#### 8.2.2. Key Encapsulation

The sample_rm procedure of the HRSS type is described as follows:

* Generate a random polynomial R_(shared,3) using the sample_iid procedure
* Generate a random polynomial M_(shared,3) using the sample_iid procedure
* Output the sampled polynomials with a set of the values (R_(shared,3), M_(shared,3))

#### 8.2.3. Key Decapsulation

In the HRSS type, the ValidR procedure is equivalent to valid_iid procedure, and the ValidM procedure is a tautology function; it always returns true.

The Lift(M_(0,3)) procedure of the HRSS type is a function, input is a polynomial parameter M_(0,3), and it is described as follows:

* Compute V_(0,3) = modPhiN(M_0 * Inv_(3,S)(Phi_1) mod 3) mod 3
* Let V_0 be V_(0,3) changed modulus from 3 to Q
* Compute V_1 = Phi_1 * V_0
* Output an injected polynomial with the value of V_1

These computation steps can be optimized but are not described here.

## 9. Test Vectors

This section contains test vectors for NTRU KEM. Each subsection contains a sequence of test vectors.

The following parameters are specified for each test vector:

PUBLIC KEY, PRIVATE KEY The public and private key parameters.
R_(shared,3), M_(shared,3) The secret values generated internally by an RNG in Key Encapsulation API. The values are serialized with the pack_S3 function. Although these values are not parameters, they are included in the test vectors to ensure that the testing process is deterministic.
CIPHER TEXT The encrypted message generated by Key Encapsulation API. Key Encapsulation API assumes that the RNG generates R_(shared,3) and M_(shared,3) with values provided in the test vector.
SECRET STRING The secret string shared on both sides of the key share. Both of Key Encapsulation API and Key Decapsulation API return this value.

The octets are hex-encoded, and whitespace is inserted for readability.

### 9.1. Test Vectors for ntruhps2048677

---TEST 1

PUBLIC KEY:

57EEE113D3506F111CA9F253D1035C2ACCF68212488724FA9EB144F5D3532E6914DFD
E79861D843A26F0A8D43371EE273D53B90879FD8C2F985F53C59B338784B88095284E
B5A49DC6B5018CCA0806247BD69EB62E1C1431947A90ED8549F79183B27B1F4A81CAC
B7B3F42D631484423516A86FBD49965E7863D06D1347317F0F6E9DB8B9E23AA5FED16
125ED59A9D27CCF7C5BB77FD02ACFF8E9812F0045011022627789D679E30B0DC2AFB5
58316A1714A6958FE9178F7BD8F045F97A5C134C9D7F816EF5B987C441CB56A885436
78F1965F2F5D4E3A6B2940DEC16DE78AF74DB0F8545ACA3F656B6701AB6CE28541C98
F7F72C8FAA26B01D3DBC9F139316380F8816C28FC5254CCED591DFD58690D2BE2B1ED
2F37E7439977BB379B9F4ECF5C8DEC407131321FAFD45AB9DDC4EFA8ABD28B3F81F7F
FC8D7AB707B1418F7035521D59ECF0271E96FCC41FAB7C6E9C5EAD20C8A770E4B8DFD
C950D36884EAD3004FC878C5418A3CEF0A61A2678B9691F97D89951BD874907BBEF6D
EEC410690EC961182645277A747E2C0FB8F7A6742104DA572C05C8F9BB17BCA5BC9FB
FC5268B3FC49E620E1A1732B0E914EB49DF377CD3A496D5FA2B9070F818C034F01ADE
E14768F37D4BD26F4A8C1C8822C79A2F5E85689D8B3758CCE34ABB5680C20FA49F997
D5C882AB4F77C10584F7BCFAF72FC7CE0405F4FE106C53AF063739D81D794C7D19C45
8AE2F98FDB3EDF5D5AED7EC7F8826558EF6D7176A92E4B0130EB03F8081B0D1468F41
58A9A534923C825D339ADB60AB6DE9F339BD87279D29E481CCF6DE733E6181E229B2E
E65731B7240206C9AD0E167BBBD44BF706E26FC2AF74FD3C8975DD73343B1718A9F13
428DE4699196E69348A8FC709F820E098365508B4D222C51D4475E3557D1DA96C99FE
AE9AE55E149FC987A987DACE81CEE2097AB48742025E64277030D49F1262AFEB6C74E
C9C4843DF9B6BA124AC99AFFA94DF662A8E23535EDC001545F6FC8D8CD1D87DDC3B50
C4BAE74C004BCC8249CA12E353C0B86AE65D0E676B0A9817404D6047A359A3246819D
185DAA114A878B43B03A3BFC000D1E779B41486CF0066EAD68E297CEA9280CF4BBA50
F9637718F3FBAFA0687AE5501A1634BE8F318A842C235E5D149BC50ED51377360D27A
60B2EB6436635A656A2A7B7B879DB9F5CE817729E8249D1A6BBE70092D989E1A23CCE
2E040190B7794E2798518D29B75AC10CDC9FBE897BA489228853F7AFCEC4A71B35633
A9CFB58429A62C9BEC7DACF66E94EF62010E98128C6361C5A8C51067E1FF45CA02

PRIVATE KEY:

D067D98F0055E2C3DEEF1076BBB755AFD065112C85C46E6C350655D9625073E94E452
8C053E720206CDB780A61AD5120C498A4CD3E60C334D8702F0F79D81418AF959CAB77
22EBDD30DF0A479E1403D337AD923E5DBCED4EE04839020F7751C075A4892AABBB0E0
01ABA95515E1B65C63C503D97E51EAFB9AC930F5A1DBCB7E9388B5EF1E75E89020D1E
5181B4D12060B6A8A8143F275E38D559D5F18A150F49E0CB73A2972DB84F57DA46EF4
D8AD11F2B4F5A9526A77901BA600FC6E9C9E6F07AC2D9AD2440BC2BB171439AED3296
435D3B7F102CE3135D0D51C4DA052E9163C6A1646ED80FCA390960E3C402241F5FC05
3BC5703558AD9E9CCDB5AC4284B6A69D36C042E297C9C48C61A85735D8C020D2F4377
4368CC183538FFE6D7021029A3E5F1EC56F5EE9ECBC09F5FE092F87657D3412B3F66F
05C99CA6F2704B43FE5422D342B4817CF3A51E62FAE2821D7A0CBA835187945112005
8BD863D189EC80750489F8DEB435D39EA10347F7D0D0419D4A9ADD5B24402DAA99B55
C94C5B71C5B35DD7FAC204B984DE339690D6DF89E276E855A635677BBEE380A1C2175
1B6D0F13145FE4769A0103720AFF6F14181A42492303553EFF4690BC397D4D43BFBF3
09A58906F32FD549A6BE55AAD7E1229CAAAD718214C6FEE3690A45532B2C4E82BC4B5
4F2D8CA43020A2F166306860D301D563F01CA3BDE59A3FC79DBC7A6220FF77933E2E5
B59BC938CB86B31D74163B4F37A0BD9C58082F1EDC89FD52DDCB633C0010C01E0993D
F867FE63299C010AF0767899B45B05B9BD8A76487D5828391DE2579B7B653CC0CC4C1
E694F7180F3B1209F27C6E7EBE367E6271667B2E164C94D0DDE36E32552DDC01355B3
6D86572D8208573F0A2C309121328E56A6A50F0B6ACE202C376C937376F642F269279
923373681DE9F9FC7375E75F3433333D58D721FBBEC08CB99DD82977F4B3DF907D640
EFDC19DDD5C2C6374B6FB2C6734B8508DDBCB82E6926AD126F34739A62E5B0F66F3CA
20C42E8DC0EDF4BB97227334E5C3A90D1A5A392D7341B3707F02459D12FFF1208D0C8
8A2B7C6178887E42D82AD7021C0930CF6723332DD20BB4AB8142BBF5D7969F2B96205
8E78FC871A33E530026DE2490405DD44084D1300CF98702EB5382402F81A4BDD3B851
4F0E7638260AB418A4673F7DF3595B96170B41BB87595A41C5BEF56CDDA831781E13C
BEB3CAE756C6CDC73BC2AF82F7EA1D1821B2F5597A7561367E14AA513BA9FC7138238
10B8C7A5D7AAB81E5FFF6249F80342C7E573A6C60C8E82CF39947BC820F0C7710CB32
01C17891EEFCD89E3B1CC5065993B4D48BEC3F298C4F3EB23125A4EECF5D1A29DCDFC
60C96B40F584996D0B91154AFDDFBA2C19DA34D82389F7361FCBBAC69F2A88336539B
020403F3A19B92D5BB65610116CED92151CE2D176C27778B08A7D4AAF6DA474D1B33C
A0C13905483B0AC84C5351FC3B7ABECD57DADC126A6210C45288F569577A52F299192
B1B6F414B2923719E7838532E4DA6C35BAFDE5620CFD2AB751D4652DB3D062477B5C9
62630123D68016D8D7ABE325EF4D20118F217C74666CB1421E7456958F25D2349429B
1243280CDB0D0F22E8FDEC6E91E5145D4A0085C077EAE0EB3B5CD73DAF3D1F05C2970
F3E962B665A604DCB58887A083CC5A911F40EF6B78009B1431C15CCE02B8C0841DAF4
D39750FD73EB8A50042BCA6139F764481FC96CEB468CDAC1576AE

R_(shared,3):

C226347CBFB10C4C946A759407E8E98C8861D9A562A78977777EF1B04AC593955C2FD
A96DE57746802C041CE163D722AB71A07D9341956538C9A12171687E9C7050E4A5061
959D6B4A19643F0F041D1B1767E15CBEA993E0C948883C9C364DBAD893898B37360D5
C10060BD66876399314E51F9331CA25C34F1C14BEBE55D6F28B929A57B841C602

M_(shared,3):

1B1B690A1157DE06E451B909A51B02544DA3540005003A36BA570B920038010102062
4036C746E0A1251000C5121001800D80FA209243F1E8A0236143F512454C603BF085A
5100B4060B00254812A73C186CEAC1ED6C52A61C0B6E185953D9003802000224F0BE6
3120688A25106A805363F858536A3486F66C0080B00036E00A7072E00511E1800

CIPHER TEXT:

A1D9CE5958DACA0F9799C9AE5D4395CB6368371BB9F93F906DAE552F529B1CA5DFEF9
BFCBCED6C74F3F189F1A165EE30A90B246DC729FA08D14DC82647E2EDDCFB9BB242DB
2EDFBD70F555241028A80A666ADFE7E597E71D4B43C072EDB54390E9D8F5A76EB85FB
1CFE562DCCFE333C3FA8ED2222998A583284E75A65E5FFF9DF51F0549B5C8C0C12D40
89A2121D9DA1DACFEBA4E6919ABBC580AAB4EFB9FA341A073CFFA40E5EBCCB7ED84C8
597147BB888B50EBCB4A0618E81D73A64BBC5465DA64A525098E27647627BFD0F91D5
D636754A4310F5D34E3BBE3502BADAAF0A589855F3AB64E1F2DBF7BE8F7A257B553F4
A1BC12DABA163420D1782FE4830E013E17397FF012F5F6988BAF89FDBE61EB1150300
309C00DEF1F055B90D1F59AC349528FE94EBFA2DF6DBDFB83A6178F5F22E7CAD8FC44
ED46A9C582235D62AB5D750F82CD731AC5E30ED691DAFD0BF0512571C5A39C1F62720
2F46CB5EE7F6CD8CD4D4FD3A68E6996B9AB77FA686AB596570AEE23ABB0521CD04185
731141AE1FCFBE618924AC762BFD0524A5108D1447AA48ACC956FD06970F8D7BF90C4
24E6F1437903233A91FEC3BE1064F853C47DF5E5622F68A317D84B770A114942DCF77
C6200CE8D7557633DD9605581CC3BFC79170044F7E212FFA64AD8307D73F6D8929A38
54FAA32129962C9FCFAF3EB1F2F3B4B83DD7EB2825920D0BC9C9C9E6C8E129CC09730
D421E403AC5A9843BE7F40EEC25DE144BAF756904FDF86C867420B9D6F06872036952
4F4CAA53CEA85AF17F50CFCC554DB287B15F134E642FB14B431A0089087CFA47ACD89
85B56346EB859CD3D2C9F9B14E0F9E5C8248D7534D8DC5029FED01AB201B27BF1B903
EA198592DAA27ACA9CE9BDF28B4831B22C9E220EB25D556215C234761F0A96B0856AE
26FD92E4B40F7E13C3C3587C60AF3D5C49430F768949D6E0C2439EDE3409858CA4055
E5CAC325E21CE1BFBB2BBD3BBA136E59C7E1DA2598975189111F0730B69E7E1B5477D
13884ADD70B3CA8A95575620347CF50AFA72EDE635EE70C62B566F5B6D2031F3CDABB
E2DC9500DDEBE760B4D80158835C2B00E6BC514F2A762BD699EA97E7324CFA5A9EEC1
1426396DC2E93C943C209AF1525490EF3F1F05EFE797731C9AFF61858FB92F4D0C9B3
4EA6AA1887501D7D961F1E7D1256F77E84BBBF5381EFD57610EC4ECC3900B3A377BE3
02F0F633F1C6C0E38ED9327C743D2EC4D7A2B06449FAA5F9D5D152908325DC77F7C26
74975B662D8AC7F67C78D58F74C8C018D77BFAF447CF55A46F790599E99CCAF40E

SECRET STRING:

49AC4D5D1634C6AFFA5A08C2B228EC806D7870B1517990728663D2D8BBC184F2

---TEST 2

PUBLIC KEY:

A578AF45974972B37E5ABF7C440247288696ECDB528095830AA9C68262FB5FA8706AB
F5DE434D8604E6418B4F42A55A2C8B121F58361A26D6F9A1F7C3EDACD6E4AEF0881B3
0C8EA0C08D2A0F982DC60435C5B3791BC3FF6ABBE349B34055EFD48667546DFAF45AD
47A43633C1930A4D8FA0C31D93B2D1F415668D713C0CAF24C4F9F289A710B3105040C
906F86433C2F6C65970EFD8AA9C6149204E5A9AA1748F46615A1E7ABD2500B727EBEF
F6475337D0D26398D4B94E722844CA476C7EBAE1631C3652449A9CB49F298264553FC
038E0DB1457FE6C716F4CAFA5390A9E5062DEA50CE3D79FCB7D387E06A7FB9A0BF8CA
4C7881E5EE357F0E85FCCA2F490B3E50CE7EF0606B9BD3A32636ED3D2FE79EABDC6C9
3F794E5C096396EE5722F3337775E5806092D2EB8D06539F2688FEB5BE0149197E90A
3F5FEFADA8CA7E1F96CE94E998603C230E5A28CD697A2DC7027403B466BFD52F92E94
08B2F75AE8014C8BBD946996C0D47D3462B6AFB4E377445EE81254015943592D1295A
0821210675ED680C2CBD1C66A4250D20F267235C632914426B6315599986B7E3381A2
135F8CEB69521016122885CE4A9E976FA04B7E50229C9137B7DE411D98D01DF2C3D90
03A4DC635A71701BDD1300B4BF72CCD73961D068B7364B53480A244A482C7705ACCF7
BB101F04233D18F7A3D32F0E000F0214C21D202D1ECB8D99B5B7160A9EDC6D8801C7F
BC53D216C4357A1D1FD0EB413B53C1D25CBE3734A580A6F1E91892B4B3A8C60064F25
34BBF10E2E96D11D69829CBD576F9B794E57298800603EDA1820DEC25D3941628A548
B206DE38C293B2C268F25E898BFCC541AF569515407F6824328006140D5EC04833F5A
985D702F814530D704926BA79194F46735D91114D5D6C1BDE43CE2E88B16F3404391B
5EAE0529622AF727F6F99AC6B4119DEB8A93BF5D49F3329F760AFD56EF77C94D6D0B1
0659B108237FAC9BDBFD26593DEE93BDDE1D4BAFE4A6A9607FD3F6EDD4AD1B9472EF3
9E33A07240842E7B0923B05E715AB1A989A955BD14D58D51B54962E3773C1DC14530F
F358282D4ED2901007A01FA88929B97439CE5C68577F5A9EF35CE796BF7E07EE47298
BB7E42A07962F6DAFB609375771A97F6EFAF8CF134BD69803E5824553DA36642E8CA6
162C29A45F652678126AA670E8FE74BBAA4BF2199530BC9ECD8C6B2A8C327790F9ABC
EB0BD4AC311F518BE9446979541FAB80867AC38C5E8A5754F7B1B808618DA2588817A
CE135033A57F709D8BB63157BA2AC331B64F86D4DEB9B19FFEA2FB7187C951D40B

PRIVATE KEY:

22627B1EDC147AC45554273783748C64731652DB85D80C6FD5223F06D733D038B0075
B54052C7342624D879B3BD998A7E2B51682ACDD0B81C876E91BD14C969795E044286F
88265EAE3C7774ABBEE08B4646109FE0A5E51C8B02DF6D91AD559EB3A2033B144772D
B2AEFC6AE78B31EF11F71C4856690DCE82E653FC01E439134D76B9FD5E07DEC006792
4591241A9059AF3E3C9556EB993E95EE7F3B66E5AEB459E0ECE335233E077C00C0640
262CB886032B789375876302CB40C0D57C85A60942A0B49D7647A78DDD266F26B6DC1
F0285B9B2792259D46D043351DEDC00C01F291DCE4ABB40897616C4B5E0235D55CC05
DBEC395D4253283C5081A2D63753154D5E96E75C2B129186CD2D9EDE5C30209E0E17A
CFF6F46DD9D0142FE45CCFC14B50898C69EBD2377FFA4256813198080330C73F68183
67DEB4CC92F45B0C6825E403271BF1295F9AB11C27605C0B61936AA75810750794080
EDAF43420F7472D3A7928867124DD2AF3FF24BE3B0FBD4F4DAFB0BC3CC38821F321B3
AEE6A2C788899C9D549DE388100F15A7D74ACE91CE981F716F07B88FFB29D3E86C70C
141A45BBF2308BF452FCE43DB979CB17F99DCA47EFDD99F34259B4D552D609EA6B08D
129693B3393F6B41365A9B65473AE0E6094A263E2D429214D5200A12D8A808112BB0A
265D50093A158209247DF78AD0FDF5D774AD0193CA88CF888A3A03D44051F90541723
923CD86CDC48AF94259B1332DE3179969CD1D45AF954E52076C2D5341FF95BE668106
95E51598E13F0EA2F8712BCC18B119A93112E2429FF78AD9532A5943C0CEA05FA0B62
345C3C0E2014BA89BB54CFF1D497CB14B3189F4079BE9E7F35B97DC6AB31AA24D98E9
A1DB803C54C2E0710D077F109BC473418D5568C538DAB85DF8BE72CD21D61312959EF
89B1BB5C2C907997893C6474B73945DBCF679397020DF3EF1783DFB9A4862EBF5F8B4
81AD7B075A5BCB2930A76B2661AFBAD07B37747C2B9A26437158E638F7FC53BF74874
183317453CE7F63C82C1C0DF3A2F4E561E6C4A60023B8D4F49E608D799359D3AFAC66
4FC8FC490DA66F6CBB16C9F1CBAFE405559292170227165BA9AFC244DEBAA2D4B3EE8
827CE1EBB970C3C7FB92D743D58BF261F0C2320B092E5CC599452B18C7A298381761E
F7EA5E1D00831745982B5FCF504E9F1C03B2ACF71578FFD3958CCF6975D0E153B2642
E4834E21FDFBA77B23B4066F398C5EF9043496281023BA73556AA7378EF60D6D570F5
9EF8B9E1B507C4900FC37B6B8CFBE7039C8E72D94FE3981B151B79CDEE0DB1EC1DD9A
024B8E9BFD6AB1B66E2D221B18B410F3AEC020223B1E635DCB2253B5932E02B29D491
6CCBAC07B4F60D7ACFC48D769E2E2E5AF71AD5167699861C3194A85E797A8EDB5AD69
2A76DDCB1260837D31894179670E9A41C622661E0CF65A1BCB38F6506E1C36BF2C4F7
4368247724174965B1FF35C03A9EDE9695916AABABA3F7F03BB29294E4DB1757CB04B
C0559E9C6B9252D1C98F9BAA3BEBF45B59DFEFD588F674CE700C0465ACDCEF298FA17
455E3C35D3319080CDD4530AE5057724C57DCF54316D9A769988C369E4FCF17983FFE
41F5B94EB26ABF946DE45039009CB0D9B37FE50D1B38E307B7ED0A4E3CDD586CCDE1E
69E444EC6195B77C6C42B6248A580CE6E3EF9A2075B1E6DF9F7FE7200D6F7325545D5
50E95FA898790C2FD48CCB90ADAC0D0C88DC053CAA65B62442244

R_(shared,3):

A8C757B487B87B8517A9767301201F66668B11257C6F30EBB96BDC7586A87B9755C0A
0E3CFE2AF36DD22EF4B4F3FA3B8150EE6AEE8CE005F03A1E7E26DA9F0C17434C9715E
474639B22B6344C0AB2197AE027D7C6817ECBE29BAC089BBB24FD5273C91D9C796CDD
64C177B7D13C71C93D0C9EED26568157238E2CEB623CECF6BECB6F10FD55AC500

M_(shared,3):

1B06690055125100010 0D301A2E006210B172046BEA86C06000003DB10001203C4C61
B1BEA5126120305EC010AAB3C00400100360B12630A120113090F044C66A278DB6906
46212D00212F5BC82F2406011BA3482409CF1B11B687B738541B4048600087141D0A1
DBA08073DA201003A89030506D952485154001852632136360B06E26D0603A400

CIPHER TEXT:

D35301A661570E2B1CC9096B5B07873FE93404C90387DD4F2B38DBCFA2605F22EF3B6
564A1DF8CCB2F25AFBE085FB9FC04020938C640CDDA29237CF5DB20DB6F566C8D1D56
F3B5C9E3290889D79D1CBA9143DF71BEE58AD2C123AD25CBC01D56BF26F64A0F72116
D1BB1369E66FEEC1ECAB80ECA3CAEB72E18BE3FA1981335453AB364A7B6D656A554C8
4A660B163B2B853F13698CEC823AC170D1520C9D559E75A46EE776A3EC2BD4C3DD654
CD5959EA35B0E87AE2AD6D114C30965050DC94F09356711A8C439163F9DC4DF63C87A
405C1337DCE40229BBF49506E08345DA987ECE7841CE97BECC0DB4CE481EC3CEAE6E4
E45641B8C09216EFCECBFFB47CE780429DEF977A894DA333C6AEA180228D22D084A33
325FEB9A7C4559A47DEA7B325173CCA596206F2DE1611D5169B554A69432912193B8B
B10D6872637C2FA313855863DA2282061A82C21AFD8FA8FAFE5FB7FCF5EC06FD8AB75
5A257542C795750B7FCEFB871EBB9F8B1D84BC95597D1589D550D97CB2928A96B072C
B9B3D8D3EADCC3D513A5C17E85B2119F47E5F6B06D87CDB793264FD74B347728AC24E
F5B87F18A6F917BD8FDB4F66B5CA9B76D38A7EAC212EB917254F7BC8B30F02493874D
2F30628FE0C5F78C2E447755742AD4B1F2223D38139E3DAE87A78DCCD1F09F7310311
F8DAB26EB38CDECC430DADD34F67A3E9AB0ABE496AF867B58070BBB44EBBD226B2E0A
0E56EDAFF2BEA6256CAC850693266DE73C0C618A105E6E35569D40DB6C4F4C8398AD0
04DC43BC095D4070E799E68FAF1D3F2A6F52A3B5AB373FF2651D6989BC3E48362CEC1
CA581D39D39AD3CA2D0EB674E6BC1F0D7731771C215FB020734D032CE9B65CC39358C
59753FE3411C1A87E0B4F0E023CDFF2C83EC5E0B434E918FCEEFFAEBB5E9BE60A4325
E41AFAA855CEB18629AC17C8715A9422D4D743617E5AC3FDD8C66079A464F7C498317
E71A936C87EFFB4C4D45E79ABD2A31BDD4748C7B4EA390659116D722F4090EFB38378
FB8C539D19824FA050F417F16F51AC8B231AC67CAE1B75854F1B94215210A57CF1D9A
11691E4722D19DCDBA5E3923902B8703E8FFD765E0321595C25ADA089C27EDF218647
087E435F0AB8D5B41EA14C0EFCD8E39B860D5793F84B3F3B16F44E23A2E8C537597EE
9FF66F0FCEA3767594EEFB00DF63D8B9746584B81E24DAD5C6F9CAA3BE5363BEC8AF0
34950628DAD3B229E89C330288569F180D18643210266D0CDDF5A1BF851A5F3415858
DB06DB71D1CFA1D38A8B53DFB5EED6D2932F525665615BCC10951EBB71136DC703

SECRET STRING:

959A21D8ADD5D8E120EF160F2AD17A6B3F071A765413C945EC6AEAF3281F6D6D

## 9.2. Test Vectors for ntruhps4096821

---TEST 1

PUBLIC KEY:

```
5C613A66185D153995ED00F800682F17CB11D38146A07081BCEB403B42DE8BEA93AF3
82E8402E7B68A9DD46A1A208A0579F650A589452B78890D0E0BE79929E86F97B307C7
984924FC70F4715BDF5AC5C2D2291F565BC5D1EFB2FC6E956093186491714CCA6FD5F
403E6B27488207A4BA7F72EB3C000CE0757084FC63325056ED60F5A338285687A830B
9403DB3219DFE27C627808DE7CA2ECDF62645CFA0922225A61A3E0D56DF346C052F93
39A562F8AD1AAFDBA3B814A22A09407061AA923410F2ADE2CCCB3A6D2246F57A9B345
1E7E5E1AFAE22A15E1E114FD0AA4EEEADA1292CAC8EC99E53722D92FFCE5A7D611CD5
F4175644BD80248B8D7EB8C4FB97CBB4431C03C5CB01B7F3CCACE17B8407182487662
558F36A5462AC7B164277925EDE918FF5AD787D6FDF4183CAB33EE354E615AABA00C8
7D3ADE9CA264AB0F1CE37D0573E67259962ADD977610BD51714E350F14159BA34E52B
C01B2530EB6CD419CF00ABA5C0217D705641537B17D19A0FEE2731B6068741E0672D1
624259184DBF1D2150572C838327A5B2F85508971C559F679DB62B2D13D8EB0EE589E
B19D528E01421C0304D2847E8D6609F43D0455405ACDAF6F979B4A991E2BB0E15E45A
269866861BE50238057F0B2F4F7E2C09AD437D638DD0343B0BD0B8D3D03F8DE3F0617
C023604603106C2BE14DE726231B1C64EC45E6DC21AC1526359888CD4D559FE432774
8018230D03668446FC4ABFB70801122D408AEEAE4D0282051609B987DFE0D5BF1481B
85F472D746BA01D6AAF53D9019B127BCE150AB941B65FADBF21F3A752869FA813D631
B2BD9DEE1F2A3875866CC8D5694878C66FACD5D993F381C3808809E992FA023C0F3F1
42D5DDE99DCE345353A019CE498597EF665AB40019841BBC1AEBAC15E4AA6D70F21CE
A5ED5C5E890828DAED4BF30B94B5C69CDF9CECFB69EC59C03F3FFE57EF90570879ACE
4C412113F5E1DCDA9D7859BB28A092FBB70358D9861B14F962920280177E5F3414645
10FEF36DEE8A8B61A7F94512C7C1652ECEED0F8C960A2B59C025C21894EB26362C967
8D1672E7F4A67E12D69AEDCB4CD8736862B7BDB8D25863C5BF7CB37167116BF780CF7
6778920BF09349B66FF1B4A62BA472B8E382BE85C45B568B432A78DD7E69CE28A9B3C
455B1030311F92D6AD5F03D0CF06B31CE620262B3E5D3636D5A4607CF0FEC5D0024C2
96386D7F424E40C0C45B5E7F33089430212998864BBF3F448F9A6994EFFE90AC5A4A2
D339F1700AFC67B96127BDC1CB8FF00D91B80108DC9EFAA684164E5BA85E14A077652
82903554D582889EAB6190A6DE5072ABC23A6A72211D1335E14B7DE77E3A7BF339BA3
8403A85889ABAC506BEF51B572F84AC1F1DB1BBED01A98AD4660A187EE109642A2763
619BF74B0A477CD109CEA74AAD6B083DFB6181C361014338E4791E837C94C343C9419
10F414C1DC3613AE440108EC23E4569CE8DE573CD8C1880753F88D7E488566A3C16F0
FF85C70704AA52B410E1D8AF8694BB746EBC25D3D0B18EF567CCC4E1A5764D96EAF3F
34396AEA73C30857685F54B1D916DE38E01104ADE118D9683777D89B5300E41292CB5
A67ED64F3A9A82854435AB0C36F10A82B5552EF1D0EF9312CC24476E4B88A892DBEDC
7A5402996C922826CD88E4C5D3C9A08A1AF233AA559E934DA68E6FC16036C8A17267B
695FDE343F4C894C05BBBFEC05928AF9C3A4D7E83CD13
```

PRIVATE KEY:

```
D067D98F0055E2C3DEEF1076BBB755AFD065112C85C46E6C350655D9625073E94E452
8C053E720206CDB780A61AD5120C498A4CD3E60C334D8702F0F79D81418AF959CAB77
22EBDD30DF0A479E1403D337AD923E5DBCED4EE04839020F7751C075A4892AABBB0E0
01ABA95515E1B65C63C503D97E51EAFB9AC930F5A1DBCB7E9388B5EF1E75E893E1B5E
49955E7E3E4B3819DBA9EA9D23B0986F0DA2ADDFF0A310595267560829BCAC325D3E5
CD1755D2BAFBA02D35C4E426A93BDAF184CB66F78E28F5C7C8CA66B877B5D06DBAFA4
85597366B214EBD08581A8219FE93DB6A3679598B561007E58B07F13B53ACBAC3F1A4
2AAD8828766B8B9B43AA84EC6AD1D66293F8822767B2AC7D9A1D8B471590B5B253045
BB5C622112A0F2C0C5DB11BF749C82BC86B93F92DF3167066C9D7B0FCCB9CDD45336D
D74669A6551D2059228E2B0DB8174756099B25FD41D5BEB342E1D3A2E5566ACEDAF9F
6CF9827789438FC8C2B98C6C06EF888DBF016773BD340BB6CF89673F07F93F89DFC85
3C2402739B7291E8CD765D76324DD1A1BE1761561B29E91EDA39C49E18B382C3AC083
0618F5550B6EC719F70D510F8749D2518C2711D44925AA5CEE7DAF64A3411C00489ED
5A5DDC1E3F46964B5E257417FEA5C68F15651D66604C4A3C376B7D73DC7AC10104CCA
A6949AC3546C140FCD398066C2EBDE9B467557CA00C125D30FFCF2B378872B0B8C064
B1917E179DC13E000714B3E8058F5F3A2F582C50A783D3CF3F3A3F8564A19E75CDA2A
1F62C4ACFDF34AFE021EA2D4243A0737B712A8C1ED04558FB400A6BA1D0206BC72EAD
95259C66CD2DCE5683BC7CDBCF92588BEF64499A8EDE1E6F6C86C97388A20AD2FF713
6A135A895AF18E27D2DE5823D3C5A17415282C6B1BDD59C4C4D94D94D521AF151AC70
C0854FA3C18079F30F925967EE00325FCD6629AD35F0FC5E15AE7B1E43C38070987EA
D6287921992E7065A170B30E1AD7794E7E8660E2F9C6108A53E17743EB278876C920F
23D9BE6FEA0CDA7DA05881565059829A84FC0F233554861130888595CC050FBEEB7E7
189F02385A81454F9DEFF0A89B13CCABF2970CD395DD0DEDC8C3332AD17B6CFF2C1E2
BA867E4743947AE90EB89B72D9A3F5E1AB12A9755CD3B575C7E5A1524608762A788D9
23DE233E8110E584C2D450308ADA06CCA1B6D56A222AE93ED601DAA429D12C11EAE0D
AAEEE36B8C7D972C229BD59988726CA90BFF09D995B42F01A69FCD4BA10FBEF43C1C8
74B493E83B904ECC50657F6BE4B554A5331CEE26EA9F33D2A37A8312D229EA5CA55CA
FCD1BC6F49E15C1C05591AE746B22F07C9D33A8B79A9D7E0B32BE800B02CCCB2BD806
86560AA396F879B150A5784F892052864BA9CFF1414A03A0BEA2DCF1125A3441F0A62
599911064FC31EC6449B1F1730BF3378049B9A70EFFE49D9573B89D7144ADB6FD6586
318081BB6EAD9F20D6210026AE5F8C1E4E6DFBF334650964CD62B3DC73A179D9FEEB3
9767377D7664C76B568C7F85A0BBE65AAB61F2C20726D433296048EBE64AB0496CADF
3847E10B91329534234D8E7B8F2868647369CDF0FF5707BED8EDB58F25DD68159FC8A
0162A85BBEA35312351E508631FBD70F158ACE9DEC73A5ABE2A0472C819152CF7CFA1
6D7B7A43489A5E48A4C2A1793B61FA5C3C9F02D072DE4EED0CB3FE789BAEFA4010046
46B1B9C9D5C63CF2CE7AB91C3C69C1D97E81E6B2B14120335DB22045697D7BB7F1E67
65AF8FD7E5D8ABCBD6598E7B1B3FEC7970E200F62267A162E9DA909CAE1A93E88EBB8
2B7378C3306A9DDEF07FF137DCACF4B6B0912B65B43711F27EEBFE2C560069BA05A0C
48D06EFDAAEEAB06309C125A051BD796AAA0EC756CEC8A2E41AA5A4EE36856EEB483C
1BD91CA5304C6A1626B54C4AD4942269DBBC1E82BD3C16831B8FBB4E8449245C07608
2904D756BF195ACBD7C2309796D9458693AB541E204595C4CB0B1392A851CD7183DF5
C0256C0599C1891453E3A95E77B8D9A5B2DFC0B3FF438BA0CEF61CF97C29B99E16D6B
CDDAE81F4E4C0555F81012E1823F36A0D85C0B7D80112E949956162F9755EC809026C
F9BDC1AA391108D05C043174B7A1050E08D41BE4DD86C22ED4A8E5AF78D2C8B5F0C2A
35FF442BF22A9195631B713D3135800AF23A4E298F955D2D0A629A75803A21EFAE699
D2919753F189832A45D71665F71BAC96F48528D97E70EE5794493F010D3504F5BD329
DB165A
```

R_(shared,3):

3D389E611A9FC752D47833AD43E5B4DC17DBA95BAE7AEC5D7EAB7103A3101188209CD
5C013682CAD1432E57336BD641CA33E726398006915D7BF88CDEECB5421182536824F
7A385AD893552AAB80E098241E520BD59EE273D224966BBC789CD9A0BCC76ED76D6D1
2CF9D2CA1AC55C4A9CC4C56D09C49EFB27ED9120E24D7E2C604B8CB1A0C8077EF8BF1
E03920396F4A4195D08E5A691F2F89371C6158E961BF848B3A7B

M_(shared,3):

D712DB52308A51B1982E9C124509D75E2375317F36866B232400C2981BA2DABDBF020
D9A010A3B2131ABB5AF1999AA13026F6E5E03B156EC80400488418C966050B63FE7B4
D8042117ECBA4388253F5665DA3820E87DA4A62E1F2B6792C7C93EAD380D2907D2152
DEB08A3313AE795C13201BFCFF20E7760CEB9D547B08BE2C9C837708C62E5C443A456
054904C10E5D646DB9C8EDB252B6849BA4124D48C09D5F00CE99

CIPHER TEXT:

C31A29034AEEF0469718549DFF4F838023A19ABA55BFB249B4059D37F879219B0A22F
17DAB3FF16BA05B3DFD44E9FD43118A41D4317EA35407AAE247E31E90CD9E96BC1179
C337E45C343DC7C783DF7C330F832988F0DFCA9233E2842A45DBFBADF2F6BE8B4CCFC
2E5AFB1BABCC22A7808E5D66167E63410C3127C0869A9969E5C1094ACCBFD2F6FFFED
E2517187F73A6A63B39A9E09A1778E2CF16292465DA1FFDE8EEA45BF9961C48CEB3EF
3703C546960549FF197A04B59C8A2521C22A171E8B214C697484383939A3E4DCF5452
E7E4179022DB5246344C19FFDD2523F8B3AACDB341A3D08AECB3AA42D44655B4F8B0D
EB88839EEE386B52DB3A635191455F928EAE7535B45B5D13539B5FF0331D09FE0D5FD
0C455369B3869212D5D59E1794F680DE7DC80426B396579E706E35501222AE1F141DD
8EFE7C9F4791225A43862AF0C42067F69C5B668A69CFCC27BA36AC227D5C4A5FC7C87
3FBABB604B27145A56D0FD0741B19E930416B2AB1F213D7B0944CA8BEAA861445ABCF
59B217F309F6DA8A2E39C583F0EE2AE018C81B9379EED51AC0B9AD627B3870E5F8981
A2A0F06D153D23A03257F69A42C3650F8CCBC0A1083D37A02413FDF36435A1FAE0E48
B6ED00330D02106119A830A9C0E0DF76B0B96C187B17243BE11E35A2C847F6FF3F6D8
537D42CB63E6E6F89B262B7E7B9246A49A334622E65EC8B77870AA3440EAC77058BD1
373D12AEC34348A12E74E657FEB5921F1967EB15548FF3CB97DF8DDC735BD20D99F93
0DE962173B4ED05CF03FDF53BD3CE72E7A1B2A0CE2F71C64502CD530C509CE1642044
E1B4F3DC4BC79E9CB818C93E68035872E7C2A95A5C50CDB84397540CEB74EF4171A1F
B9C775113B68F8E41ACC11B63FCF9D5A95CF840FF53F3440AA4E7F064544DE4528F03
4A828877B2A11CC5BB3DA6ECD100EAD0D839CF8B37904EEBD7DB2F9BDB913BF3A351C
AEA601330DDF97F9EDE498FA5CC2B109699E43A9C98699A187DB24A595537EB22BA89
B58E08624D7419A06F23CA5AF5997EEE495C2BF3DEADA613F60FC3B9C342250541BB0
0B19B96A6A65EC1A0DD4DDCED734AE0E7FD1244EA14EFDC150BF3B55C0D5F2596469C
575CCE35BF9872B0D14DD2296BA76915F6DA5D341D8A3B808D346A07D6FBEA5DB0C0C
B0332DD5240DC0105680EC3C80A1E8E7275337BDFA3203CCC386C93D9C51271329339
93FCB2D50F16DC0302BC55E8B72E06C914264299020C25351F5E07CE4E726E94D9634
7AF8F04A5E59E266246E8D9CB22D7C6B8C42259DACECF10CF75851FB5909B7BFB444C
26AC801E9C1743D514ABBE73B69298D8F4DED587627A44471270AFC43E5791F71D699
AE36C898FEF4686F940C0C63364A040840D8022DC0A53EA4F24602CC360E724A9F08F
7C7614D1BD91208C789E199B3EEFABD1AC407F2478892F120288AA00C9825B106AA49
40C4463745FB0F7399B570DBFD75AAFDA2217C9B529F327DBBC4F7923B17ACEE60DFB
8105C46C9309EA18C847F25D3256726C411A0E173E70F79C04C6FAD60F1E3C152CE7D
A900D9044BC4E97FD2FC83EE2EB059416F5BBD6B242AE89AFF3A48D49ACC397AD3083
C758E1EDED79FE8EF4FDE6F208B1C6E9614BDA68063D8C7C95842D8A10E4538876E20
53037106AF38FFB12F0AC966643063A0F1674C57209933FD61FDD25FA2CC5E9F7D662
412D998E0788CDF87ED76F115D8F545247DC82741EEB6

SECRET STRING:

293992000DC288E8152F9451F06DD835C75EA008662BACE0FB97A97B3AFB54E4

---TEST 2

PUBLIC KEY:

32AC335F19C615AFF373F03D0BE92569E34141C63F69D9221C69967A95F2300327C24
37BFC74A71C8AC4DC84B8016A1B4DF448AA6F5476D2FB75AAC0DAB4D031D7429A2653
BF7AFEBE28CC494DF4BD14A74E92D70A4F94B3A201583FF414000449ECEA5CBE08BCA
F7028E20D307558D9EF3958A02537018E4FD937190048A82427E84F0C386827880979
B6F26FE1A8BA882CD53BB7C9E62B4A62D213CBB8D70D162757ABF9CD64518BA9BC0EA
220CBFF52E50AA405D62AA3F13B0476BF7F96DCAD4905AA6CE55D7AE8DA9318B022BE
34282740DCBE3E787EBEFBDDD513526C65F6493190F4601A78660A7101A71D7B0ED0C
E6907463A673051AB11E8596A489BA3F7421A5CCFBE625326B6A16E52B72549205340
EAB875FF7B21FA90D14E4292E9774C33997E824BF901D1B0D57DD7A6CAC8FE43086AD
2C6DBD9ED7239DAF2B9A233A64D1DB8F979DC8398392CB3FF967F5870D5AE6C55C447
5923F4CD885A8CB065465EF77B72D03AB1E2267C66B2726B8B6D3394FF5128FE55CE5
AC1200D6E39868D772245B8A763EB42725733BD70E8D3F0F4AFEFF331DB767D5AC44A
5999E5ECD4A0DAD4C6A4CCE79F1FC4DEA894A93CB8BB582FFF6DBCD839162FB61E10D
3EE1E255BFF21405966038FA4139CAAA590FFF2E78F836D45C3DF9FFF95F45D5479AC
B25B554540D1FB9FADD557302BA3473262C717AD6618FB9192CD04CBD22A3A7C2D822
7DA88E3BD9B24427090A0CAB186436217FF45D0D3B87F155116BC6D3E47CCC3BB047F
7A67E827F6881EFD71C30366B63F00F91050D62A0F469ADAB5ED8956C0BE2B4BF50A1
A2D47E50713C45A48B6DC714068E311E2D892C068F008E20F89679BFA2C651660702F
F20ED43A2D1275E688548E4E121A9A24DF49DF279E9E75D9FBB57580CB7E52B83D369
542ADC6F5E14FD940E5A2A3B99353B9940C847D74D216F39BF9BED62BF633F802F03E
639E695C1DB7DCA7C9A10A73DB7B9917B7AE40BE857278D6D116D40E02FD20FF1E21D
1558776E43E7D755F547C63BF844EC8DB35C58A13BD817BA1AF9D4F937B28A3D3C5C1
C22E58CB33605DBDEAEE61DDB54B5C688EB8B934A594089B87D56064589ECD5C2CF46
CD3E8EC6C41473B5BDD2032A780279DC0FDA704592867B40C26EDAED76DD68F059DEB
67E0953F5CED45BCA32DEAA203DFAFC3D226F9DAAE7A0FD6491A54340E94A183CC418
9EE2D77A330364870916E99D9647CF235AA0F69F9834C0C810E80F1D3B56581E46E05
2574AF202EB96E2A8698091A18D469441DA59D36E851C1AECEA6644E89D215DF40198
ADEE7CC147BA3877A8055EA6127311CACA22927573333D049A55883E93547C35D3270
301125CEB37D6A7631AB09103536BBA31AABC44B1B5C5C5A0AE7A3CBE3640A4B92A00
FAC7EBBB56534DE4C507D4A536DF504B78E57196F0E9F773F9311670574283OEBC946
DD3FCAA26B785D824C9824ED843289E9FE570D9D825D88E08B39E89EE6640B00732A4
FB39FC14284B525336D4966DB3C3772DCA12F11DE37FE8A8F880F43A5D3EE4F3FDDCA
93B1D580932C6B6E868A3664ACF0E944D051638A4FFCB1C44353127DAB64D093B1208
14B144194B9C745CF1454E311B45743F0DDA185745C4DBAE19DC82F6CC5D3FB965109
73E30C46AC57BB0E2E84F9AC9DA8F3D499BFFE822C1D8244359CD5F07EEDFDA774DD4
C30E368211F63DBA4D341D418FF424B5F81BC2608A5D4

PRIVATE KEY:

```
22627B1EDC147AC45554273783748C64731652DB85D80C6FD5223F06D733D038B0075
B54052C7342624D879B3BD998A7E2B51682ACDD0B81C876E91BD14C969795E044286F
88265EAE3C7774ABBEE08B4646109FE0A5E51C8B02DF6D91AD559EB3A2033B144772D
B2AEFC6AE78B31EF11F71C4856690DCE82E653FC01E439134D76B9FD5E07DECE48453
78E2430A2D3A50EF44D7D7E57302CB48F09F9625072524497C847995EE1365DD3E2A1
93FF12A4495675D2B304595881874797A18483F8C3C0F1590963AA88CBE5D7B767430
C03AE5416055AD3A2654990843AD92E00B3714023A09DA32181E0225817C067A94589
C62E60331B849CAB0B135A837670342F09235A23B1BDE9DD18DBE0A984969A35B110C
EE90A0C09EA1BBE5DA465BD12C8D7F9BDCB5367C5888EA3F2BDADFD622BAEFEC0CEF9
6B226B2301E0B28D115517E8A2B2721877FED168DC009EC0A9C9F7EC59182F9B18A05
84D099655D3890EB6174A43914BC0432B6481C36693BA3C7C1C99A71FACFA45F7B561
AE35307628B5357D948EB642A9CB862CA81616C3444C07790C884B1CD4463EE2725C7
A38F8900A6DA59AF4BB9A70497BFDDBE1040E72E7C6A928F29904D7A6BE7EF6273DC4
2D80897CF83297701C446FBDC9426055CCD65C5BB7C6C0ED1EBFC95CA960401685969
8C7D964B817B5D74A4A2C409450E0A15C46C841792C87BC0930F8636A60E6A2218CCB
CCCF4460441A09BB3EB09948FA68527CCA12D0163452AE94927E8BDC9F23C2F1A0129
58F0FFE312ABA3DABCC94631C54C5402A56B1A49E10D53A92E51042635B2F31FC5DE4
14D650E40DA045DBCBB5662DDE8343678AD20C31DA33F6952C1975A0F8621483DC234
3B9A973365D6C5AF4F05433FCB823633793574C09E3FBFB063685F1FD80690C860EE6
787A8BFCBB06C2AA8692322949EFA38BB198F75589B84B5ADB22FB8A6DB3204BD3ECC
418D2DC2C0B939011A22CCF90DE3A56CB9DB1FE4CC64292568B63FCEAD011DE4379E0
E151ACB34C4C9224D5F0E1620F87F3FBAD25727838A9BABF9CA4C56D9FD83E1546358
EBF082D3A9F6B0D4571F35E87F9CE575380B3FDFD203D2681C64EE1C4E1DAB7B9F408
AE5018CE41A3F764CAC3F95FE83871BA1784B366280BA5E059F32DC8B28AB1F4E21C0
431B31A4432EE7A79EFA69A4A0D8A8E10C78082296BC8BEA6904EC825326D5EEED854
87E7AFAA3D29DADA95BACCBF2C54D8228EF8B176EBB3EE6488C52C3CD690184EC7EBD
094FFD84A5E6F749F5DD2E10B8D78F35586D28466588D3A6203E569F84134B0D99A6F
8B4AAD4A70B1F514C0999E212FAB7884C02AE3BDDADF1A4881AB5BE4DA6A2E5CF6B3F
50A800DFE01595AC926DFFD4181E4366E4ACD4EE6DDD575F7D0726307B3A0F0B841B2
A280114D1C98E4C041CD443CADA9353BF02EDF8888FA958C7C6CFCDEEA5CDAD8357A5
0A4966B63DF334999A47D41BD586319A96603C9F86689FA80586A6BACE7359AB0A053
CB8C7D75DF85197D80C3262A84EF7490A39E0ACB11F2F76D8220E478E62C1F212CCCE
C599C8046962E7DC57B0707A637DD90F0A275CCCD5733BFAB4D4168FC8A56014C3795
D6CA6256F37256A824CBF9ECACE291B517106206343344C3639C1AAC736ACDEE377E8
329EFF55CBD09EF63854849C9D870F837FCFB1413CFABBC5C7A82BCEE5B7718EB5AEE
03EC1C672ED7C50253D28F6C86AC9CB1B1BBAFA64DBD4264B93D54719A04462629535
59C6DDB4E1535B2920B2B268BDA225CD8347470F309F3CB4F7949334EFC5562063F9C
ABE90FB49D3E06BACEC896F8705CC332E57C1984C278C8C2B5BFC37BF8069692BE824
D065A06F9373C1170F629080E68935B8E8BD6F235A9D2A67C405E728BDE759AE6EE21
E14D994465E50071235AFF41232DC9280CDABD3D2EA40760E56F94787D496727A7129
100FD5AFFC0E876432E348FC2DEFE4CB0CDB3F5B6336E125838746310CC6B16A34EEC
DA2947476DAB1CEB5351DF5139D0604BFE7EA69056465861D5EF25FBBE94EAE24DBD8
316BEB59468075E2E77947704122FAB06BE7A88C01F104CE55C5433693C1534D2B592
ED4DFE30E41B626A36EC0C372DDAB90D056F98EC3BBA8D86B7AE9B8CBA3EE2228BB0E
13AC0988ADC702590470C688B15A0564791487E0D812A0E556288F8ED1CDB201C8457
7180E00672FA7F2272107E5476F3E0689C4440C8134240E01A61590BF6FD817CA3DEB
3E1297
```

R_(shared,3):

55375E967EB40482719E8B5141A94FB1389A792E29AD4FACAC1484B8C0E2641DE2999
6ECEF32E6DE670FD9C8F035A3DF5E1FAF076FEAAB9C7E5C780060106592BC147C02E3
5E4026AF9C1F5A38D319A78A926B42BE52A86568A0983E4ED09C4E819C17590480B98
921BCA8F2AB04B4E08AB88D71B1A4D75920644725A292180AB30412F04BF086217C5C
68A1D2DE78AE003761551CE913155B0B3BF2CC5CA11532C0C349

M_(shared,3):

53456675786C73A61E2554B3197D036E401296C07499833F87634D6E6812C28C73968
CB2DEF20A3A7C095ADECA2FC053A8D624CFC7ADA0CDE18B07E97591731AF2A59B7A51
AA4EE38308A61C8D9F1119B81318560705C1C5052D818741CC1ECF8DBB2110CC2DA3B
E64A7A451086B21DD6A71DD9B0156E292C505255860D551AD9DE22F7C5A0A9635D713
10B40238DE2430BBC708C104573C08AF48C1C4AB88D40BEED155

CIPHER TEXT:

5C9F8FFEA0B0127114C64113174A8F2C4ED7440FC90F4E2AB95C5D9C75D399CD475DC
046C8910FAA98A009F8673EDD4832A2982E2A8057A3AF9FBF184BCD76BD96435D2D95
E9DF40F79B1AB309A63A36180D786EBF9163BC63A4A1A57009F21F5BE69BCE75E20BA
5AADA23F022796CB469304D377BE81E72E852F5E30B48B4F361C9497868D2E6A5136A
F546A266CE1099B7ACA1582C4CB75F507075F1611AEE3FB45C1555AC53B57F57F2467
25FB751AF3BF6A268F6B19BE6E569D4D96ADA6500ED541B18472B0C0804B95DBEB9D3
DF2E09FCBDD52F4882FA9AD026C6751417203EB77F67E45FBCA5F64AADFFF76133C9E
2EBD5A1C9281FB2DD53715D411AD799C3BCD506DD00E0928B4FF37DD487107B8F250F
7240DBF25D3071337D668FD0B3A42347A430C3879D906469483C6C2CFC9FA790E4504
EE6658D2791CA8983C8CA40C9629679C3A7E711D2941A5561EC91B495A1331BB5A321
4795E0039BE952BD5AE00CE4C8820107BBC7B597E56522E279C782306D5BB862974B4
214C186786CC41C3985D058D66A17D7B161E4413341BCDD0957B61E84829710419676
8066E2BF0ABB535EEF63A130966E8409976EF500D8DC1CFE5E46E4C6148EA4880F046
2AFA07E376065D4510037A6286505FEDFA6EDA8062FB72BC43B7812C39FBEE35B3713
4AEA1B7C4D71AB45DB69486C6EE22416C0F11E96F8793BEEC131C849F32681CE8B3FA
1A174806894516BBF93FAC9ED8EE089C450A0169CB2982769816D7AE6AD673BBE73A5
FAD0BC38C126E9CC379AD4FD42A75B3C0AB9DD62A9E08DBD16153D715CFF7C5233AAB
AC035192B8FD918DD305856EB1A676C1831674D936CBD6E3E33C699C08492F4AD4061
549966AA6368EA6687805173EE84CD26DF781495505DC78999B1DE01133FC890F08C0
4D60D308524AE3A5154698C8A0EE65B1D8038D7895C442DDFF51EFAED0520C37852C4
19042CF67DCF648B55D682A13FACBB8445CD8BFC44D20496214C5DEB42055FFA54EC1
BDA90BC410404E975BFD5C628C9B467E85082F91DFF7FE3A880F9918EBD5DE96513C4
F2BE281335537B9407C6E92D31331FB72E8E376F5B7AFE82F6846652BAB6895EC0766
80444222C235F80192A38C7A5D556FD98C6FB6B47D31DE2638233AC80B1D98BA6C852
5448887CE4B8F0D3A940361E1EDA890033EA74BEF51E3B58670F476B38816E040B837
44EACFECAF2B26234F83404F82FE922029A3F91DF2FE64BE793B7F7D73A90A90C410D
2482A1BA6E4F66B97EBE6FB44880AD7C56054EE6E1A5154B68E8FBB79C6A7F982AA49
6D0BD30F22E43D43C461E4C70F31B4FFBD5B36CE8F2E7C3DC0B203E87AC31187C7F3B
078C21E0DDC3FA791BF56595062551510A9D34DA8D5246E50562CAC2F97264E4FFEA1
BFFFD15DB183B93AF642D098E97AD9364E9693D4FBE3E206E6080CC106DF69F04CBCD
5CB5FF098EAC0473C1B4F650BDECED5AA1173C9C0190DDEB0EB41E5350C5FDEBD116C
640C257CD4F0BBA6303A3C67A4588F03D3D1F32979001F6EDAB5E7298263568365533
9709E61F0C832E44738DDD66A656C0818BBE2393F60025B00C62EF223B83339DC1D6A
43F4CCFAEA292D31E78E66AF0956DF43F76B454259831EEFFBE6FCAA5470E9ED780BD
C6F31D577ED8209D8C5DCAB9423D3AF105465AF34414CDB256C7CCEE403AF03015626
5ED2C8937273D0AD28FDC683F2F1B35F992299512B606

SECRET STRING:

F251BF793D31B7CB7EE72992896F35B8F30907B48E8636C4E748BA4930E5630F

### 9.3. Test Vectors for ntruhps40961229

---TEST 1

PUBLIC KEY:

```
5E7AA1494F96AE4E72865B6F0B656577FFB990D67F203B7571957E42C70BB6C839249
014478D72C6933577399701F944CAD17DD426B97E38BEAAA3FB7723F5203150CBE5CE
63E7912C3FA7720E1871ADF5FC9F0316756E8F56F83D55054A37C366700C4980FA16D
EDBA6C1439CC0640ECE170A6AD2912FD96D9883F2962CB4D7E34F5606FED234496E62
23991C4D96B590D73E7F112F0568CB1F80A1DCEC450F7B3307C89AA18E1B67796E976
762B58A3DCFB702363D9BA3F99A43EEB83399BFA69C6CE07B416A5DA6750C1C71A54A
0ABE620FD63283F009BB2427692B0A37DFE3297573F087D94A6F4F508460DBB406529
5ADEBFC26BBA70AFFA1B6119F00151A5B83E986299AB3E5717D31C85AEC13E488C874
FFA7D30418C6F99F25BD81B45265E934EF9C47C601803442FA0987E8BFBBFC049891C
4808CC2448D1958E89AF62E1ACD8C14CAF5A7BD837ADA853E34A09CA9A22856ABF93B
0039A1C7AD9B45C710F318DFD73E4EFD4B05233B52D361D1948DBA543DFC63773405E
123C7853152E35C8EF859C345260290039420CC19F9106C2736532F713D7242815C29
7202FA11A7AA5F5274F98ECAA3B42390A45072A5A5487CB67E294F9D3E05604690D93
C600FEDEFC5F31790284C3C052885AC010C73530D1624A290B5E3C9FE02D6F45065D5
41E53D29B99C9298674EDBD654FB2492A1D988D5F4ADBBE320596135754C3F4486F24
97B7E1D33D96D8061765B0188D5D547C137BEF68668987181F3AA4C2A16F68C158688
BC87746B2826A8007EBDE4F6911960C105FD4051E9D2AFB66A00902DDBC3CD8677C98
433C1B71A1DDB80C8372D765667DDEBD3109F25A47B1309B86DB739D331B5476BB91A
6FB6BDE146F519682E34DC9A383F76FA504347A27507B541F554A796943C2B416943C
C6F62C2401DBFA2123FED28FAC9BA4EDDD48A973A9F2BE37113BDE5C87152F7D1B34B
547B3794C68B1FB0B1C739FCBA061EFD5C64A694C233B10D9A2683EAC81579B2D2540
963DCF78B3F57A8C8B986810FAF0986231D96CDD6DA93EBCC45621D50B4A788D3E0A5
D01C0ADFFDB781AB805B114D50D05B7268219B716EAABA87A9371F15125358EF3AE98
AE77D4B33D203279D795281EF60A5C7D9504B451566D44D4790E337229E5E6BA47E16
0834DD3A231D75C579226ACB3C2C5CFCACF6EB9E1514C1FBE97946405DC45BEB4A225
FA588A4CF353E39D295B56BF63318279EA53B695AB1EB4030B823A7F0A5535500FF06
A55A29A170BBD4D38AC36DC01768C7E28FA483F486BCF5D1E5EAB2EB4275AF01558C5
ECAF67712B5CE199E0A92DD0995BBEF6CAE229BF28DAA10C5C8EC264965036FA27B0C
F8D1EFC47CF970575FCC47B845CCEFDF45B560EAB7FB909729820D56D429E3276AD7A
ED47B1138D6886DA67496EA1759F63FED9D5FD752D08A8B595075E9533EA496B5AFB2
B91112FE2B7A782E04E300766989984A6A132C6AA55DB4688C073BFADBFCC4E0B57C9
1167D82D3A43189F9E17FE71EA7F4E53A5316C0472E8BE48BB20DEFAED1A30BC538D9
A17CA27C7867FDF51241928BBF998BF92246F80183161C24FF4551E359D045A15BBA7
A8E3F0A490E042658C72DAA6D2C97AC5C8FF9A9A07AA5490745C792DAFC04A1AAF079
C3507F41E5A678FBA1DB4B45AC8760FDF0D912D5120590959EF9FE587D1FF221FEF63
A730ABD6320DBC60E9CA370E6439D1C69553675A1AF4FA60D35171C6D2164574AA870
37689E4FF74338EC598156A17E515B98B0DD6B00AC10FCEE8C2B55E1A6DA80F427F93
8E4556D85A870F5A46125B226E92C27A5207977DC15923061BC12E34FA9F56BF184BC
E03E989B5591DF5E5F1E6EDE435DEE2099BBC156D9559811F29C2A7C2064D9C0D4850
88F6E979A7BF6F958A8EA619E7956889D1103D1BA07D5200E739C7918A7CDD753506B
972DFD5653D12CFE97AC043773BEB083452DFCD885883D21AEA3B43DA7CBB9048CB05
6F147E77543FDADB521330D22D0C12249CC6D64285806CFA0FAA9B65FE29F1AC9CEEE
65D33A9124383688DB39E41873F3C31FED48586DFF1C97B62ED16E1169998FB57B78A
A49CC5FE4FF74368DA61FFBEE055606595F844CBE3DF69A59C81F52C5AF6A573146AB
6A3624FB46A3B342D7D52D683CDEF5D7A7F520B42A1A03248CB8A6BD8C60E3C3E0845
876BACFAA25DE9FC016283B81449ACDCAB599DAC69D55ECEDEEFB60236D6DC85CAE87
1248C63E5EF85C39A27D79FAAA5A43482009D44133A6081F2D6D8251BE722ACE6977F
AB638846339D51B9B7C0E1789A32B22C166323B2456270A44296E881A10A10DCD0A30
```

F38DB811AE0FA8A8314A3880AD6D74A4AEED0AEBC420EE628613016E0906AF9DE41F8
DDE545054E1DC0B7A18C439242D60533A3CAA6986E1422CE6538D7AA2A5339CF4357C
82A8DD60DB27E38248095F9AA3F24F73A10D99867FB1E42EF38FD0610357AFE44B320
B28C31A098F9F531E4431FB0E0D1C968810FA0B4D2881CD3976BE01908A5061AB9E8B
A7AB07381190EADC67DCEADAF33E7CBDC9DD184026234A126BE0B4F60B439361F2B31
B7CA6058CD54C3BD2F174197972

PRIVATE KEY:

D067D98F0055E2C3DEEF1076BBB755AFD065112C85C46E6C350655D9625073E94E452
8C053E720206CDB780A61AD5120C498A4CD3E60C334D8702F0F79D81418AF959CAB77
22EBDD30DF0A479E1403D337AD923E5DBCED4EE04839020F7751C075A4892AABBB0E0
01ABA95515E1B65C63C503D97E51EAFB9AC930F5A1DBCB7E9388B5EF1E75E893E1B5E
49955E7E3E4B3819DBA9EA9D23B0986F0DA2ADDFF0A310595267BCBB7A7B31AA59C5B
C5C8A53D255803C364B4A64C0301DE319BB028F336403B280556E05D66E07E3AFE5E7
816164194A3CB42972A59B0958540CED924080CDDD7BC130BFE5146A811C6231C6F0A
F30CBA106134EA0D6860B8AC8414EBD8D191EF2DC1E2CCC04515032073110F10B86E7
954CE8AFAB992666B7548954516A1797ED8F85AA5044CBD5587824512DA5D2B87368C
570EADB7809C8BE7C20B8EB88319D60EBCC2337551F101906C60E591778D7BEC07355
4DB44BA95B3BE1820399C3D6335B34510D559F01560A9E2969BB93954A2A14BECE759
2575E5B7B51195AA113DAC249030AD9BE67E49C4F7C69C1DE6D37894D6F0B22336A7F
254620896FF0108070731BDE2891631590C447BBA56C01A4ADB469A38392EF8A2B3A4
6A239CE86C03E324E95ED77366403081203 9CC7B2180F04644D7E7F06C3EE83842416
446F009DDE90B7C614E8D6FF85025925702EDAB1273D32F6ED7DA2B0DC8265E43B2BB
AE86B742E112F4DF6E37B4AF971172C39D6C42775FA211E9FFC3E9D64BF85EF5ED394
26DABC33EF9EA6D57FEE8A20A2BEC2356303C784360D358AA149B32C2BD76EA11B7B5
19EC37697766222B77D1A4B2E38BD77701DC098633FDFEBF9E69BBF8F3AD982DDB148
01C15F582EF5D8092391E6ED06EEA50DA7AB03CB9C2B44AFB038FFB73D3993E38F6F5
E22391F102805AFED79AB0D17DD0A02EF2EAC00A7DD2D6B07218E99793E49D03C0DF3
E15F784017DAE764FA230391AC06C707F099FDE596618587869AE068CAD35FE5B75AD
673227FB403AB0D3E7B2F1E4A63644D944CC90975009F53D025EC6626AA258641E7C9
D04492257EF5B3CC31723F7FA0336318C6C897D5BB5546D977E7973C1C1D2C5CC06FB
648030A608AFD8C543B628AE54FBAE554F1152A20DE67123ECBE4DD34B9AD0C8A1132
C6AD80BBAFED91061BF7436FF8DECA7BB3787FEFBEA95E1BAAFE4B181D0204036B7CF
9BFD559CFB0EF9BC88ADF61EAA4EC3DECCF5E5353B17B4A9F50E5A7669A4C87F28DC7
B5ED9690255C7C6EDBA7325006D5033CBB09712529FD06F7D2D822BE3D9F80BED86C2
27DE87CD3FFD5BBC33F2A3405DFA1D2F500834C32F13A71D55B81F495A9A34B0D3CB3
F9A8AC9A5DC94F18872621F285165FE970791743CD23B551AEB638BCF6B8D442928D7
DC5E61FEB2FE0A85AEC6E764FB8AE2FD298B23BDAE6B647C6ED0E89370D1E88158D47
19E3D2DED3429FE4149F88B22BEC9DE87F0B4B6794C554E340987852D9D15192A6B62
D12AB3AD3C4F21E26EB2264A0340DA5FA0B938FE4086CDDE267018FE17664004F3C90
33D738E28AB4AB6C5556C5A3F6D24D8A10320009947AE3A83A75D67FE747EEBD5E4D3
ECA912EBF11E3C479D2819E91B839E8782420298142D3B036340CE83F9A7E557BAB2F
FB56B14F73DBE9F60C2E7084E68C27F28CEA24D65C5C352B2E201ADBA18D8D7AC84DB
ADECAAEE158209D0ED1C0763B8CB2C89BDFDB23AC5153F749F62BA1111909098FED35
165D7FC220A2CA516DD3BEDAE35897B346FE945BDBBD63FC21037D087EFDCF62CEAE7
A9265B4B78FFAA1667723B338971955803C3CFE4F5575A43E3F712EE94E8098AD942A
D21BD984DAA85254D0DF3D71A5A47E6477D94407111A494E56CBB5875E0AD4C5E2B57

CB98FE2D56162FC95230BCE39F17E64E22BA1DFC36E46E3243C000019CC529266F544
91F0C193C254BA08A551C309545185B4A7DABA70B175B9A3E79A5FA0A71D80312992B
9BA5274C4BCB122C9B4BF21458688FE202448883F3E41A1B9E5E57BA202AE396B75CA
97BB2276A5947BE974026E17AC0111BDD327C200934C629104D0AB074342B1131CB48
C0CB392A45BCA625FBD7E1EE74A3E793560B8B6EF51A19573FF870057F19FFC7B1CED
89789F3468AF8EF844F97B0178AC9277CAF93CDDD1A205BE37C10FDCD1F63C17A73F5
A1DC63D9AF49BBE86F252BC67AA7BF77492954616B880D725C290333C0C767C5B9FE4
B97BD8CA3809872F5E8973C85AAC29893D79805642062E96F2C774F36B4AC84C102AD
132B2E12F87861CFA9E1B68F522FC1C0AF33281B65DAD424A88811B632AEF79A833B6
E54D2BFE384E7D482230ECE00F41E3ECF0C97F5487230D4B7EF3D4D35AA44030DC7C7
EE67CD8E4EDE9DFA9C4306321821C756215FDA71A1088FE535E40F3BD65426EA70306
19528D36021EC1833E54E58F7A8A96169A4D15F7FFBB1EF6BC5174995DE39A0EBEE21
AADE54BEF0904E23E25EA92CB7FDB70B04FEECF664009DA427434207601B25FD1A3B1
051ABEE3DC63C80BE49746044B853BB9613C4A36088E002EFAA2935644E8E5B6AE7C4
AA2CE2E632A7376C03F6238E57F315DF7C964CB794DFC56CE4AF22983FDB33E94E201
FB7D420F4D43CA96AD753336AC2E7E282E16F27E8FB2012D5A4B917C1A28E9D53CB56
80BD96E3A4B59DC7A2C4E1B9B6B77FDBAAA25C2D7E192075B7091B6004BB10AF7E532
57830EB00E232B553973C373D3FA2617F2A134A9EA9347B227BDD2321FE257687D26D
85633C11F358EC6E217089B90296AE7C0CB427D4E0DA00A611E61826A45F5891F93EA
BE1535C1CB768F972AA46F11A011B20BA577B9272C8F07737A3622CA3401E84C12B8D
5399C8A8A098660F9D605056D334EC2B2623333C834A166BE4DF70A8429034AA095E8
C9935D2726A1E922044ECD194E5C6ADED997235FF553AF755214561E5C43CF1C7804F
C5D07FC5884F1561238E608ADC870964FA32F3D76F9D8C634FB5FA83733773510ED2B
A96C4413A3195DC5671A6908AFF9AA3A4B28B6683185E9E16FB31A39285E855C9FB03
36307880FE7F90B912BF1C587545A1316F72151B25B19FBE8626ED8700C90601C9448
462F9DB9F7FD3B25A4718E0775E5434B36A82C71CF0F201A6D8C88CB07B3E89075F00
7488177C0A559C5B45B782DB8976E1EEEAC2C5C4B4F68EA556F59D9B04E45237433D8
724B25D23AECA9E7AE256AE92CAEADAC76201DE1D4A405A560FA7158B8A6D4AC75825
55DC9E9B3DA5BC46954F1B2D2CFF00758E3296886E215DD57BFBBD0F31A6E561AD0FE
CFCDE77A767D2AE8AF6A97C5F53AAF3F3CF89D92

R_(shared,3):

49822BEB0E22D400F0B8958523570C3596A55A943BC8C4865522E9975E320165D49DE
35DC38E373C3945CEC4C0290CC406240564F09D8E7199B0A80DDEE2026DDEA6B1BF76
2A74511776636AA9AEE2D7BB53562B9F7FCDBFA6462CC2C56542810BCE86C27F5464B
0A95B49E6CC858212D6DE109E772C24C6B5E292361B077F421E44939F5E7BAE6617DA
CF4E6D1FD3EDA7037FBD06DA405AB5C581567DA2230E3E7047534F08D6A77A332D746
8CF1D44AAE6AAEF6F4F26C25B30ED03A7E79DA829A9A955B95B59DA7D24C4E986D2EC
B0E74B538DAB297133873E12613C779F298C4F5E44465C020F5BBA16AC98C2CC2B006
DD21F7F09

M_(shared,3):

```
18370C1B003057380064A8870431AADC02E1451C00057300BD03526CD13BD800666F0
100B652611508A259A20BADB400AB05AE7200B70C09091100A2A38C002DA501215C6E
181B021D1A531239103C000807B33A1409A20F2D24A80901B5011B69AFA2AE010BC73
E1C25A40436AF573CC8AB09E70A2FA3A45A076B0212093B0165AF5C150004013BDB81
09003D1A4ABAB41E5F36125056000B17983DA5AB3A9A00BD01602100A24F0022491A2
A3003C31B033B3D235602A50000002D1424AD5176A30099A412375C0602751E0AA5AC
37004836517EBEA7317E361E13B50100243F2DEA1539906DA861BD00660200CF14275
127891A09

CIPHER TEXT:

C037A09B4A3989195084667A2FF2D5DAA9BA75371AF45E3B4943F618E5DE9EFFB78A8
F2EFA0D59265CDE4D33FD7789A3EAF75CB7D35FB24A35DC2792EAF5C4F645701E17C7
03FAAE562A22B94BB1888DA45768808BD2A970049423DB188FBF96B350C38716AE8BA
6064798F1EA0AFA3CFF8BBA97E05D6555F0C36824A3174B35F607AE090FEFBE0C8590
B40937E2670F38E5BC040A0A6639FC0AA02EBE8719DCE5F1581BE9579FA2270D2BD8C
F9B81AB93DC80094BDECFE613A7524D21127DB10A08B77E42CE2B9D6D95BE0D31C6D8
C3010AEAEC0EDC7D47820BBD2430A5DF9CD6248A090136243FA3BEE2F02CF70AA5F0C
305C2279501B880BC8FDF2A0C149A6CF6FC7D7C8BDAA5143AF85A00F2E31AC5B23357
592297378F5EA4E093F14D36AAE6B0B5A036E22212FA6969BFB95175F68D093EAE0B6
3BCCC85134715A2D2EEC55903DA807B87F7CA53575F89E9CFC4F2BC19D13C72E133BE
E1893FF86323D3477A0F4BA4E92E5C68A795F6BF36750B3DD9E8C6DA3949415BABCD7
F037317DCB73034706FA3EE7711E3CD1B4893655B26E884B767727FA691224C5873C5
5942D4B8E447A1AC021DABA8C0A0574F25352E5CC845996F74BED2CAC8D202DA02646
180943D5B8DA2166F01B98B72C2081562E8268B3A64156C41C917129193C5EA7EAB36
4FA111A1C714DD1E3E5015320B7FF773DB842B3757FBE8402E8C043BD1A8C712F1ED6
16C4B765025D7C892975FE9C78A0B822ECC7EE130346531603A73F7F06059CC213A8D
1A9F0AC74F44D3180593C1DA0CB26E445DB8E6804F19988BE8BB9C10A6621B76DC6AE
055F2877C291A145C8206EDF355AAC6C614D90D4F1C7FA4323CC882D82F0942552025
CAC94A7825E41159421349E11822144ACDB501808E3455346ACE4DA88F0B47BFF5F29
D96CF55F91E05FFC021ACD2854E27ED29C5BA5F226663C16C525E99D202CD4B0EA449
FF9069599DBEDDB5BCEDD0458FBDCB37F6E40F0673296175B882DDDE724980A6D80F4
8E69165EF1D2BE0B8415234A10FF572CBDD3E2867CFDB6755F5083C92D6C9FC4A3B8E
D80D13A872947FD08FD540BD499EB497A8188552C82A7E57F306C1D12BB26E40FF3EB
9C2ADE63B0AEEDB9FCDD587A3263F061A316C3A3747567F19EBF65E907EBB2EC69751
08D35133DD8551CA109C83C92CDBA4C8B0BD3F314A2B20106A36C42FA206CB6CCD08E
45867B0D760A35D50EFCA8FB5EE7A5800945E3C6DD4BA6501C227ECC09E1BCA943A95
A257F2E2C08A9E7BF1CAC3BC3EAF1D7A9B0E5FDB69EB367FF5EAF124F25D6E9890C5F
BD673F61B4692A13577C11DB2B6B42935D1D1815E235E14859A3EF7C4F9D8019E961B
B4A464192AF77B1B34B232F65066E4FF041F20E569A9B3E6C189696D8B78EAB1F088B
592285C8711156EAE4956501D8567251EFA96B9B76AE759C283647F8993E1027D65CE
106246688CAD4B348666907129C0A5DE4BC951D0F1CF964B3834076FC2D02FCAC9412
EB0036515EAB393974B6AAACEC6A1D5E427F503ECA3996DF393B83598B87EE7F4B764
AD88CC2CFBD66900D00289F303AD1492D70DA4CF4E4EAE8CB92B28F320DC5A78E7ABC
82254810FFFC78CB0B267E468C8ACE7F0733497889B5114CE39A1DADC52C556557FE3
45CE3C523DDC7061BA6443CFD5153675FC24E333A1B45CC7C1F6C7DE4CD6B406E8E5A
5E43817A660E61CAF30C19F6E0A6DD6F8F41FED2D70D58157E1505F5FA6267FBE56B5
F0704B80DE3E71B17C209DC5E3550F1A52FB7EA1D6F6C95FEAFB557A182CD0E877B40
```

276F58C48B3E630B3459315E9BFECEF4744D16F94AB70A316F4095E6F95F4DC44B5A2
5AD281A5465A9B1FD765289360999FEC84EFEEBBB2181313C492E71EEEC3D435C9AF9
43815ADD38714EB051B014C47526C836772E054B87DEEFB4D38599184EA48ACAE252E
277DC987196DD23896C36EC2B86C872BD76C9DCEF428DF90D14880F56F9E449A96F26
59DFCEF65BD2595020AF81177BED602357F70BC50E90FFEB6A2A3E884EF95F1695F4E
747D45FB45DC5FBC9A2A7E6C6480B9432B1374B371F1A373B566D342022623436F078
D31F1CF0F9EB50086C980698C137C2A39B5F253A3D2C645131E4A586603E3CA027E1D
F78BD9C0A47863769D9EF8C9493A68FAB8412A173075FE3627AD39579C514FCD1883D
43DDCCFE5DE88B7F94C0BA8DB1FAA2547AA65B4788CE094546B75E35D0283A3B6B1DB
F1112C6974BA256540C615A38781BBE7006A3A0F99D15AA01AEA19F19E5B4340B221C
8130BC5506A0D2EE77E84BAC264FB162F5BEF0577CCBE4C1BDFA565DF8BCA9CB63D91
38BB9FD46538621AB16661630D39AB984ABC2E99DE71AC8481BDC079470B9BB71BD33
3223645470142476 0AAECF03317DD443BAF04EE9E9F22B64733B5DBA145B038F3CE8
16C145411AFA8F3D93301863E5EA13ADBB4C34312718ED48B0C61FCB5D6274364C4F6
5DF54877B0B589D975A1239CFD98FA48DCD7C5FC2F7E1B0D7643C11C4912129AB350C
3DF28B596F0FDCCF3F59B3A3988FA25A34ED15B18B29BFF1DC676A4A1D6FB36BA6452
3C2F0BD3B19C1F8CE311000901F

SECRET STRING:

DDC673F68DCADF8BD205E6018D809E6A194B31723DC866D8FF3DD014180862B2

---TEST 2

PUBLIC KEY:

B494D9E8233ACD632D7A600341EA61CED92195CE82DF5B9C2B646DE86DF506B18CAC7
3AE6811D159E3332F6446D04FFCD54E8EAEC1F5848F61A8DDB33DF888AC80968F00D6
F4769F9800A55D3CD7FC89D42D0444A8FB5E8C2EDE1BC864932FEBB2ADB2D39EF9298
2218F48D429B1FB71C0E8485EFC4824BC1B5D06C1C43DBD8BAF56F74F5F40F4A04EA2
12A7423598FA45CEF5F327A76CB136C30EF87F3A35ADAC7F3E4D745E658EB9526C321
7B7EC32651687C09CAE493393A1A863F76B4C557B1EBC35FF3180D17EBC4558BED6E1
1F5F81E8DA96B8513BBC4348790E7049EEDC20D8300CF45B4962E511DA3EA48AD876D
0C298043F356DEFCBE9FCF26E07C764915992A1F7713697549B05B6A94D47EC374164
96F800798306127E2DE75585F672F0ED66B84DE40F53E18B6F083037CFBD471034770
7BFC3B3E4B02C8DF7348DD050324BF2362B6E2375C0080BFE9B3E8D661E8EA17A51DE
D6F779E0730EC6907B33054620239A3031CCBD197335F480D6DBD7ED14478C19D55A4
A6B6529ADA1AE524D95B61F08CC47D345A81559122993465DC6A1A14F487AB4756F33
834EA4AB494DF5841CEC908C7FE150F1451C2222C2B8528B0B5EE4B6D9320D8F8A1A2
2DBC5E5ADCB01E39E53E4D4C36E32D0C107117D2F48861A736D26D8125A1B851E7FEE
F62DF94EC79A90198E0BFCF3699665CE418483B1EC295D56D023508E1F9BCCCA756E9
D59B62D6F4EACA9BB9BFA0B46B027D5C62B445991A0BAE48A13992792386203E1A47F
F819851769C8A62F7A9DF4BCCEC42A9359D18590980371644ABC33A649194642D6F30
411F32153970F23386C68179367A693DEBB3D50C9214FCBEC968D176A0799F70B131A
421A17F97BDEBB1E866BDE3746E0303ADB176245B2AC4E2D8B37C41CCF328F0459213
8EC3B1E24FBA8265793055F5E16E9713E3F31CACC802BE0815E3A75EA8B09B221B1BF
21217CB304ACCD2A3627CC1BD00A63028B4F322D82BFCF7054A21E8A6BBF792646474
7B2DDCD91FE439CE39497366E97106525787D2ECD90317D2D5A1D0B934C5BC987FD8E

DC21C90E3F61CD7754C1807C46AC8A0208BFC329E49A78B12AB6A30DF65A2D830286A
0F95B86FC2E90EA02CC11234C2564ECCE8E925A5AC6574FA3508638702905295CF2E6
361E84A62DE94208EC6629738A7164C6E09CCA74AB2F182C3B9D1490C637D26AA5B58
3F831E3876CE2789C1F63D2DC82DF03ED2B75EDB2518C086E05256E3B13F516634227
FE21E706D160A2FD015EBD367A08BB32B7FAA11FAE5A8BE71557B731DF2AB1E86A919
2DB93F067C2396299ABA2C3EDA131D43038BA8E4FE9377EB3D3B255641F0EE8F1DF75
67330FA36ABDB2AF5A75A1FA54F18D783C229154444E67175400D214D51992A9C6E7A
C54FDCA8C5C4DC5FF8C9541F1CC9A1E8A525CC3605799057705838AB7417D97FD20CE
4A0142EBCAA0E8D1248A29EC1F7B107184416E913FCF9B1509A562CA9AD6B408AC9A3
74FD801D83F8A5931277C8CBFD86CB9DD6F8E096A1745C8C90120EFD78115DD4BFC03
055BC261F0750BFB101922936C81970CDE5B14B5519B4DABDB47613925D169A31D3D5
4BC0B292136D08F0AF13B77C8760D891E9761339C9D857448A4B63FE15D5E9357F872
FB792AC015FCFE6241E7C0CC8CB926CD15878586C2016FD50EFFE198F43FCF70341FB
263889E29A4844124C4E374CD713DD4A48EAFADBF2D3DCF1F4FD93D117183A2FA5C04
44A7044F790C0F131A5AB3A7EC69ADACE9E942DB0212BFEE598D017BC9B1E59CBCAD7
F80BC00979E34A3C138BFDDB822203232146893B99461FE2BC5D2758E691FE33FFD7C
F148E114566E2729B58995DD068551E5854F7E446098CEC4DE27B48A8C3549559AB86
4CA65F2A284885BB75952ED2BD176EC26AB9B2BFABF697AC09D635EB194AE063614F6
C59FF8A7A3A825982579F82DB552F98B33B0C0E685F5DAEB969C48A5304F7270947B0
C69E54EAA12A2E31C387E1E9B8379DF368682DCE63CD4EB84E13741ACD8D5DBEA9EE9
0D19C3094D4E6CCE825600A32D1D5DEE438731BFB91448028EC708CE93F38E17A78D8
91E06D337A05DC851C5614245E57377850F1116680A484BCA793822DD567DC55337CF
667419BFA563D975F71FB1A5E4A10B5D8352B427D85DF3321DBAF0DCE02716DC3AA3D
F613E92DC88B7792FD54CB05BA4105A27749742692435D5E4C3D24510626B86145054
A60FB38E9F6E67A6E9D6350DFB13FDB5D0A81945945D5236064372E75DC10ED55D8C9
C38D2EE24E65BD8D870228DC86093676CFDF868F3196C8B9F65DFD56ED02D6CB449FE
6B75071E9B95A8DB985540568C7772F64BF3548FF715BE03AB97ED3F1A650B1A951F4
D0E1D89FF282EB43141606CB737A31CE37959D92B5CB1C098CC312E3E82D0BDFF8E69
07F94EEA567F5AA4E626B496AFC9E569E32A952AD8687E2D0944BA056F12E4D0C8BAD
72C2FF747F8D694FE174D04BE2E30E465EB465CF6BDF4CFE8D3E7593EE2C36D1DA7BC
229E2F37F6A6FADD4D814012034369E390DDCEB4CD7181EC08055F65D964E2723DCA5
0FAA66D56C022CB9380F3906406

PRIVATE KEY:

22627B1EDC147AC45554273783748C64731652DB85D80C6FD5223F06D733D038B0075
B54052C7342624D879B3BD998A7E2B51682ACDD0B81C876E91BD14C969795E044286F
88265EAE3C7774ABBEE08B4646109FE0A5E51C8B02DF6D91AD559EB3A2033B144772D
B2AEFC6AE78B31EF11F71C4856690DCE82E653FC01E439134D76B9FD5E07DECE48453
78E2430A2D3A50EF44D7D7E57302CB48F09F9625072524497C846357892503CABCCDC
6C550E773C20AA78525940D4E405EED1F64CEAB917882C934302CAB3D456999BBA518
07EC70769E8587B527DAC11D26D6222F8E4F9B6D0A80A85214E71027716830DCAA1A1
4C28F5509638BBB8C4FDE0CE42BB28D8B667E1FE87D1A85BE8D55097E3BDD6BA0BB7A
E320EAAE2C342713A3453572B7C60DA966ABDBDAAE7AAEF0467A9B9A58C39CAC7D77A
8EF7F8803B05D604B74E53AB1ABC4C86230CF49BB4266328B6423DEB9DCC9CE784E47
5DC5B3EC2EE520E57D53C7138657175606A1685406C73803CE6F6A413ABF597E2366E
71C5D9F9A2313B15358CFF26C09178910EA58111C938C4E3D12CF9255758643E18679
B930157325AA8A12A9C17ED22B06B1563E060F69839452F256C24EBCDC82997A48B59

```
E2ECBC76428CE1E01A3B7EF9B968EC6326E3DA768C9D035807D14E1A5645FC79B4652
BF844FA37734664D1A5505D0233EC92C71DE51EAEFCC099444CC23C8F5F9F8744C1DA
DF30B9F09202911866F84AF92BCAED5C4FBE8F54F6C0906E41CF438DCE281EF315CC3
ECFDC14DE18CA81BE1548363D151D3E60C31A4B38FA226CCB7617A7C67BCB7C792551
F32B6BFB5EFAB7A75C3F563E5726358FE84D4F95BEF3B047DCC90D2883D49747D1E36
C6F84047540C083534A32E7DA85A36DD8800E539FF05D704A152D3AFFCAAE886191B0
A889C28A0D53196177847485C33FB83C8EDFB1F921B04C432BD3ED6EA27A9C17B3D2A
8F708C35594207B28E7AE14725AE16EED9209E231A5D7811A731CFA0E57498FCA4B68
3FE7F5A8646D667055F0445C2117CD98FA90385BF50A2C70168586592F73A894EBC31
7317356BC98F1AC914C8CA5DBB85D5619634861DF9721D0D7E0691DA262E323F57EC3
BDF93A4688A8CE4C2C8F3B381458EED85D4102AC253C29440C855C37F403EC92526C8
98C0485ADE67C2032E1C19CB77C36AD51BB71681A5196B66DF571454C9DAF901A8231
1040FB495A5C3ECC9FE5C3A3795C00561EBAE2A9755AF21DFA30AD507BF55142738F2
F0F62F987F4F2B5698A5A404060A51F3A7B624F6C974C358A39F94B7F9148C907EF62
8B570CA873BDDDA161580C9D2F9869C314A116921B03599DF5E6BBCB376DA9562A6B5
7BC5DAE63EE29565F7E877FFA6AB0B34F1B0916C18BA2DC30F0F2DDAB842E2837CEAB
8A2D0DAFE65F47EB0C1B3EAF7EFDC5F24908A1D2165111EE3115537C312ED4A324F44
33BE80588FF322BD1D6E4917BFC512F7EF420F78B4D5B6EE30363968AFA5910EE0193
5BDD20F7EF639D662B95893240EF16871D551E94D0936B227AD9F3EB587234A671858
72FFD174F7A09B74B9E047D4DB45868FA1BB1B6BB63674BDB2996B4D1525A9F782A68
55DE447A53B680D3089988DAB0DD507EB102EF6F3975D238AC79172C2222DC79B50A8
00635058BEBE66D5052B4BF72507295E31BDC7A80AB84A2028CEB2AF6C6940D211E1D
4E54841D06A0462569F60AA6A53D32973750564251B9F08EE601FC481F88D45253FF8
04E1C9191C867FA9834D68CC65DF7AC34D4FC1EE5574157534E8B62C5B1D33CDB92FC
0518A89DCCABED978DD22BC17B429C523DB70BA538603F8F5BAF47D36682A5BE84500
61734690F95AAB6E677F7C0A381DF491A56B8E2CE3CE84CC6E4214432D40E6A5DC7B0
05A8FC81F447F8243872388D24CEEB40012BA2703F80318634B925A9AE4691FC71B31
3DC152BAC0C4A7F488645EFECFB92FB7DB38FF6B97972FB2E33D25A306283E339170B
0DE6D90A24A33660A9B63F4291AF9AF8287FEF16AC9F1756CE9F73F05BB6E6127CB5A
8D92E562FB387BE7B38827107DF300D751C8FA276D25A12F4D638B08E5A2542D17D28
5A204F6F29CDDAEDD4ADA56F6C035C4B5AF6811D4D83DEFA09E514B6F131D433B116B
271E15FE0DA26B8E370793C486821EE28AC8831DAA1245E422FE16A709518FD0194DE
5150ADE844EC990BC9E34E9463C7B349A4505F8236930EF1A6E291E5A5F6FCF6654B4
B08EB7F35EBB477D7E599E5629DF59FB74FE7F4C53520FCF5F2B9FEF22E37563DDF52
133B7F999846A10A34BF9C2FD7B6E42B8B68873231388F5C3D1FE8916C5559E5EFFD3
C8B59B50A9AA74538AC567728C36732A6F319EB5C5D0D11FF5F4600F3E1055DB66849
9898C7C796572A1DFF85A1FB03B6CA868DDD726262C72ECCCA3416B676F6832212452
8451FEDDDC1E8DC26834F5C772D31F3889F28608150A93F8F54CD0FB9C50A67D73CFA
DEB2A5C9B91DAF545CF61228C18C76DD6DD4BBE953DF17882FB3B2F929F5BBF4044B1
D806AD44D2A7B9CC49F600C7675F1E3CD2506BFA95CC86547EC40F0AD3C8B60B2F155
B3913DBAEEF8ED7FA4C6E8046F23F1A70262AF46E0B6700BED89FC93E3C2DD813B72E
602B8A18A1FA7C9EA837EDE9B1C3A7CFCF0171A52949E47DCC3EAA629E312EF56CFFA
ACBB2929212FF25C1D1B7433473720B6B515FABD57E9F4233A99A4D199004E2626A3F
633A23E47C624912ECFFBC7118E61132B70601D475370C20546913DBC69D6B92CB12A
A5D5EE8C04E24DCC001CEA06D28C6AC84DB7DF05BA48BE6D6D41B4D99C58F8A8BEA1A
6DBF88CF7BAEFB5081EF1D931D8AB773A3CA1D8C8CF9BB3A2E2676B9436A47DB4D777
F128BBF32B59DE0352C6D5D473E2E4B522D888A01D8533BB4414615938F96941CCD7F
989C53ED1D974E4CFBC7EC575EF1E2F8617D86B0358C91F912451A3183C905A54AA2E
```

28BA8D23DB2504CA852B09955E63F4C213C7E4A6D4FF8AB59C1BE8F3DF57221AFBD75
CC0B7437C2ACD17EE4130C2C279FFCD00C0EBA9165BC3C6332FE4ECB6AEC0509AB6D7
3CC83C78E51974ADDC0D73CB72F70C8CAEA1562D6F0F03EDC7CD2977612622B685221
CBCF4E059D494181D1976E5E485291B0F0EF051571643D0D5EE310589C97E8FCCDC3D
34FD2B8365A55F20B67522BFB76175B51AAD5A35D98ADFC42B7106E21422C60720CB9
12B6A3E6187769E0F074B6F48E33877A73F5C2D3EA15AE01146B74FD3A6931DD7CC62
92927082B876355C07FE6670F4C9F62A6969E16C4EC584BF459988989BF6BFAE0CBA5
90B416A08E917E89B8C0B3D8433CFF5B951F9F7C

R_(shared,3):

AD1F9698E77C196437D43A26546A1C3D05BD4A093CCE23722A873B8EBEA79F066AC6A
493A4C4854DDC8DEE02BE112B342CE617B77FC489E054A673CD6E3C7D56EF7E2A88DF
C840A2E489253AA2A672440C64548A8938A226BA0604A0DC54A88A04553E6B4E87A80
A0F75CB256941DAC9E56D418ED2CE3CC1BFA3B4383FE92C50AD69A21AB0EF6E693176
79B28C4D9036D32B257D11A92F5330B8A4B2864CCF9AB73815F11C4A4141B4B38B2C2
15E559D464F5ABBB83C5B5FACC2EF47DCA6B2EEE8AEBA1F145ED5A6E5833BB4C6BC68
D728988DB17FBE9762DF9D35F178152354C710CFED0818E74E05BE8634949F501BE2E
68B1AC204

M_(shared,3):

070F3748A25188321E1B418DC60603B31F530348A96E123FA8BD10090A195354000A1
DABA3300913530251038 91E631BDEB60202845C0A4AA5871B0345073C18BABE110836
5212A30002A21B0012A7370C123DA4AC53353F012D5400E36A03026665CF1C03B0065
B12A212A47609011BA203000100620052670 03C3C080E540312150D0D025425080F06
88195413438D3F142B380F3CA821192A9739A40612C62402CB3C5A172D60757E09018
81B2F09AAAA1BB4BDCEBE511548A5440403B50087516FA91B0000B02A0A01A3036F10
A8A8662DEB00125374DEC3B4AA7EA200DD8745A5300942D80CD1066C02263F41A2023
40937AB0A

CIPHER TEXT:

69811D8CFEE0C7EDF013AE0069108B476C85D0959DAF2B9757B3FBCA3378C959447E5
3AF45475BB11234851F70B99DEA79621603AC063CFFF5246D71AAFA8DFB424EBB2245
A10F96CC5D9A7EEBD9C62C9BA2CAE1FAA1478DE703D503AB9EA9FB8518174360B1062
2A270305E355AF4A66F51913C46AD8AD2C9DD9384E7E0898E7E91579E671DB8CD4C5E
B146EBB29615A6D7B233C99A2529562E5DE70CB9ADE6E403F012E26025DE36B55B844
6AE42F1A908BEDE25AAF53754ECAC650E190624850FC4AB05AC68EE0530F96F667195
76D13CCBBE1927D81D2CA3597187B72814C75F53E28EBB2E17B26A4F04C88DE0DA7D2
41CAE9970D978B81BFC43980EBEDF3B40EA865F7243012738D9835F4EAC5F88136479
3F983BC6590F652C15720B44FD015D585BF9EA167842438EBEC89A018E1503BBDFF23
2D06C604DE9B08CB8A6FD6F5A5E78D032E051C2BE47A57EF2E000D041A713AF9EFCD6
019481511994A869ED4477CE3D53F0CF94B67C5C08B53D569ADB0A42FC958AED6D8E7
EE489B43237EE861739B46D418CEA3AF5B91C0C585AE61C9D9C34DE086FF37263E2EA
BC796109569A280DC8B97ACC92190F36DB38AE73F89C951FCF06CF242FF23576392D6
F37F57DDE550539A93EF3C97B4A31BE79CDF521C27EC05FE3C8CA84D42C88D2AFAD58
DD1567A27CE3EC19F11DC941DE9444849DA696970EA982139A3A71BD424D5A28644CE

2FCC83F691113CE4E24E2FFB44C0AA47EBFAA876E8E923E6CBB1CC74042AF9325EBEE
48BFA4343A75A64EC1717B2969B1DD9290E9462F99358625DAEA318D255A5B03CC003
7851F461B41E9163644445620BACFD2746AB70EB0D2EDC52807CA92C43F412747ADC2
198900954903AEB72584AA8150C4047EAD1460646B750D008DFA4F3BC8A537954F7B9
230EBD7922174348697F945C19A5D23BB76B96D865F679A199F8C4477288A6E85B9A5
E4B52CC65FD9AFE78D6D9B4FEE2B7FE9364EF441DC4C6F45089E917A62CE6E770327A
C05D7949E1D856973E84F57B3723CB13AFA541551FFCE69381A4396AEA934C120A525
36EE410872B8DB0983A627FD4B9D85D479286E71DE3FAD60F2E9362776BA7B32507CC
4B8DAEB932F72D7B21758597ECAC79B0DCD051284AAFAD731B7FC5875D8AD5A972084
83BFB2180357B8F57FCBCFE87EA1CFDB9440A67B72B1F1F9A2BFEC1971B405EA84B6F
B0FAB58B0826CAAD718E49533E0A4197242F2FDAE7166D4E3363F21386CE728AE3FCE
33CB2F427D3B9AE5E5921310A8B4684BCE5810E6087857728C7EC75CAEABA43F38042
FA6C37376E4F5097CB1E699928569ED2B3E26861BBEFED6A9CAA25BBA2C12ECDD287D
522D507D51AEF9B3C7B99E2FAD9F22061CF67EC731A4CD26E887380E27D64D61350E4
E9CAA061DB2B6EDD65BC01B2DF657772EF38FFB6C82B8A6B97B0C3F14437CCA0D1F85
96CA177A9E81793744DBBDC31F8AA9B58699392B031A8E3571CE26BE20B8D2FFCD7AE
5913892A2485CDE116C73ED9C0C4451C3A60D89407362D219A48665D288C618A41258
F29CE2D7CD45C0AA41BD2036197422826999E8C55CD74EFD9B1A674856C6C334A6F75
24BFD72444F25B3FAE45C3C8B37F7D5AE85313556A4E6A69AE1C0EE90A105E4964A19
2C8A7FC2BBC9AC0E8C2E413E77596154E74DE4E0FFAD913F9C43C7E53B151B71EF20F
42EF32311E4924BD7388C9C31E01499C23B38FE6F6DDC5E9D1031AB968252BFF02A35
A524AA444094BD9BA43EAAE731B8CE714047EEBAB1CF061811A81E310FF4C9A338389
CA401A8AB21F95E212B34014C8A2EAC82BFE0A33FE7AB631CB9CF35B0FEBDE914EEA4
166C80D30B74D4A83F109AA036343695D6E9DCEB5B5DB002BE2BDD719026924E084F3
AA9409BCF98550C872F7BBE0A2C0A0F888008B12C49EE4DDB4EF8859B1523ACF8EA44
029D3B2288E8CE75381474C18DC5FAE6CCBEADAB5B8B0AA91E819A8C5137EB22CE6F2
5A2EDBF64AC7A97916ED0C66374770CDEE90256E8BB7347B1914555EDDC19BF0F9A4E
8B94AB0021299719C2C7A015F23A79CF9E1812424421C647A5899309C216A8B693BC9
4606F645A3E59C4E4A08B95A986AB773645B9590AA2F9C812CFB19DB4D5EBD570552F
F16D0B5BAA8836BE91CFA5BC9CD81F01254CC2F6A768B2ED558677FEE174FCFA2DB3B
FA485327185709863ECDF22F1B97E3551573AE2563562343705918 21B2CF06C31ABFE
14A1F42AE6A1891AB4DA4CB9A7049AE64AFA2A2E9571CF673CA3035FC7F5B1E32A2EA
93553D2543F7AD2F6224E63F2AFE6AE1EAC0CA855C0391617828F40393DD45F7DB0C0
A8626A9F9E8A077A5D57FDAC3B5A56849200C9959C6FEAF3A3CBF2DF96412C29DF57E
4FA048EF1ACFF03A011DA2EB66B4C8690C45B889BF71E697355A471F3A55DB79BB8D9
F3083ABA985CCDA0E836F663299B2194E8370D314800A167A9C98E57B682F59EDE6E1
203072F11754AD09546D8A614E4B51FFB1229549122E33142DCD8256FA1337EDB8DEE
954CAE5EC93AA41B7CA44426C04BB28B0237C1252692F3BF1A47510DF6902A7874AF1
FC8BF35C6D2769930ACE7A378D2

SECRET STRING:

2DEA93DA4E1DDF214CDBA801525D560D6FC2679B0666D6E9D5CC4F1A154A6DE2

## 9.4. Test Vectors for ntruhrss701

---TEST 1

PUBLIC KEY:

54050CF5C4E5AAB6CD62C2EBD092AEF03A2FE5521BDF836E5197F23F22F1925BC3BD6
C35413983E77DB48A80CB52AC9403F72AE8B10B66CBEEF480B04409B5B6C67D8EAC5D
B57F5FAE2F20914B7CB4FB6BD471B20D781863F39A71B1155E6332D3B3415A7869DAD
31CEAD13036FC03D84007B39F52507DD659D4F2A9B45C55A4B27591CACFBE7C0E5294
3AE7864C10F76681C6D31555E6F95980EF5B3E408E022ED406C4860E4B6710C286C58
67776F5EFABB4E4AF3041E841C2A32611E219868C7715D08D91AE6E30D1A0CBA8F747
12FE05FFEA26DE995DF9C03061B4592D2EFFF3846FA64B35CADA90667C879E7BD961A
EAB1103D2AE3E9D4310353435C95EB943F2A42D4A40D08C6A6DB8E5714196247CF48C
2619E9791E7BD0C33900DB4BEE1A7E3614DA0A510933BB8C5FBCC8C395F505160B67B
4B09C2D36F4430297E26B50B2E4005FC2A43B4A3924539067931B16DEBE7251D0EC27
B8825F5C19E296C53AFB4F276DB6B451A0E67A608DCBB0661B818B7DCE6EE24E7EE64
B29CE81D5F5D8A90EBA0AC2A2A14F05A79D249D5F833FC50DB577244E7F9DB1C38515
A4FA8A6176666AFFA5EED3301252CF2BB4486AABE016EDC863120622960E57276E221
FAB7A5247E91276C1063B82FC07E4DA91E52551438D1CD1FC2BA9BB7D8E73FE1FD592
D40334FA1C3F6E06DBDD56848C50B5BD7A8185FBBFE9814CE06A59EEB379657597C70
1D0BF5F0EC52928B489BB3D57204EF4D4F4769F5ED39F5B9397F5A4A179D1AF0B1146
3B91CC177A6743C7027B1EF957C36E90D8A1DFFBF55AA2C60A02EFE5B5669EEC7DC98
345D8DA3851C77E8AD37BF8F54E260E89FADB4385317EBE42DE72D4FEBB64FE40CAF5
5E2B9B4E82930FA05044129E416AC0224ADD03B4408C50501AB7F7779A461ABF17239
CE949445A3C754E7DB96E2A1AE72F7D884F9B5131D55E1F4B1CEDC05A157795E9F69D
7B86793C5B1E085DDD7DA065BF9BB22BDCAD305267AC28F510F3EBDDEA656994058D8
E7E3902C467DFA112370C37CEE77E7A130EDDC454212B38DFB4A7017240F78B23C9A9
0A2C983661FB03AF46F6D6258841E5568B4F521ACE028019296A738A1FEF595D5B167
28EC96571A14AF4FBE593B837C05E9BACA031EFD3353D0A62574F7CB7DF79418E866D
72B3D3015C0173B7EAAC996F35320716897518C9F5AC7339534192009ABF73CC11351
216D7310E118CE4B8D2FF03B49157A52FED5572DA34D1E1B6C52D942C083710A46880
D8D96AD1E1CEA6B26543C09E194BFD4D24D89F36B343BEE70ED8021C5D47A1F9A4470
62FD6966A461C3DC008CBC738015A90B0FFAA05D4AD6A5E3EDDD0A2718606E11ED808
EBE28C9FD1BAB46F3A7661CC508C5754EAEAB3941681615CDECE45FE9EB1A3E03B2C9
490C187201F267B8BC629618CBF90E91A95FA15D94484356A58F8D596DAC853B1DDE7
211F18C4986CA9DCF4CED62362C22C792CAF9ECFA8E5B786DAA81E5E9E8DCD51F9D2A
BA3EBF8E0DF1A78BFDFF7338538B39DF6FBABE0B6271E2351B92672A9476F09EDDC87
9261BC0F434DFA3BDE9046DF531FC3CBF15484FE3807E4B059EAF326578C3BBDE905

PRIVATE KEY:

D067D98F0055E2C3DEEF1076BBB755AFD065112C85C46E6C350655D9625073E94E452
8C053E720206CDB780A61AD5120C498A4CD3E60C334D8702F0F79D81418AF959CAB77
22EBDD30DF0A479E1403D337AD923E5DBCED4EE04839020F7751C075A4892AABBB0E0
01ABA95515E1B65C63C503D97E51EAFB9AC930F5A1DBCB7E9388B5EF1E75E893E1B5E
4995E90F71691C40B00352A96CB9BE2E1D94423F897DED5FD466E84CB72290014981D
E962EBF41B42BE1E8B8B7BE2EDFDB49A558A681458196D3B3950AA73F4DE4E8089BD4
E161146FD11651C955DB4661DFE0C18185EE2D7A25E24DBACA2EAD84541DAAAC3795B
B1FD2536CCEBC572EA471845B669C336F0FE7055DBF16197F5195369446789F0CAF8A
0E388FE6846E5F35B0E309F96A932F05502FDFFECB3071CF7FAD853A05B24A715CEFC
AD72E4C56EA03ED498C90873D99C3A80DA48DA2AA7024F7E4AF7DC9A6546DCD596DBC
8F5A65D564E08A119743768EF84A799DCEB49DF243212B823E5F0C8539CA9F6004F05
6123330450E25D0A1C3CD3C8A4BF331F4E5AFA770B2F795412B472D04FFAC26F1E826
E72CE336A295857A7E65EBB1077C74F36102FCEEF34552954AA831A3CA6EA4EDEE226
4DB71047FBCD42200D2E973E01A92CDD71DFCD290D4E55079A952051D6E790AA0A856
61D504113FD294C967B848D72F58DBBEE67C279347BF03DB5DEC7B0CD1D444A852EA8
31B1855E9458557E6250A9BD4CE5F297EA469732A0CDC01842A38A8F89CBB9BAD2319
A6EFA95FE472A7D87FADBD9538837B6D00CF123AAB07585E2A0A8EEC91AC7AE087592
AC737695A7CC66A1CA199622D2CCF3C46D3B53D1B4D840A5B2231B4E7680FAEF7DB87
76E02E5B496C22091D03EC07A44D9E910F591CA498BFCF02F792D03EEB55643A91768
9101161940D6B59F9943B720366E3B05549CE7D8972DF1A4F3C63251DB61084FE9365
FFEDCEB7CEDE9E277EBAA43ABE567F92C97A53452562F05F32A7EE347EA1600E0AB97
E686D0EBAF0C258EF8C7632D6CCAAA5323DAC2ED8FDD54578904931A614CD4E8D3386
C93A4160C57C2F72B42EB2D35AA287F1824DA821F90C2042255FFFD38DB3998355799
6F8677396137963FD0306B5A8702714477BB3501F7558E66DF10907CA9410C5370C2A
99075A7CB066D1AF78EE91D91DDA377B36AE2DFA265AF620436FA11332BBD61DAC032
4FB90BA58D74CE6299E29C04EBF2FE4441554537047E35B3CA436118EF28638A32A30
EC1ACEB256FC1BB84CEE8127C82A725D1E803B61956E50C4D6AE0DC53FCB5CD0685D6
6E1507BFF52FFDC8EE6D01BD2492CB44200195B26948608F1EEA7271CAF8970D49744
4EA546377270171A534AFEE05D01E05DA2DEE25049C14492B92E72B8F89EBB1E43563
0B7440226EB3E8566284065123DC025A53B8E9899E41B636554828FF8A79B41043314
C5457981A8886CE2F5B55DE20582F36CCFD5A85E439228D69B1A927516BB054F3795B
A2530941E4973F2D09DD3C73274F3AD046A1DCE4AF78EA5AA18B768368AA097E7D6DA
65475754F975038803F9832E5A9A0FC7A7F74FA30E410A89933BC124C95B31657371E
3BD6E5378B6E8866A47D3F141ED57EEF1FF5AAA64DDB7D99AE3663A5448E9A5E3F1EC
06BCD3245892D6C56CC0E76B0E7B360306EE9C127AABD143ADAA3860C42EF1AF592C9
68642C39C1DB8D3D0A030E882EFC5C30374F5CA68F19B325F88201ED3338FD8E0A0F6
1D4913C0B3CB685D75F96D55E24B9769B06EB05D17EFBB84E3F550A92FB398127214D
167E76639844D02E6CF8384007CD1B21B540D0FC37FC80D8488B3C4F28F7F77498D9E
60690B733EE47E0D5428AF4FCEFD4739333DA1E94E3B7B94F6F1E5EF8D90A7BE0F91C
379E9DF1561A34684F0F1B2EA6B1598CEB1B60C249CC88C4A115AFC06B1A3A7779E2F
6AB70930817C7AC336728423F13F919172A1D6F82D2B09A264610F3DE04F056602BC1
C377B0EB14193A1C6E6FC6DA8E709C0B3B456F996337536DF40EE5AC8571FE7C2BC7A
19

R_(shared,3):

CB7B130DAB1925412FE6025E1969C14A875804B933782D8AB23B9177EEF2869BAB652
605A9A63D023133B80A508FDCCF265095E85B92092B151FDFEC369B41E2CCDEB001EF
37A2593C2C837619225BA49B5D4707DB123DED9B7549EFF0799F512657046393713CE
FAAAE2F6DB81A50502A4199082186797C72B196E392BC081F847FA178E4DFCC3644C2
209B

M_(shared,3):

DE4C0A6867B1980796E49D6343A35D61CA710F8E6D81D34A1812BDA43B3371E86EDDC
73047D46CA5E560687B1C2D7CB110A2196B5C476F405277C0EAAAB6B4E902DA29C1B1
11729B7538B106DD22ED47A8401F61053873EE6CED69BF1FBE098D9B8E44660F464DD
639D2CC20F2BCE3E442B7672EDD66E77E11205B308FB42D2AB9D23F3AB76447AAE199
BCDB

CIPHER TEXT:

```
4FB29CE5CE753444A0B941D877305F9338ED3F4F30F5E8A0BC1F41AD9817B1528C9E8
6CCFF4E6F6BD364C1EBA2AFF7D48335E71FAC9BFE5B85E9FF19B3E60EAA3517E88913
F41CD010492B9C060D89BADFA5257B1EA77F1E32AE2C2FAEAAB587AD305FBB99961CE
88D39DBA48D8BC598EF3DC8BFECE97E67301BCE081EF8EE521EF23FE70A98834B63E0
21B4161D1A9CD003C300F2E9BEF0FDD8419153194363137F28810462D512161C82FEF
9D5C11E88250B00BF51202E02341078B40F89BBE5EA8BF0132C6EFBD75A2C27286DF1
4634425520C7BF6603A6B805D1B37490E2F15164B4D276C1B4DE297F397B480275B8E
39908A785E5B49B296473DA62270C2D0A396DB1898D190A043D042D4FD7FF4EDB9046
6861B2C590091459D022F9826316BCE8ED5A57769DB3EFB51BB2FDDC3C7882D3FC386
0C338E1664B7CCD93ACCA5EB9342DBDF10B1D9B53D39EF8917D9CDB0F222F6BB2BCB7
ED50982846F39FA486239E738E48E59081BDC46485CF64B8D3A0CD1D430D266B1E89D
AC0C00B8DE19D8A8901BC6505FCD7A384A8C04464298D9E27420C6D973177B6C00B8F
4E28DF7B6750AF0B7F6697270806DA8066479182DDBC866517AA494589A3857B63A40
04672BE2D52105282C752E0D55F1C5A29A2345BE51B391A6DD96F4BFB34EF0A6E4301
4C6F712E3B53F5F60A5025024810CBDE012C2FFB9BF4864BEC3A6B1E08D6DACFBDFE5
4C9D875CE88F3488F2CFBBAFA3833406215167A86DD4A6BC0EFC2E4CB6F286FF4670F
23CA8D8AB78F55000F1438AA2CA11927B97FD59D77C44BBDA6B7AED96FB8F66A257A3
D101F4CE024D98E9DF157C8978624C8387658543D9D9645B57B923DE2702D4FB10074
0A82BB21BD8B79F14F7955684E49C4EC7E6B72A2F1736FAA1FEC3BB3B31DDAFED95B1
E50A713EC0050D5A95B9489AACF77847B87D1CBFFAEA90F1AF0EE5E2AACB5D80E9BF1
42CAB92722B0ED72BE31835C9FD0CF160C1400516BDC81AF7CC710146840FAE056A78
98FFEFFD819B64C3E2E946D2AB4380631D9978EDB610BE0918EDB7C314A6F9714E394
DFDD2DE7C788B0E6B01A57FB46D0CF27FBF6FD459FBFC7FEF840D0B863ED6EF1E0A1A
93ED0CD2432C55E8CDAADF6CB31B1F1872BDE39037F5DBC94CCDE7A43ABBF8902291F
CAF063D6C4C17052F63A06AD88AEDA5BBECEFB914DA4CAB60F33E9A7AC89EAD9A0DFB
03AFEEA456AF7558649133E77862F2876A3E21FB57AB2293FCAFEF6BF71E55308FAED
720216BB66D5A89172E38587B1B35D07F8DBAA5470F726C361C300C7B9672AE9B9F2D
D8E7A171E3807DB745DDE434AC32060CD27F446F8AADBB2C234975D42308CE37C6372
27FCF7977B0C0142772AAFC047678508086B5FEA059506DD6601E152DACD2CF235B72
FFF07B50874F25312551B28F6DB1E92501E1E0459A82AD54DF1CC9067FFA316D31CCE
6747643EF514AB6C046189D81E042E7E8FC9F2D190090B1F447C8F8672365A0F52838
A178537B0918B2A28CE1F3A207115631F5A9C53CEEC453306DC03AB078FB672BF9A87
65364E70904F1ED2E5432F5E9B83C5C7B5A7DF47D3B5E2B1C015A4E6722ECF9C8A06
```

SECRET STRING:

```
10AF7BA1D625B16172C5B80E2EE53AE9B7F3EDBE2E226F113EDE5A0EA8D1A978
```

---TEST 2

PUBLIC KEY:

F0878A54E4BE5E0069DC240CC201D51C9B29F01AB8441513C3813A593E8D4AF3E85D2
823205B4D13E994B8B9AF131F62D0CE72C28266692E058D40651D33A23EE143754BB9
BDEBE7DDF4DDD70763021B8BED91D2CB8E4CF79160A4E67B8F40055F78A363A32DB76
E92A68E3A5933168F6AA1FBC674A7DC8FDBDB0F4333E45694A5EA0DF8B2A60970C5A0
473FD12A7442840ABF62B087B85DAED723558CB5C70440F2D17662709617ADE86FAC1
4F0DBAB13BA206FD34EF4069B42D34BDB6CE573DE103C6BF1807B1D99BDBA792903B9
D455F1AD1BCB69475252EDF44A5A79ABA587EA02B5D29EEDFF3536ABE9F36BD711505
ECAAAFCB69563CF5824EC678E8405E39F030CB48B3A6354ECBE48A3A2E6E81F868A67
92CF7FB365EA198186629EB8BE5B4465171A6FA059AB01BD498955F0978D5DC318223
3E14DF033EA69498FDC2EC75E6AB590B59461EBA392F1FF5AB83CE1698846FA960BDE
0052E57E562C0C3EC03F859D9C84B45B0090AE0FDFEE94D9B6FD6EC225AEB39E90499
F61FD72C04C5C0E163C58AE963B46DEC1D5C692CBA28A4F695B578DBA6D68013EB4CA
7944EFE482F8110858E3235AE2D91AED1889573CFAE2F27DCC0531B459258C86EFF57
50836487446A7BB314E5F9AF6CA2708714B4AC09B42030F56E50AFCB8FB4840429CE7
6881B96825A6F653011D7580DEB04333E6C0758D1A215B7EEBBBA8E51CDDB14BA1744
6E3E220F801645D4D79E8FF7BE98C30EEB38EAD3638FD978928980208A8FBBD45B501
5AC2F8AF74002116EE1FFA9F5E14BB026796ED5A799F87A83ECBBDF0E7E96791A312C
3C8D40AA28BAF11940FD3EC7EEC6D4DBE6DD0450BCFBEC45E5E152B775A41865D9BF0
9D72D9183547AEFA8E517E01430CC0D60C75EB6B9721D6C2525746F534FF4802A51A9
861304D9EEF15D6B2ED49198A5968DF9809EBED6C53AD4BA6CC72F3BFED57C56D12FA
E452DB8D12381D4D4D6B061071D39EB27D20BD05FDCC25A7382C333FFD1996FE949B9
151DF647AF723BF8ED5038C128B69A9C21A55E59C958B4C3E818D82725E25A1407272
C325E511708104BC674A7E284958E7EA11EFCF12A62BFDF5424AD9DD721EE1DF346B9
097CD0FE57E688A32586D2F012F18783467A4556A47694E9C7AA7028B405F5454447B
7AD998173DF8F8C5054BC22BDC511CBE84297EF58B48D93524A66795C536F891738BA
AEDBD1F5073B161B506B166568D519A5A2C61DC23CCCE8392419FC22A292BA175C193
B509A8AA8F2E7CDCD7A71EBD880ADFA3F00D294C466A494667AB956B9E35C0B03BCEF
9599128F63CE9E0B0A3F4C817AF2FE4A7DFA18B74E44E6C456EB37F165E7A6BDE9078
28B7371DE39ED79006E8F7557214AF0D9F7D0A8339170989FAD5532CF3C0F244DF4F1
97578880E5BAB75A03108840C07869D7D9E79BDABD80FCB87FA1C56CF497BF87322BD
42784B485201825180C77D8DC3345489A0A1CAC1F15E1A33F9C386B6D79226BBA65D5
F0623E56E418F5EEFF4B5BB2B693A2F7E1E02A8012194FC3BE4BA387DB2C4449679DE
5A1A77731BD9E7AB8A04C24ED1A129865B1A5322BBAF74368F217239D9C3859F870E

PRIVATE KEY:

235FD53C8C14D3DCA757301CCA8CDC64C519A4C3CEBD158D7B3A48037C4B771D6704B
6570444C52ABB35D8803ABEF1AA9BB50EA065C5139F7F91A0367634F079EEC24C46C0
6D2E61661ED08C63D98E7350281A818EA89E37DD028F88ECADA7866AA203230A29C3C
333D77EB1D2B01ED3208F749DAE758CCA266548DE1E2BEC4C7C68E7ED8E9591CCCC53
D2C7C2B80EBAB36724715602EEACBD8565087E9760EDEABC516319462C60EEC13BB16
92405D808A12933DD83A1C0ABBB5C1D1626911D6F87092293EA4B707EBB03207E4E31
6CD41AC5C047DA5BB615C3201A7386193085F08182A29D13B23359D6D0713ED623588
242C0B73A0F1D0D58EA5AB78D5D8705A69C749893D6846BE664D99E987E3EDF5CAC24
C7D983A0D5B97EEED28A67C793B92050B69E42348D76B8F3517A8F9B687748609E355
FA3802EA418DC0349E496E61C51141394D0654AD711F509F93CD1EB898D4C21C31F83
6214A78098B55172E8338ACC147193D651C1E4FD7CFBA12D55DD04A4DB23148E141B8
39D03063D114CD5701EA027AEB19519B0F173EDF2A55EFBE00BF2B3FCA19269F2A32A
409AC055A811A2E2A4E6028A7FFC8E1002C9FE1E306A72E33CC8365972237BAB0855B
373CE1CB89FC4D75A06006C092D771ED5657E0079E9A08F6CF6C81C9A132592CA14D8
FD79FD17BF2E4277950A318ADAECE52E811DDB38DCCEA572FE890037C1BCDFC90864F
35B976A57156693D0C4CAD0ABDC6603DBC9D9F25F931B539413115F9508BD3927B4D2
694B1CE8793A404BF425280627EEE70A1041218AA84BB4C6BBBA57C4A2009A8525187
481A1A70CC530C0C252F2F8994C2E2CF3E8CF4C82162D741A8C8E4B6D4557D5EB6DD6
A1DEB7738BF998A3D969688A4804D28E346ADF3A658DCBEDA6105F557BDDAD814AE17
AE1D9FEA66502DEBFF946144917D2A35734ABF37A239FFC94F7C12A1CF86C5BE52A82
2491312C92DBF51D4294F5835FDD525B933D7047EB92D4F675CB67F01D320883B1CFD
ED1E9EF06E75EB2EE668F2C02A8D0D7890638544361551248E2FC610F45AE0F670324
23A8E1BF0A316DECC1DFFFD84DE7811BFEA79BFA95754BA35D4CA7C88785700E01FA6
C5E9384E20795D5EAF8D3A5F09F12CC97FA20EAABEDE8ECA12C2EF19833A7AECD05AF
F81FA806C5F5F003C4CBCC529D56399C86351CAEFD0E4EB619BF1823542A44A54AC34
3334D3102A9F76AB1A12F1C7225ECE55FD14E4BA6378E9E43988DB3A83A4743457A7A
1250D272CC1059BAE05060000450F6D9A078F6279638731F387BC2D7B405FDC3130A8
024781EACA678EB956C8EF8907BDB0F82D71E30BCEEBF24A9A5971124629FDF74A132
4E0531629872C12CEF6CA62B27F1655F5AB1D6BE0C07E52774C97D9DE6276B4B005B0
AF69B637D51AA8B5FDEBBF61E466DC65856B43574B53838E59A7AF9FC32602552E181
7E8D504B6D697B42E1910CBE4D5FD5E11F2FFBCEA9B87CEE7323F984AEE586A3E9ADE
A4588DF93857B4A39E6D2AB3B139B58556EA0DFB686B5A92B34E80D90CD3E532DCB65
E904823A0BC347BDD2007FCDC0FB1E2C913E2FBFCC5EE0122B6D0B4253A496B4E4C20
FB6526E0ABCE7BBECF5B53AF05AEF9A5DBB981063FDE7DC5DF8D5EA28A2E57A9E8662
74720C5BF58879789940BABB9F67E70B7FED49DD6B8C065C01874C73015D168ECF31C
31E546581A7B3B54F0F679FE337E4D89392D024B01BD64D235DC16DAD48D74EE0AA67
E18CFCFD7BA573EC333C7C93BCC0422A321B7AED2C098E2552611EF875BA78520650A
B67B901F56B823BB342DE97043E1A64D753918D656B406B2AA58BBB5FE33357D0AA53
67449D7042AEA9CE0F4C6759AB26BBB9765B7F7B809E1525293AC3F18D03DC68BA066
C8028AD45353CFF1C732F290609951DAAFCADE54011ED4E26CE31DE1DCC821585BA6B
22A58E456B485F6A64466EE3669E70FFEE54A96A2905D77DE9EFE1A87BB6CBE27493B
89A7002268AE8679264C7B330DB8324E1427E3A6685F87CDD412CAC22A91FB140185D
14

R_(shared,3):

12C98322DB254567E8DCAD7BEE570928831AB9E1B4EA35586626491FA2BF2E2378517
96A05030C031FD84E0F05749A7D8FD1C82B8D9C0867A00665BBD1402C27806D6D87C1
8F8BD4A597466BD54970590D2F8517D0AAD090D6CAAA3101397162458514 92EDC2D73
89EED0419ABEE93773D84524BE638AA7A171F99EF7D2E75860B0E2044BA08ED49D7B8
6E74

M_(shared,3):

F2DC83ECA99718C7857221424360951A3247995C1B3C00BDEA6BCE844A646C9FEEE81
9CC1012AE2692AC5AA106889C101F758CB649D28A5E1065BAD5AA8650E0EDDA603671
5FCC3F5ECFA1A4747A7452ED1821DE5A8B756B3FBEF2E0DE604FDC83DB0C3D7979D4A
4B80A59C67DAFC1684956DC0286D0E1CC1F5AE25F5F0656CDD757EFC14908EA892FBC
5295

CIPHER TEXT:

4FC9BF46C657A9C9DF9506DD4D2B92F62410866982617E1CC7E52E37B2A49F673375E
6200C83C229FF9B2E3A0F98B4B21B971F324F60894798CA01DF961FD998DBB731BE05
A522A9D1919F3EB4DA23548934B59E29B164B0765065BBBB92F5D0349DFF953159129
B5881882ECD4C909879288DCF29C402D347AE0FF477AAA2DB52CB26A0CAF6EF36A984
B42E358AD26D5E481A533CD1AA8B7D8CE8651430A22017EF37EB69DD84C2CE28DA4B6
0593CE711E56575E6AB714B8389FA28996F545193786A62B0C586827C4A35F147F303
93EE5380F576C588191ADF12D17AE15595CE9622CCE5EF90D47F952F5AC8CBFC9E4D8
4EED634B8C75057B978A3558F199711CCA1EDDB9D80100B7949F0189E29B7B35C5A5C
22403BFC26685867D3DF7AA138CE01009F7933E38000D247A0470256305E2623F45B7
D73D027BE064E2DA2FC428BE8AEFD9C712F07DE16186F4ECD018BF1768BC7BE48A1F8
B142EAA49E1086AE7A32B5901B0B48513647DFDED0C83BDBCE7728CAF24F6A7783D58
1F8868E848C1590C8437DD37BE1A9F9EE7D3B97BB8E7BEE89BC842614E3B209BDAD7E
07F82272636F9D74CBB36649F857902F27D7A853D8F8437F535C36FBA3E4D1D151083
3E6B09A5AFBEA696ACA85E8A75D387127145134C66D91F9950B5F8EA8BCEBC6547117
3863F762410865FFE639A14FB785FFF782DAA6D336BCE7C5CAF22852DAF8BDDC5B775
00A16F6C6F800999BBB6E7C23D035D5A7A16DFFD2956B461F1089DA71C83258065B13
655FBCCE1423370E5C72D2B6243E56DBEE55A6D40C315378990AB4081E15EA364442B
73DC64A4AF7E83C390794025EC71B6F06A445BA34C98598113095E54AB105197BB3A5
A20A29B26758AF0240E15151484A6E2BDEC66BD26A5FB327D33E795726B8CE95272A8
0783A41D860BA08DE182D3A9913351D0685D5203C46FE0D73BC2DF7C7DDC6A202B684
C384FF0CECC4D9B47CCCDF9B4325CC2D58C2543ED3284BEF57A33BE0A90491B54D495
36C86E04A83CB9ADF6DFCFA40ACE84E137BA3956DDB2E6B7BC18CC85BE3D6EA161663
6BFD9037ED0C9CC158F3D0D7ECCA2B096CE98FC7A17AE02F8CF7E36A184F72505BCAE
21319C868BA6A0F0E5A9D420E7A6DCB02AC83EA2FDE469B1F6D0B86E4493707EBD8D6
483E699CC103B0C47F2D7FDE792339C6DEB3F59D076740DE7536EFA7BDA8DCE6A30EF
57D848FA57744E02018E5F1E8AA294E7717D39944EEC7E9110D25F77F0CCC5D2C5DB7
1D8026DDDDCCE35CF096A423A78752B9DE66EA95A37DE0688692E4CA0438A6C27D549
778FBD54F37A1757FDA6889FFA05C412738E5E563184AB5BAA3F8FA8B74C1CBAC94A5
E510BFD961830C2881B60513BCDDD34B3A63176E3ED6CD5EEB37805E1C2E2CCCC42C6
9E7AA9B721A00EDE5F4F08A44522558A07B50279AE3C71C18F932E967AB274AED2DD8
248F07603E6F550264D52B9A423E84482CD71674019DA1C75AA9B1124E6ECBFBBAE43
63375357CEF1331D58941B45EA1C3A7170FDEBF1DAB6BA7DE72EBDE3FA0B139E39000
903B9BF8ACEF28F6D5EDDE30746605105C9F14A678BC358508F905E1CECD0831B402

SECRET STRING:

BDF966451A33C49A5C20FE7F9D1AB6D2C5541D0E2CE155C7363B10A20CA23831

## 9.5. Test Vectors for ntruhrss1373

---TEST 1

PUBLIC KEY:

```
422B9281C50AB64E866C37984C68D8395F4930258246B4C5B4B619264736937324A61
BF0444A21B8085FADBF4FCF070768AFBB832E732598F0AA15772F5581A4CFE3BD2BCE
685E3A3BE324F90CAEB97330E2207C958648F6E8D7BA0111F4950D6C303AA4E9B478A
40D857B9946703FB3E93CB7C75F29F2642C5551F2CDF6BC1721C32AADB45BAA7B3888
C5B7CA5E6FB3DC411929FA923E1489A00B4D58E9D0F695F9D06D9C4DF646D55A40FA2
41BC430D8532659512E4BBBCF0683C1E6110A6828435C528639A659D13521C05FE149
6DCF10D869BFC5230F884235EBF7C9BACF5D30789E42347AF77C42409C248365DCA41
13DD8F139E8308C1D3545F86964BBB9DC880905D8F8183D4EB5CF310CBF475C21B431
3A8C392E972E84294B6FA93CF99FF398B96E93B75F065FCE94CEF223D367F14FDF23C
ACABACF9C4F7CCEB8116144564A97807C6DB0B0518708154599DD368CA01C3D66B346
40142B663486C772514DEFB5519BC5E1A81125DCD1247835699E6002E9947A80D9D34
61BD24227CF97CDDD3111074ECEC50E9BE690EE64BE968615FA1BEAA9FB620A5AC931
B490183A3C23C7B99F248CBF36E34A18D68EC2F9F13E9581AEDE83C67588DDEED9CE2
6D0732DF967503511440D7DDB0560B686A36EF260679AE49837F7F753B3728A9C4046
573A62F9614292A1CBAB47B0C41B2B69CED184143ADD5DDCB8DC50BED3B55BC67E0C7
CDB8DAB9414CC234065FD540E1F06DF542BAA213513FD38614DF64D54BCE9AF236400
D48174C340B1F1AA13101C2498AC363562B2634E5ADD12EA46F79453897B41880AD82
C278AA3B10EF370A0F3A1F42AE79785F74B7977B57E1659536A2E072BC5D43CDAFB14
94B07060198B98A639C4617C609C9E6780B03C46D46F81216BE9DC1FB069213A2E539
2CDD2EA940D3176927252DAEDDD9430C20330832254CC265845464DD8C1C4827C8069
62612DA775F437CAB7F619C5FB55C1CE104A6E407C136EE2772D727F7187BB1CFA759
8A041AE4539123A2581295EFA25A358139C604790B989E4844C25D1503E8E1457BED9
46CDC3F9A815A57C4D7A864055ED11E28F8843B9032DAF892F4CD0D9FB209EE0BD55C
B78805554E882FAE61E8C0A395C0A342060FF149E1941C7374ED7A4A447AFD239F193
82787FE3ED2C7146B70470E24558701049B73A3A012307EFBBBEEE364894A33554A97
3FC65CD5B484056E49DA36D5D4F92AEEB03CFC1295A023586E35F1E431D505F745713
6EDBA83950416E620307D9DD8B8476BDA262CF051793B72FD9B62EBBF91CAE490CDED
1A990959C0EC4A64F8D23DA220238B29AA8630650E94C468AE7F63EF5EF8A12D6351A
EE859694E90E1B1C74643F0CACF71328E38E02332F8CFF01C7DDCBF71E78CE9FA8A01
57FC884310C33C1E18A670B6002EEBB796BA3E18495825AFE3E070D7F1864FB291D1C
768CB2243E44669B70EF623E890E0ED88B5FB8F35478267F305029653AE8D317BDECF
ED457087CA1DAA258F636CB703AB84162B37AB777AD8B64F498D5700D03590616EDFF
0877B4165310973C6A1B7350D25CD1D1F8BE17426D7689EC47971AC2FB1B1045289DC
3EC510D7C73783E3C99B06DAB8D20E32B8EFF294136DA15B749BB86F847FCEBEE6E72
7A1C4F28637F5943C3A2CDA3B6060B92438E23D3CB7E7138FAC9285AC65E24DB8AEB6
1ADC1A6176AF58758D2082DF99C2AC36900D698BEB55AE8229398ACD4C24CDE5810CE
B4BC99D95964A47ECEAD7CE367E3F72DC3BBC4C823F98C18D72F1C55B400A8501E8F8
CCDB81852BC0386DA0CC1FBF8F9B09AA325D42C720052C9C35D48C488873E13183D45
D4D0E1BCFA1A6FDA01A58036B967D8ECF5B99345E5337D9F3AD331B125B2A46ABEAF8
C099FAAAC4C748EB75BF5382F190E3A418A4A685D44A6F1E6C1E6D6F91ACCA7F6690C
AD35D7F23C5D89DE7E125FBF8E932C6CAAAB2022E262DC18A6D22AC2D02858F48C83D
1D46D8C08CAF1126F24BD8313CD9A8EBEF44FD4FF93227FABD8773E7FE738046D47AF
63D1697B7EC48906058FE19B8ACDE4C8A273F6635D91A371491894E70F2BC424E126F
7D599C7EA197E457E7933B4303BFE3140B986579033A3E6A518275C561440E6F6D79B
56D34BEB9DBD9F87B1DE50487A01B6769CFFB8179023D0ACCDBC499847BF328C59AEE
176CC23DA1596EF60B067D09B6FA40E0E9860FCD2415EBDBE04245E461E2309148504
1A36BBB0E00917A541518429B058607768AF681024D310D429ABD935BC065E4D0377C
D64641FA9362A6B253AC600272E0DF0A2CACC859836F002B3BEA0D5D6C39AB3D5CC24
```

```
022AF8E3EA9265177C86F91D4A10F30CD4269D177405148BE31F00EB4A10098088749
25EEA1511F970D473EAC9F5317A206FC5CFEF5BC79CEBFFEC572454BCE2D48435A215
4819F5391560D228798E81B2AFC47DF585AD7DDA0F4B9E425862B0E379D2A183CC958
04508079A25A9C0A2DFE2C967E15EE66B48CC0F12D8654839BFC481732524BC9AEDCC
CFC7B0F438793091CC94EA1B88772235C1C888161004A0C1F5F600001D93828EA8CA0
C9A45B02EF1465028FE0AF3C9A44CF3BD590238578A8912FB91B95D2CEA8A19BDD375
BA837009B5E70AAD831C80F8F62D999D24B570C7336266CCD2BBAC9655144A22FDF84
1458783E88CCFD5418D5633C956397E25FE15B2A558DC2F99A9931C91AD3B1FC992CE
59D0AA141216027561AC558DE2C78E2B93E6811D2A7EE06856988999B1360D51BCED7
409322772AFC8E09687D0EB7423721A9D6BAE79771D18448952A4ED2FAAA4545BDE09
6CA0ECE59FB6267D61D037821491CEC122BA063C6EFC95E2BB3A78F5BCA1F32098216
9CFC8324F13C9B6B0369B441BD0BD903E64FC0F2F04664B2926C6CC400BB95F3245C1
1B1A6FCC0903AA197731838A84816A2B8D23747AF47C377E1F094C3406872DF2EBF54
CA6232291EDFB7AE6CC6B74FFE58E10AB460396FAA67ACABC58ACEBE437AD04763626
17129A81958DEFA4B1F39F072822A4B964B483AEFF9EBE4A82E673EB35AF98F86582B
F29A6A6D7E02DBACACEA35DB2739E86C03A43828D776E4E6EED5EA85E8A7FFB3DF4BE
795D3D96A0BE89BC487D6F2D212DC2B5E4851AD1B5E8A8B966DDB51EDFA73E4779694
861CF7C64A10C59AE60DC5DB9E1C75D1A3E35CD958DBF2D79398B3A171F138BC9878E
40CBF8ABE1B4F6FD8E6898B9E63822FD3BB23FA8ECF92DEE2B3138883C9B1826A254F
785B717555C8D162C046D334EBD0AA351D17547AAB37AF158D1DC8A4961C6B7246725
DFB86CC19DEFA992429E4DD6C1707C76BF67FB390AD07007C4A8C877707C08230748F
7C2F0D0E963C9ED0E9E2231089EF4EDD8177B0CBB
```

PRIVATE KEY:

```
D067D98F0055E2C3DEEF1076BBB755AFD065112C85C46E6C350655D9625073E94E452
8C053E720206CDB780A61AD5120C498A4CD3E60C334D8702F0F79D81418AF959CAB77
22EBDD30DF0A479E1403D337AD923E5DBCED4EE04839020F7751C075A4892AABBB0E0
01ABA95515E1B65C63C503D97E51EAFB9AC930F5A1DBCB7E9388B5EF1E75E893E1B5E
49955E7E3E4B3819DBA9EA9D23B0986F0DA2ADDFF0A310595267BCBB7A7B31AA59C5B
C5C8A53D255803C364B4A64C0301DE319BB028F336403B280556E05D66E07E3AFE5E7
816164194A3CB42972A59B0958540CED924080CDDD7BC130BFE5146A811C6231C6F0A
F30CBA15722D34E6AB9C0D752A16EE24209EF54D51395295F9C8CC538B3192B120690
77C2DAAB29055CC886C1B7265BA1DF3FAB0632C8B6A1797DBC9C84876D6F34E2A36F8
D16DB22EB5E7AE322C7726486ED020A5A460A1E95557D1EBED367A2D3C32776C40C31
59505DB6DEE0E06F64870E5B2AA0CA1696AAB6DE0576A1F294296BB1E3912CA96D4AE
AD3BE0869505D58E77A224062C41C663660DD6F4107D8AC17B8417E9A884682243C4A
E9EADB450F3C26253BDDA51A55DAC4B396BF4212937F89D2A093ACBBA607E016405FB
E4DEA63B625B8D064DF3E3FAF4499B367878FAEA8E1378F8BEC103EA4E7A6A5B41A35
6A06933768A170BD0B7F4301DF78552B5782468DDEAC5872CA5C739CA542BB2C128CB
E52C4BB00B1C88EA06B9777DF4E2735637AC6253E9614DC3DADB3A8736FB3C80121FC
2BA62BE7B3CF5878A24AE62675C4181F067A9AC32AAEAA3ABABE56E829DBC40ABF115
5B94691D56F412CA45BDBB44042B19B1974A06DAB0C56732BF401DB9ABE9D30B9E97C
650E70C2FAEFB17BA81078CEDAABB5C8C2ABE560FE36FA42A4CE7A6107D40ACB2192E
0E9A5A7DB8C5250D011D4B882FF956D2D727ED20174AFB35925FD7242939763BDD490
8D7CE6C4F95E55E2CE5F02D7A517FE5A32309FBE25CC81E1F0C4542DB1F3792CC9D22
2D62419D539688E33306A24C18EA6995AB8C659F65D2AA8FF4968EA8C741991EDF972
57E83081D177B78BB78FF983ABF6A5A5C170F0AE73F66BC2A58455195C19F1C3716F3
```

```
59B9247677E2F3EE2733BDDE3BDD040BE14935388AFDDD42B909B8E87F23B76E80277
65C66270806C52CBB14AAFBB881F6CE07FBBDC5E43865EDAFD05962AC44CACFD1E71C
DDF38DDBD5630AE448125DE49686A620CE65F3E15A20FE4AA5898F93640A44B95A151
538F272AAE5A0E99C5B59B63B09D9E54EEFADE4497D07302566C90415788B67ACED71
4A845178C68EE405AE7B8EFE20C3CC138772072F83D08BDA47649B6593BB406F9BFC5
0A86F2EDF6C1EA9FCFB48BD893C70AE09456B682829BA8EE0E285E63142FB00CF96B9
A60F1DC21F18C0AC91983B3213A3A2C20F684EC0E7B3FF3150064D129FE15A654B17D
80E783EF5D5CA155047D9863CEE39F7DD2005FB4D8DEE5E55DC120CE7A0977C3D83AD
2F3F09445505662686C894668EFEE6A5FAE7B09CDBAE1B7AEA4BE958C74F05FAB2D7C
5414BE6CCFE2725E62D78A2849EDBD67471B91338A2B1CF87A8D8BCB3F220372077D5
F3731C1A9DA966F35417F9707278656F0D15E1ECD08FB8B34E0AC1848553FACBA98A9
57121CF036D11D06965229A63006B0D31F9537141787666C824BDE6F880BF8CB124B7
5C51C18F6D4027DEE29AE9A39E3A19BA24BC0FD3D240FC234AA4A06C3261980541178
C14C0207A2D2BE619D9155103509ACC71DE89ABB9F184233CC271DC06675951CF4129
56D88ECCF6F77082959340E712C68A3EBBFDA98E8E73A9C2738A2C2E380ECF6F0C672
F5A5E32A4F6947060A453A476883BA32DF45C3BF7A23B59C55B1E8590CDF7B3B3E553
B7E768E6C4FC206372E959755642BD9A2E51762416F73BA1356D54182C96EB4C3ECFD
22C475AC7E62F681E0D124A5B91138618B45B5BA68493316E7A879C923A1B81792F08
11E49B4109876940412442BB5188EC1428E1EB353A284F131F33488BB80F623449106
E41E3F5C3A06EB24826EB3AD8DAACFEC5929F2E755081071922D28A64322A0E795699
D1187D56261F651C99EB782272DF8778EDC1163F70A7430EEA68EC511072F8A4383CD
45CA77963F1CC022E608F6E669D23B07797D42FDCA23D028685E47908D424C8AEB5F2
6D0A326D67567E8B0AB3033890DDE6A9321DA9D0BF102823F91E86BD43EDA6DAD8C92
CB87273A8507CDA1783BD5A96C0E3FC2034E39CB409FF912C4F84B43582D13579268B
8001443A336E23C41AAAA95054E0F007905CE4AFC7DC39D3B8A400E75D347C0C40B83
D03F1E589C4FC3EF4D99C852FABB1678032440252772AEE75FB8054FE031DCEECFC0E
9BADE269CE8277646C8E3DE6E4868D698EE7FA100C200836D097CD9A54CB29940A606
A44E1B867FA2711847217B5650D152896F32DF45B0785ED6B81E3E40BFD2D62366FB7
978FE7E1205F52614E707DBDF0D4A4F9764B3D30A0E867F99A6BF732277888B0C1786
1A69D9305A14649FB0396C2B7B69354D966E9CF96950FC6292B13F51C795F07F0779E
34D93E9A4137FE8DD3C9E99C8A2E18F4D883592C51DEB045051930D73C20C85C672E2
505A0E503F6546DD5F1737B11CB08CF3166634AB9711B51BFBF07247F0694D9EDA305
11EF57CFB4926160918E2DFD181AD81D2EF40476131114901D1467D245D225EC9FEB2
167B58FE0F837F48970A06076245095EC627DE9A55D7D2C0FE7EDE6C71561AFE07809
BFCCA441ECB6CB9306082CF5A65197550C4057D7A51AA6A2C7064CCF1821356C9EF23
ACBFE45EF0170B2EBCF4E8AE71C96B3A04A57B4ECC4A1B2E9597D33F980BA825AEB97
E25D1B8405E6EE7DDEC4E5FD2F3C9BEA6BB7B18116959353EB0994C9267C03BF4CF2F
9C272D3336B7C4E82BF6991331E081340C38984FA0FD03A423A23A36E8C7DABD8A852
317C287E3528E66AD7B65B461AEDEDA21665C199A223E7261E7BF1AE01F0B9113AD1B
1722D0E2EC54C15C85AC9289B328CE2BE6BEE661EDFF4081467AD0C948590A55CF85C
EE2E9556EA0CAEBA0B56777D082DF09436E7B376871D524676420FBE51369F9A0027F
BD18992FA22F00E02F76DAE64B50DD6957E7A7268C057003142DCAFA768B3C380B671
8BA9551684332191D2BC3214C302FD202CA284DAE055E2C4DA760D1301E65DBB6F046
0C753DA40910C4162D28DA537289EADBE72CA7EA2BE39112DA2FB15B702A49426BC60
9CA187C5035606C5753139B7668E7DA97D6548FD19389F09E9997B74145FB4C7A5E0C
456F07B54EB42234174DD6B148BCB3FE39DEF4BC99114761E2CEA5FF2FDBDBE6F2E77
78891358E948043D590DCC79A75F0D0C94181C3591DABE538BE3422E635000122E3BF
2C1CAEA84E1EF5196E6A23A7937D30EAE08985A8864DDBB0BD71C09D54025018C4AB9
```

B05A7F71B4A7089740EEBBC59CB7F128C90CCFDC551E43C6D3604FEDB3068547035A6
6E151E529B3A414AD654EA0C85666B7B4782B38309819E50656AB91C206650002D0F4
2B5A2EB3E2B351F85A1DE9AE9939597194D0EF2BC54A6D6DD5E84A9A3EA0159395751
71946C7D4049C8F4CDC8C30D7AC2156819E45B03FB3FD1064046CCAB0DD90A56B839D
2B40CD6C739897C35D5A5959A45E44B75F360A06461FCAE18CD29622FCDAD42FED213
5AA48EAB935169765733E7EF6CC6B334CC36C7D8525B0432FF1E366BB18758CF1EAC8
8813D5B0E1828618CCD1C72B2F6C5D1ABA70DFA0FC269896BD7C24BF8FAA32F08063C
A1EC9D0F9EED5E7B97748D6BC68831F6801014B1B4F524EBA67AF23E91DC6D2EA7A98
BD015614278E791E1FF5BAFCEB0D55AEF641034B239DBE0DAED357EA67F44965F8439
A36EE7CDF13260193250C2862A11E58AD394E4DE0790016326A8364F9AEC51D4C6AF7
E92930544435CE8EC87189620950D94A1EC9E12E497B14FF8D60322925EE373784290
02FF15B2B12256AFA6D8F281B2EAD5ABFA045A1C5E8A2B6F38C448B432051F022B77D
F1F2040C9AC8E33DE5232DF1BAD1BAD3E712742F2C5C032B7E2C4F9DA0C5AF7D74BA7
56285D0E98FDCA7102F5CF746848B736199C54F58932C855714B9390F276C0A7823BB
7CE5E7F02237CF84FAE94DF3A33311971B3384289E477A7F5B6136B8628CE6F73DBE7
B72BD694DC2E456B9C06404B3A3C0F6B

R_(shared,3):

245A06550D0A0138DC0938DC8677448C3CA12DA9B9E308587F7AE42E8239718C62DF1
01289C76F50260BECB0D7B6825DC84829448CDBA135C355C23C1847DB66BE2B6CEEE3
649FBADAC10B28AB7B176516253C4F56A38C78881C5B03A07891A36C8D88DCB55B329
79872DAC7C2190E9E001E96118F772EEDDF63360C8DDC46A6B154EA62E1E6534B7150
A90CD3E5D1C0CE94C62FEE64A00C1F43D43BE2AB60D830E79F2509D79D243880B9921
EAB95E20E4CC39A9A8C6ADD6432F08A6CA57CBD9CEAC219923775D3CA1646DC4A8BAE
6784B9803D102E02CB8F5DBA70DE153CA41938A6325F9B2E49E9EB6ED39F14E67D19D
4B0D98C1FCA9488958B93D71A94F2C0D47FB0706B29DF1AB58B5233B02185260F06

M_(shared,3):

0C84DB4FEB775A28E44960B67B493913ABBA7797C02B302F2E675C3E3FA526938154B
E4D25A17B61204A7172725108C35B74354CD6A745616DD7A735DD907EBA205A7B3C0A
347CC06426418B52588D2940A126AA2C93A0931C459BBFD5BB3898E13F5AC2A9D110C
71450D0930654AF3FCA7D7A0572CB8BA6CDB06940243FD3F16492D442D54515101186
B464DBDF66C21EDB4A7B0E02CFA3C9EF0CDBCDA9602B407D949C4A759A5E81874D482
EA61878904CADAF3F55B63CE78243AD71EE849C0318E58A430F08E04E66C2B0BF2074
BF72542AA8986703C440CCA845311A774273E2C9D3A690CACC221A7DEEF1B141F0F2C
5556510E4D90A5E8397A97E408D9D70B3A844F28A6B9DCE9170A9DC903DCE34CF04

CIPHER TEXT:

786866BE5C8037D1CA44A16FCC2F22AA4642CBC6390738C153FCAC5E5E27EC8046B8C
121EE0420A98E43D8EE785539E84C7011BDD33299372C1299E7126AE257D1403EF2C3
13EE74B2B935838DF8535ECF80D66A082374A5A60079A842661250512D605D80C7359
A508521CD6E31AE410D4330E29C6CA6393DE0CEC4F066B495C8AF7EA049AF5A46A41E
D019F0141FBEEFED60BB40E123405AEFD16DB4B8A86893AE7526C388704A6F539F126
3CD044B0BE950B31D8D05E2293AF81FB9037B48525F136CC7E33E58158981F8C5E92C
7A3A062F80EED0DD93FA89536B5F3CD89C5D245EE47F9203769E71898C34F89C7791C

```
1E8A1C92FA72583113853C23E5B2261A7F94D285F69CD5508F6E451CBA49A3A4A65B1
4099056CEC8863A712F7B447038599F740BA60B55C1CA854B542C3D9291AD455EEFC7
F88FF455F84405E0403B63D20C70EDF93924D8F76077921690A5BF6FCA199B4C7DA64
40DAAF496A64394F3CB488E8C66E6E07927AA716F36E4148FECA73FB31BE58A38512F
B2A9F757CE9703ECCCE8810176753F11DA57C3B6F6B502046A7623DE79CA84A98D7C9
9F941C513A08894CE36246F8E6A9661B96F633315CEDA2ED692F8B8FE75920BDB5253
68B12A56080F39F8416D60523ACBC74A317DAB729EDEB04683E4DA391B5F3DF982E5B
5302D7E43D50FEBB429500F5ECAB10CD1C4ADC1CD1D40EA647BF069DB312FA100DD7A
1FD5CA6B4F4E70F00DEE4C46BE676DC1A88EB5E8AD6B7D9406CAFEFD0DC3B68D5B75A
EF4C08C53CDF7A434406F19BDA0485FAF1E1617ED7D13077EE6BBCF744968CE13A182
BCEEE7F87CC389B830EBC8F80DADFD7CFB856C1567E67264623FC19CECB2AB8CBAF15
25920AB35CE5CB401E1EEB37DC030FE87FB891C07E9324DF544FC97164C230143E35B
4D31196AFD0FAC5326CF8486987D90AC0DEFAC3702D67FD5C25245A4A0463A1BD647E
C7417886BA0E52BC2DEC853AA033A1170D3DC819D5304CD06A54E7512F8FC4961AB54
0705D1FEC514B15495AF43A50959D2532224310872F8715DDE2EC155627FF23A1924A
DB58C1B1B73598DD3500BD53EA5E6E843BEEBC31461749B7E78BA2FF595AF117A240E
F4E27DF5E6F79B078F8D840BE89FECA70252A0017FA13EDA87E6B126F09C58B3BCF42
E874C3199CFEB6CD245564AF550EA1FD47F4C330D2374BB5861A6D257E435BBAF2161
967545EE817B5394348FA4E917FC1CC1C91ABA2BB02B0D63E395FDB03F8539F295AEE
A42AA38AE6A5B85FD0BC6E9C5521BD29A08AB8FB92361DA54C205062BCD284FFA6493
CD986A75010FFF7034716E98CF96CFF1027E9862D556C7DCCA40B08159AA52E74C9C5
A668F1F10BAC7B27E289D47426F548F55B49B9D3B4974F7FE16F1E6E1275F8A7729A9
F53FE6873EAEEC0E39F64C6684EBC71F1C98175E560C3FC2537AD261D98193EE528D7
9E7CE264E3FD80DB1D05A05577A94CD08E42A3968385393C0E11C5B65F87189E5641D
9490E974F6C7292E1A6627F4DC121FDCE93ECB3CDAFEFB6F3B4495393A315738CD97B
98C0FE4284523A7AAD6D75BDEE1BB67E2EE687BC3B0E489C9C742A05A765EA2DFA815
9DB15D02839B9B065A6B3F36705BEF6EB3569603A9E5CF14A2D786A585F8B4A115567
643ECFC9859D3CE7E764364919A658F19DAFD7FB7F1C188E16502507D1D0713C79BCD
A8B4821160E994A92CC6CF6DC269951358111917276F13C4F268D2596A164A4279C83
2AD1272F2DE19C850749C9C1BACC1384BC8AB9DE94C92D6BD27590D8E251E4FA88D7D
7AB3D5717C717F956611D3CE02AA7EBBB3B329A29785398BE01B8A2CDEB2E1643B1A5
C4AD942AC629EF29BFA4F6ADF52A5E384DD1685B2BB3033C61C19EA2208BF50400D09
81635067D35E4AAB60EB1114117779F89449EF6AA04112345C550DD6B6A6C15BEB75A
6A1D3D2B906FD75F9263B3F624519E2AA88108FCF4D5E9AE68C69DABDE61AB31F1EF9
985FE8AA2F175BA991373CE699277B87F1DF63D8778F060EF8146BF14D150E6AEF434
9C80E92324EF786F891015925A49083E9807226BF444DA40C8A7039DC1D71E9B3A28B
ED76109F8D46716FE73F9ED6B61B5CAED305842266B7EE5A3DDB74A5600764A6A13F2
807DE0D820F01F78D4D6B8FD9634B210CD39E5537C62EA7A09FBF4613EEAE0CE3C34B
A9F0D3CD42CD1D1998FA8A143ECCB40236AAA24D9867A9FBD55ADB290DD24F898C41D
7D8D719C3B6A315EC41FEA3838244FC94240B7FC4AD4786DE66BB2594CA4DC5FE482D
6876D5768E21D895303974B0D879E635B657BCB11B729C67D453AE46D783D9DB02718
23814F8C14AAB27D2FEA633B93A21F4CEB43E6652CD031CE0C9A9562217C7623DF85B
0719643D5EEBAABDD1AD85233D94756EF37D1EB4BBACBDAC4840457421437E1768FEE
C465C596BB33800476394BEEC3985DA007FBD83C16959916F48397D676BF4BE3A2CAA
1E4CCD322A22C04846D2B50A572B2B932D859905E7A69CEB9175E8DC99C440C84F249
BF57BB4EA07DAC78077F8440CAFF1D872FFD963B20AD1B148AF3A5F56EA5041F13840
A85A15CD186568F4BEBFDE5B8A9A076E97A6A0B61A292AFCCF7BBB37A7B0EB6FEEF1F
2ED323CE541A8FF5F6E81634EB41DA54C546C9B050869D74B1DD88061DB568243DCE5
```

7856A9628D4DE72C6321A1DFFB4C4B2EC8E8D678218871331A38EB43C52F7B87AC9D8
F69BFA35044845F28D7212D14DE5DB277C58B427F86A2953925C5422D817D3E007235
B5989F7F7A6D5C98359C75A390F72D7F8B3EF20D58B8FA73880D64D177B4E9EC42CCC
6973714ADD734783763CE19C235475865FF7C02B2F42D2F7D357D4474F3A417DDD1E5
319B8300107A72375FCD130AF311617AD9C2D74BF28D20E43F5BFD5B097279AA5A4B1
E894CB50F3CAD0E2076FBBB5035262EE36D8536E351B36955E0B1748E62ACAC0AC1FA
62CD729C2AD074349404FD28BDFCE81A37CFA2E6606179A87A2EEA6ADEBF913914C56
10E241BE1EB26CD8882B1FB70B7AA7C8AEBF2592306F1BD9706DAE9CA4D6D1AB51049
E141E29B8515D61FF707CCC9CA91082B2312F9DB9CCDD298723CD37D92EFC0CF3DDDA
7D3B5C72F77CFFA1AA914FA15C1009217659EB16EACECDCAD1E66C1CF2A8352C817AB
0676C5518AB4D0308EED4BD1DB8DCEF5800B58CF3C9DAC62ED458263E1B745EBEAF7A
EB9E05B97DF787124C436D5A33B37C20C8D53BE50C3D0DD49AEF59F3A80B116FA2353
CCED75F5893D57D1E1382445280ABFAB7C44DB15ECE4A282E527E645E1DFC4B7CD57D
A26927DA9BADEA9D216FA0789724ABA856989CE2AB43F14BDFDC3682D7C8B758885E8
9A367C44C08FE7BA856FB85EEBD2F3C1090D77FF3

SECRET STRING:

ED35C61D4669FA76BD727C40B6FE8DBC463818741E61728403980A70AF96E319

---TEST 2

PUBLIC KEY:

A1425F95411C22BA7D0AC607A0A7CFED2C58ACB5651B36DD08C878789B15A229563E9
41CDDD66B518FADBA09D938A8DD92024CC4E2E0645ECBA4A40C1169B0EA399D49E7BC
6795AB018783233FA65F8719406278166FCBA2830145C6D9F4BE5179379317166D553
6DB3BD616503651B4C0723974BB84DE0259A0A9D846B5593D2EA5336879173902A80E
FA81B8959F626FD51F59BB7A0343CD8474A3571E8D76E66C3610BACFE84722E7D311D
8D1580AA348FA79BD5C90114869014D1DF5A40423BB69D79ECB224B44A310893E04BA
61D4EAE63432EBAB8F03C0E2EB632BD258857D0B815E3DF931B61F695C2160C8E1C3B
269437DDC5DF8675BE1C2A513AED50F6E77E5D71668F3852641242A723862CEFEBEDA
D8AAB1B22C3F986F68C4C0BEE5500B1C6AB4AB25562E9A55421A97FB02F1617A2D64F
F90328053DC783D8D6714CBF9BB38FAFEB0F29E4AE7327692894DFB4E9CC18C1D881A
2B3E23782767E246A5588523D83864D8A116D48B3CFEE17AF409A0127EAAD15DC4C7F
C5A3D3C49AFD25D064FEE18A0EF0B6203457278BAA9BDB579EB8E7DDA095D5215E7B5
34C75CB3BC233E44276C40A9724C56442A36A04868644F0B9DB7B17E58F03A0C30DA9
DF3E6CFAF738CF6D78E62B3A7CFDFF2DF5A8E35770787FC6BBF5F55DBBB69419B690D
88A4134CFF7C80250B10A73A60AFED74443AF258C3E5629FED7F765A57B48260B014D
A248969F1656AB0B9CEFE75F9EB681D88870FF1725FF6B3036D63E34C40458DC8ACC4
EEB5451A87CC3A85F1B7ACDBAAB7EA4ED0AEA03582868EE4F375996DAB7B18E759B28
B51353DA68C9B248D8772CE2880B28AE21E1172187C0BED0D166989FFD81DF7F0F811
0E14A1645981EDB8CDC509EE6307BC4C75863D84EC6E50DF414653DFC7587B3047073
721DBE3EB311ED129FBB2EFF9F4F8FE60E803581B28B5D14E16C1B4E55CC3296FBCC0
561CCF5EE2BAEF940703BC2C0D5AF27A52E6DCC3E65F1D18F6350F082D0EF1283CF0F
B065CCC1BFE234D3CB93786C50585E09EC99F1A882D662901FDABE5FF29EB2B718C81
73C9549B7A992D0769430C15D191E7BF3E961808436F306CC91B5BFC2ECB4A1C0C53B
7FD91251CBFF9FEEB6D894D653A1359E6BD01F6E9597C8D007C653CE99C8DE0C663BE

0299902A7DB0F65DAC7C3A7DFB576F158A72145E67ABF83098F23E7BBAAAA89ADE614
7672DA6AF7C939B86E5744697E3340AFEFD867456733E994902802F51773BF5D82C52
3FFFCAA53BF3575F171355ACFFCDCC96A760B94B62CCEC4AEC71F383FF243B57DA628
E3709B075A2A2FCD720C702635CE301D87CC2CC5DB3561864143957EAAA2982F04365
FDEBA918A2508B9243D471C7FD5B1C3CC3DE7242B1E503B248091740BF4DB3E69C29A
8A0D4F600D0FCB44C7088FB1D81C352C98653AC50F1C89DF62714B0F30F5E47F88DBB
065850FDB2B41F82AD8856592C3D7C903292CB420D60098AC7491ED1F13FDE628C841
E0B90694F210E89EA92D7701D1C772D4283C511313C2212F6391D0598FCD0915C668E
7D1679E5EFB83D3A243352092E089E74CFD9E0160E67E0724E8A552E9403C91E11784
151E14238A37AD3EE0AC0A59F3F0929CED2F5753EC4655ADBCA3E9BFE8D582B922EB3
92C5ECFABC2C06C63FF71071C42FDAAD5A5148B763C1B035D74BA731DAD286979F5D6
B90BEF07C02CBB60D8510EF9D56F36DBFCF1EE164CF331FDAEAF7B473907CC3317ED3
6AABEBECD672BC6C78DE218AF9C8C61F609A2D8EE088D676A52F72B4505B8298A94CF
CD3E987661270E906B2A60FB61236F1240FE1C8FC7E5A46C7B1BC718EBF5D59D396E9
A6D622631260A435A21562FA88D5B7C84A6EE7B88BEBE24AECCC9B83F1982DA496062
6881E9453C3D441EC7050CA05C8E4E7CD101F546E30760362D59C8EC0FBDA765F1462
4542B68C03BBB728CF2C36987C650E60AA15CFEFAAABFE40C5AC186CCF4C19D6DB0DC
7AD649AFE57ABD437766A16DFF849BD5B891B87E3CC68C5E59B1633A05B85B2D3BF78
3248E8207108A84CFE9014770AD7C85AF0F128F12222B4AEDFB0D60B0C85064CB6DFD
81F26D1E083EC7CFE2ECE224069769C485C8D26C2F171AA7FB8D11CE49D5DE1070A38
8D2373376B7F30C712185ECBB3FB9E1B0F1C2D9AF137DC5FDA9343FCDFE688FE50839
277C39AA485F4323AF4BF3F9DD156CC33A41C02254FA27706E0980DF2025C8BA22EDF
3C80807C9B4A5495C9460C3BEA0B5E22FD96682C625BDE4F82BF1BF10EE9930D6EDE1
CF1CEFD0AFD815DB47397812C09BC887FD04D2407C8CDA347F925C0867B5BF611AE9E
9B18197C0CC8FA16032C92C9297A1772CF2A8E1760F805343A1D1CECA2BE7F08EFB72
5C5B7851349FC419790FC96CCDBD42C77CCA5A7DDFB360716817F4CBB02C625D86D3A
EFDA12C799036C0A82D3D50150581442CFCECF158AEEB00F97D26C08E73AA2F0C486D
9A25D7E6C498617211807AD47255AF14BD16DE2C97C7AD6C6E64205EEFE1AEEF333AD
F01E5915BEAF9E39452C9EDD919FAF6A83BA050D9018EFB30A023005A5CD21720D5E8
CA336A6421339167BA60AC06FFDA3DF9B8C24AC97F088C341FB18DBFDC762C3D7AAC5
54D0FE859BB4EB24477A21B77E782201A9493A159072C70C5E567BAD7F442130EB21A
59B6F41606F269902C3C82BE157C4D8C4B11232DDF82E65CBF0AA0D98EF6C17B45F1C
9BB237939D977CDEE0E128C8C3A3300339BC3140146B7E14D3F92211ACFB7734AE604
B65EB12ED4CC91EACA75E8258F2C109830A6C2C3C2E1B929A0B546E44E0FBFA73D7E3
8F4B11BDEE4D7C345A8C1C1299E266C9C9F9A5D3752DA1A9906493095E96A7BE34D2D
7EAA06A1AF00843E2700C439E7CC4B387E0FF17317DC397697298448E8EA51D9D4208
C024DFD66017EB86C7E2E115E9739ED4BCD1A65A27D23AC1A864641BA3E1114956047
25FF58CC332D4AF961A52A51DE5FDEF8AE8DADE3DD4E132C2CB77A24FFABF7B5FB005
8567C5A4F799AB32D56011B407C260F62CBC824CBC61DD541C767962AF2B2CB3C0B54
865BD69ECED4D72A46157BB4941764E2D5A5DCE657351F8CFB97CF34AF4C70A2DD63E
1E0CAE4D43DDFC6161BC856951CBBD0D158968C669E0F5869127254CACFFFA3797D11
38AA177148E24962322E1D9E4488907FDD87C8C348C66A2F6525FBF4463FAE561A80C
3B96620F726AFE0E32FDD0012179C7B387A454D2CAAB45AF1C05E25E051DFD5D428D2
EB7AFB7F18608BA594212798C9BB10D17F5A9014F1AB23853C1790F688E5661669653
B12B85402EB78736F8297533D6B907939077754E2FDC0490DD856D541E5141D9C32C1
088E37891E531EF05C3F8E156C28365B3AADEBDC6

PRIVATE KEY:

```
235FD53C8C14D3DCA757301CCA8CDC64C519A4C3CEBD158D7B3A48037C4B771D6704B
6570444C52ABB35D8803ABEF1AA9BB50EA065C5139F7F91A0367634F079EEC24C46C0
6D2E61661ED08C63D98E7350281A818EA89E37DD028F88ECADA7866AA203230A29C3C
333D77EB1D2B01ED3208F749DAE758CCA266548DE1E2BEC4C7C68E7ED8E9591CCCC53
D2C74D0A242246D74CEF7CCDC502822D9681F04008402D2ED79CAB54D94003E861E57
EDD46C9C5E014AACE40EF104525B9D5206485ABEC96CBE72C4E34AB3E27B17E62A80F
04918ED186CE6C5C4588DF1C417D3A25704780BF0AC7A5A4149F0D308FAF4E8CA7101
47071A7C6891F44A224BB08DAD822CE351AF0EBC61CF0A3CFA10D183C8322E6BC0075
BA4A04876CBD7B08E75DE90DCDA5BD024502AEC5A86200964116C2A84C8322EC4285C
01B053765F28B099F4D94007FA1CE3DDF81E062A2D7CF7CCAB3B7CAF29B5B75678BC7
1EE0DC1056532A1EAE58ED63B3AB068ACD1F03E53C2CC0B5B7AC6E1204D29D887070A
C81A2375673135EE36835B24D336903263FE3A184746FAAA51B88C4E4E9608C54213B
C788CE90653DF2F2562791DFA6165D5C494AEDD61E40445E59C15F65CC94E698C39F4
F645807B8BDB6402B665655C0922E3B4282F16D4790B5AA1940AB15381404769BE724
5494CFA5CFB9194E889927D1A034E7E7607B53361B03908897B84AA26C6C4E81ACDF1
E78AA9679DED26A29DD7E44A99A22BC97E1D2D5E9F1A6D146716668014126B5076C56
53D4E3DB8023801D5D7DA2E8D0B2814F30160A4357DC2FB50AE41990447122A0B42AA
96AE6E1745B2109FF5DCA94053B6D1D52980C9281289C4610037683D8CCBAA7BB7CAB
486F16C580D8CDF212311EDB241D6E3E8D382F09198DD9C5275F4C515314BD303DE9C
8640F4C2EFCB638DFB9FF8BD09ABF81FA7274D256F7ABDAC636E44CD4E0E83C12DF88
D4AEA3E890CEC6B89D84F744098B3BF4E0600CB749FA882D664B553F5FCF61880A2EC
A8490EE3442FAA9E6533A3EF313C9D1E1902B2263E1378EA7111B0DF54F4F7EE07BA4
BBFB0A511B8E4FEF29C805E899D639A003E0D8B55E8F9E4405A412CF871A97EA4A3AD
FBDFC2D28711B767C234AEFA179CDB5F372A0BC592558019242E4E5CB68536AF1CE4D
7776EEEF2A6C978248968B4D245D9952D835AFE9E56274C42091672B8D17E538C47B0
FE7BDD0BEA6697AD484EBD4EFB0E946C3125784179C7656AE1F7D27AD83CC2D609B33
82B100911BA806CC68C115688F09C4383B40C91E9B2BDA08568C10F4B6DD006770E62
0F56A16F7B0FACCF02C41C8EFE88706DF3C2D8EB2FBACBB6102FB41A05532C6473F04
C1FB223E7B1BECD3A2403D88E48778C3E98077B14F30520F1DD1F80482EE5AB442FA7
64D7911953975B173097766F4B32024A3A6D375F8DB8D4918F40E2F24C1D55CF838CA
FE45B0A9A380E36B08EC2A5E8C756FD6F5AAC7D7CED7FBC43E8B439A1C5DE79007AF7
05CDB0DA44BDB9C39881BD8C05D36714532F614B40E69FE83B0D8500DEB2358AB7AF1
9711B4D7CCA9A543E8533554FA58A9DF2B67738D36AD0D38725AE1E96FBA45DFAB2A4
90E364743F2F6B98E9D581B580AA8FB764E90F9DF21329A42B0E16420CF1F6EE23DE7
D10B2DE8FBA1C831FDB2CA018E0F3E48C3808846283AAB2E1FBD9819BAF869308EEF7
A649A6105A07BD63B6EC42149598B40CB9DA77C51DE66C1AE126C6197FC239C42F0A8
2E31A386CDD203C0869C07A55437D551BBEAF874690411D414D884C0D4DA3693D3990
CE13405D2D31C95C0D3A7ACE8FF6DE39F07D6AC79078595DAE165C0DD17321615BC3F
17B81DCE8B7C9204CF88884328B6649AA924E5CA55664EAE6A61D9D42FEAA351FBAAB
E35268510E81E3BBCABAFF108B03B20D71000E3AD5009C5A5885F36CADF2F9666317A
B223F9EE746723A52A6A80382B7A84CF5F150008A0550DD249921C7A45656EE77A655
98627AF9B03EB6D9D0681849FBAA9674079A9DC5AEA1737B60AD8FA3035A1A1443202
1C2E060872B459556C9314A64C46289796DC09435B3CC8EA5D8CBF917721F6743F8BE
BE35EDEB8D4434E6A91F251F71773D723B52EE6442288C674E95925134709FAF31D42
B4C7A11483277EBAD215F46C7876753A4D7572C36C6A565B4116979AA84B5D15D321D
5FC729CE794028FFCE15C384A22FABE33F1314EAA1310DAF4B1F37C0A771EB817B0E6
3B58F62179BF4A74FEF5BB04124AC36B8225722317D080693C7F23D17A60D117883F4
DA9603DA73ADD80D91C1EA647526A4567744F543B51EDF10DA0367F2C452366FC14E1
```

A81CB00E61425905FEF907590F04C1074FA1E89BC530F7DFE3EACCDEC65A4AAD8E95F
046637B8E758B726596F26AFC101756E390CD33379AA90DADCC58B72716E8914E307F
BE9DE26F72D9905F409E5C44DC0CF9193B0108AF6E73B294C1DCFD8F0334176606568
D56E7E235A4A3E7FAE7B9E6A9833D46903BDB050B5A6A00D052381C621077B59284D3
52AD64C5C1D6D87CAC889053EF35B053EDAA0C22F7851A7171AC71DCB0949B53BE853
A76A1609B7E4DE9244A6DF11B9B77AF5AD69146F842C0D00C21444E4AA738AA0173DB
4370FD522BAEEB2E4093A8F1F1591B08F74745A3053922936FA345092C20DDC2529BC
6F00226EF51A81ADB5E6F0236B8FBCCC1A94BEF9956CFF08A4EDF7C489075CA2B66F8
E551CBA97A6578BB73F8F14F550217682D875E6FD825421D582EC9ED4287385008240
50DFB98F92266A3D89BE333417A553C46B9060E4DB050B9B1292A5597F36BF4A23085
B5C32862F0EEBA9FE66B342F9AB465BBB9C318F9942AD7D9126831AEB8A974C1E2869
E7E182D7864C36200207965D7300C45145EF330E1A4A01A7208666B1168079AA6F18A
7942D5A566FFEBEC9E9EFEEC33081700ECF55CE4A8F721E25414F02E2C06C354FDE32
D7554B617468CF4A7A0A55CE748409F677B96671031048FDF46FE30B6E3EDEEB3E190
681CF3ACC81C19DEC5066B3786600D8C9E08E18C1AC9D217C034574437B244CB88BBA
29E6D12FDB554DB0198BBA6E459B4435D6C03D0B3C757A860E6F082CC129B4C2AF22C
CF64FEF6044FE34B2D4E673B09F037247A32F34AEC08CCB26CAD2A939DB5A9667C6A9
EF167E6EB825BA0B1D50501F9E766A76298C28CBFD1784D2464966206AC3D8418D79A
7CD685A9724BCD19903390793BF872A7D0132ECFF72C536D35BC6BD060541325500BF
EE61FEDFDAECE683489F944BCE8AD4E540F0134FD9260F7201B1A16E0BA8109DD7EE2
5B4EFA167A8BC388B74F6739485465792EC3E0F9E397E42438716AD479CDB652C1CA3
2E68EAF0255463F60C31FF33AFC37FE2F46FB48C7A8152BBFE0DC735272838DE0B07F
6088B946FC330B7855E6E3467A2661BD3448E645C840B19A32676BA1F43910E99FA90
7476D4E3AA4F20B08FED77539BB3ABD437A409959A33880729102ACAA3A80D95B360A
15E7C7B3EBB9BA501D8C3CB2EA793E61EC478CB53BF9F46606356905D59025835CBC7
506EB8FE6B0E8AF9D98BEE4F0733B6DAF5616A4FD6AECE86C54069F774DEFE1333661
D4B511659EE8A499CBF1738B17A9B292BE4493043AE8B88B7470ECF833528932E8C4C
AF60935056FF9F838F7BB53F746F3078B54BBEC54E0964103A90105149868EAAF82E5
F31F222F07D1FE8C6086B1B10A685AD3D18B27283460D28AAB6DC3BCCB0AD7892CE3B
DA630DC932D906854C436BF1B3C2A0DF40F0BB8220D9F824D0C98287121AEB5D9F2A3
687283E736BD081D4E5763F259B896997A11F67342890B13809CCBD73FCB9387096FE
8E6A50E2D04E25ECCF6182F381A17A02499BBD7A53C63C94FF08E17700B4CF3DC8C55
9CC34A66C91CE1C966B8954F36B6A1466B5AB5E59E4901416CEEA67FB5A8FFB196811
0C8032048E1792CD105BD347D7A47A4F0B474BD467E4ACC7CC4C09E12EF78C51F985D
2744BBAC2058BAB4FF19B740BCF8D8489EFA78B2305230CFD9376C5FEB2FBE8E0B26C
00F6208965F081C4594633E424ED36C36BBCBA996EE1D5B3C82F040010602FCA90D31
BE969004FFAE3743878D985412067D22B055E8FFAC3A0E71302C6057777B0C2CD220D
A76F87EE0DF0CEDF7A7684FC7B6EB515D5AEF5EA290D976B16D8BD3E03CB805BF6293
C9D0B7D0F64881B10103D1C24791EEA8

R_(shared,3):

9FA869D385210DEB0BCF6FC1C2B313CA3F8BC7447583B7958D1BC101ED98DB48811BC
0D3EAE3089F12ACDB2C396CD79C206C5938E09951500268AECABC80EE6741C952EB18
AFDDBBE8D9A55F2E26929D814E54A3C4C46F1F13313AD66C0920D3D43AB3934B108E0
340DC4C4E3ABF942A324711B40329CEBFB02071C5B302CADC8973607635AFA7C04AEE
3EE63A73363C0413BAC55A2959C7CFF1A29F538B59DD3D7741C8D071EEA501861D00C
BEAD74069860564087BA440A8AFA095F1E2022C5C392B741D9220654C2E337AAD70B3
B907611E7C9B704B90AC1B8849CCA87AC3E2DF83F1CF3D540DAB2DCE7553EE293725D
DF1CB8E29B5CEC1EDF1837CBB48AC156639E85F5FDEBC47CFC555DDABEABE8DBF07

M_(shared,3):

6B12B7314183E522D084564CA595ABDBA90488458E28C595802121321570A6CA34B24
32A8B0F66B5A3C13886604213E9BA38870D0067B12F600C5546563AD0370A040C9CA4
7165563592F0996C93721256E268E340C78FE37BB8C203806333A824877E855DC2857
3C0D15F86817CF0ED908C19B55FE1E1BA1D76DD16C38B3BCC97C98D8F0A57E66AC79E
42497FE761E126ABE1B80886053CD20F5DD3CE6AD9E78D4E6326E9A24ADDE2ABA82C7
61BD02F0793292FA195AFAD340C53E06DB3AA1330B8404B5422ECC857235ED824CA2F
24C0696CB859AB0CDF62051CE5CF5E981BA0F11109440C9A63C240B3AA269507ED4AA
135AB612217EAE241A041690B1D8C679CD251030275E6BCD549488545B189617C05

CIPHER TEXT:

51F896A35A9D3F34D7FD83BBA529FF526375C7B1E441F766C0AA9BFB8203B1BA51EE2
64D09391B1B2A4BC15678BC421E5545E8789A690730B4C7284B1475ECA88CF9C36222
6FE500A2B07727EA2C1FAA1FF216DAF1B1847219D37E4AB42AADF59DE63E1FA01F50A
61A4DE3C60CB73AE0C12FEC80EAA0A5DD891CF18D4E5C720747DF7A40B69C1DE6B031
3CFFADDD0CF9227748E4269F66044B2A65833D3B1015C0F9D195DE1B2F4DA8D6E5782
3C9FE6A7847CFB2B78A385481F6C0DD276411AD12D9C7BC394513B6BBA962596A375E
EAA7E3BA8761631B9C16B743062F31A41423E4DE32DB2E4423A13FF19B1283476AC7D
15F529C65B7651532AAC7A89367CAD29497628EFB7B51A8AB0D1D10D3582DEF6E1412
CA2E35A41B576CE26023BD03574570DFC80F0E3333EFD4D1AF29D0CC3C7C29FCE5485
FEACBFA2B57B8BE42D5AD4E7443E5230454BDED912620C6C4A053A37F60508CD6004E
B9B1C8456E83EC612F6D86DC8B1CE4D2998A087CFF2D79F76B61F90D52B1B06FB4CE9
09C3D4736CCD452F374963D87F6AE77FB87A1E54153E042B1BC9EBEF62D38905FEEEC
9AE3AC671A4BD939CC414614056EA7B5F722080FEED8CF37E9CA6F74AA692968EFFA3
5EAD6BAD22B8F4348EEE81140B52D368B45D19CC6E4B17B83A3FB3B0431B56D0B5A1E
D7236FD5B16A7C6DF0FDC59501CF80178C5C7A6F6FF8542679796C3BE4C4C4EA56F7F
D23EDE679EBE797D171784F2FE9E560BFCA2B417A373C01901B4568103C63C9004ED8
EDF05D2A528BF835D9C584AA6B3567B9E8BE18A80BDFFA797C09A744C7288702F9AD9
528E15B4DFCF6D7BE27B8A887B7587C0D2838FFBF5E7AF55ED52343D0FE118D4947F4
8C00888895147D9F91E2350BD36FD22704CB9BEB7657AC4121570AE16EEBB5CB15177
FCE2CACA4E049088AF5BAA7D1EAAA3C0B5E2CE9CF3520EDBE46DBD9B6E66C0B094795
556C3AAD046E884415C38BBC6A18D152217AD897261052160ED7671C0E02151A4E346
06E8956E5F50442892CDEECDB5CFBD94AF571667443F6251E3BA343913C14CC855578
2B1A2233C0586D7389F54C1A36BD3D0F92FA27C00BC7DD8935397F5794867C49536DE
3FB3E614AA380AB534589C19327A0629B0920B0C4FC17187FE2ACB592821AD43B78E9
8A544CC88A58CD193260EF2D0960A5C00C5FBCBD7146D9794803AF0D12265409C5BF4
E89E70024045256368C9B7D04D05CF446075BDB9AD96864A8D14DC5B0B622975CB8AE

FD06C2A1E8E65BEB076B580A016390811D7DF180C7DC1590A5154561889365EDB40CD
0027C064F6F8499F1F7B3E1496064519FCAFA6D6A47B4823EDE1DAC4092762A9BEA91
99207B026778F4638607CE8DC1301A16415AD6425473D7862AA78AD3227B4D48B45DA
12D637E4EA29826BE8767E3EEF76026DACC54308D19BC9F60B8A0FF834EC410C52C74
AA7091ACE45281A74F90F0B50AE5B09FC69C3DECEE7D213128B3C4DA5879BC95CA1FA
B69010F370D26253D72B95890AD703F41A9AF89B84811A99392D5B9410FB310DF0B21
6BB22C241B5F460F1853333FF66A63E8FE5F11386B8CEB78DE67DA2B6BE59FD4467D2
C9F7C018FDDEA52354D2833FAD0F42EB105EE9734A5BE8B4C5EBBA027EB3282C94713
EB6A111391736AF11C11CB5223C561CA02E335DA0E76C08531D1EB4EFC74C5452B56C
972AB2FBCD5E32F19D4DE8B69A0D6E5DD31F504BA7F4CF74B13FE5D1BD98EAFF7431F
5116047C179041EB7E908F8911B37E9269F4A648EFEBF3FF9137F953F84F469C30B49
BEAD19397883B028BD3461E0A6FE69F907E8DA455DBBB24F6354BA5DCB46E1C52EE44
F5E6BBBBDE9C41D423F5FAEDA589D934A404C1BBD0B403674485D90AB2F03E2CF31B8
4AE62C3BFBCD4956A91D0E988FCCF64CFC81CD21169ADF3334E47AAC5D5DB8B37DF5A
E11C3A3D6112AA896C6A31EB8C00746DD3D06101E0F2D1C73A98112C9650875BDC655
E72260C33424B534C0C7100CE0382E42F3C011FB9BB969645431D1F0C4DD03CCAAE23
3E9B164F9A0F2764C1D077D651F23FFE5FF83B674A7FC6968673475C46759189DE45A
D4C1E9ED246C70592702C50B07CD2698E2F6B2A6CABA527E89B261C3454B4C21A6A79
C87F6EA073B42A2BCC4BCB9006E9C79CFC942DA8960986A90E0EF590AAE990B1ADD03
2C706DEF43E4C4BCAB63661DD67DC14AAB30AE9744FE6B8CABB622E77AA6D131FBD6D
7A37D363B519C5C65A5A5E02C8DF9E4C24FF2873CA1C7036BB9E531601CE4111239B3
3C37E7D989AD69A384C48400B2AD2C91284008794C8A100D4B8E9D8492C4AAD0CF8CA
26735D863BB25EEB30B631CE7189CDF1797B07B52A39135A3A6DB44F935E742B50899
57F5384797C084ED3C3F51F851951911983ED893AAE6DDEC8930ED7544A7DED458739
FE81F1019A6ADE2A1E0DEC992E99DA20076613E9F3A1BB9CC0D8E08E0D1A82A4FE90F
BC83905A19C4F7C1ADC9EB114C70065A7838A45230761E156C2C7C96D763431652D94
8FC0688F3991DEDFE6EC1CEA38EA96E880E98C19412096177E2F29D5F10170CBFB9AC
418E85ACFC06D78C26BB4E751E8C38E55ACAD771413A361B31E42FE9D4708A3E0AF92
9D3BD459FCA24FFC227DC8717F089DF1DC03848949D5B82D8CA687E8C223361916C4F
FE452488A231F00F4966D63835C4E36E36AFBBD28C3EEFA9C8B46E1F3ED409E132610
F2CE7584D37F77195AAB73C045F1673DB8571D4EA2AB71086EA0CA31AB03E2051C47D
75039D3AE2EBBB62E97ADEF2E0CD193B2B336D8B832C1309C0D52BC1D4D03F19D5960
643841B0F023F08FA694AC2BA81E6367395B9ADC829E4E4A20D0AA232B474859B3DEA
F0D79C0479FCA489510571025B4FA0AF2580DBF2000A02D054C76ACB3D91044F227F8
D33C7AE358463A2E1C237C7C6EFAFE45EFFAB3217560C3F0E7425414530E69A848C51
92904749D89B1B0DA16267908048F4867A05A74D6882E50FB41DC134C4157CCA2F818
2C33376CC170BE497F5715632728466AC5F96C5A7D1697E9F093D8D50CB47C1730921
8DC37DBCC66E57F43F7296BF76684758BB1103C69CC593BB3108D7B4BE4C309BD9329
CE38076C822E7DF79065BCC6F168D7CB882EBDF61EAA50A5CC760B0670F6144058257
82014F774B6AA826814ADB00CE2C0371CF566E3DF27052EE5F632FE22BE6C91445F5F
C1AD0D332C08A0358A60980C0E63716BA8BB91BA005185BE6F22EE28ACC78EBF0BEA7
6DB5876EEF79F5EB3F506588BD3900F5E04B0201240237FE85E226592279C48066CA6
97D0253586B112C75ED81CE2A917FB4FBD72F0D1F3F1EC7A44AA2883BEA3A92E96915
0BBDB61EF05104C80BE0961E665BEA3461BD03A68

SECRET STRING:

BD49CC3E69BFD304E21D4D57B36BB6554A48EDC8117A955CEB0C0F6A00EADF2C

## 10. Security Considerations

Current best practices should be followed, especially regarding known plaintext attacks, such as Meet-In-The-Middle (MITM), and known ciphertext attacks.

Lattice reductions via Lenstra-Lenstra-Lovasz may be possible against NTRU with weak parameter set selection.

### 10.1. Parameter set security

In all parameter sets, indistinguishability under adaptive chosen ciphertext attack (IND-CCA2) is a desired property.

Equivalent bit strengths of the described parameter sets are outlined in the table below:

| Parameter Set | Security Model | Bit Strength |
|---|---|---|
| ntruhps2048677 | IND-CCA2 | 128 |
| ntruhps4096821 | IND-CCA2 | 192 |
| ntruhps40961229 | IND-CCA2 | 256 |
| ntruhrss701 | IND-CCA2 | 128 |
| ntruhrss1373 | IND-CCA2 | 256 |

Table 5

### 10.2. Public key reuse

NTRU public/private keys can be safely reused for certain use cases. Reusing an NTRU key may be tempting, because the NTRU key generation process is considerably more costly than the key encapsulation or decapsulation operations. On the other hand, if you do reuse NTRU keys, you lose the Perfect Forward Secrecy property. That is, as long as you don’t zeroization the NTRU private key, then an attacker that can break into the system can extract that private key, and then recover any symmetric keys that were negotiated with that private key.

If keys are reused, key revocation mechanisms should be considered.

## 11. IANA Considerations

This document has no IANA actions.

## 12. Open Questions

* We don’t specify a flattened format for a private key. In my view, there is no need; systems will generally use ephemeral public/private key pairs, that is, create them on the fly, use them for one or a handful of exchanges and then throw them away. In this use case, there is no need to transfer a private key to another device. Now, it is possible for NTRU to be used with static keys - should we try to address that case?

* There is a tiny chance of failure during key generation (if F happens to be selected as all 0); this happens with probability < 2^-800 (that is, it’ll never happen in practice, unless the random number generator broke). When this happens, the computation of the inverse of F will fail; what happens in that case would depend on the inverter implementation. Should we ignore it or address it?

## 13. References

### 13.1. Normative References

[CDHH19] Chen, C., Danba, O., Hoffstein, J., Hlsing, A., Rijneveld, J., Schanck, J.M., Saito, T., Schwabe, P., Whyte, W., Xagawa, K., Yamakawa, T., and Z. Zhang, "NTRU: algorithm specifications and supporting documentation", 2019, <https://ntru.org/release/NIST-PQ-Submission-NTRU-20201016.tar.gz>.

[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/info/rfc2119>.

### 13.2. Informative References

[FO99] Fujisaki, E. and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", August 1999. In Annual international cryptology conference (pp. 537-554)

[HPS98] Hoffstein, J., Piper, J., and J.H. Silverman, "NTRU: A ring-based public key cryptosystem", June 1998. In Joe P. Buhler, editor, Algorithmic Number Theory - ANTS-III, volume 1423 of LNCS, pages 267-288. Springer, 1998

[HRSS17] Hlsing, A., Rijneveld, J., Schanck, J., and P. Schwabe, "High-speed key encapsulation from NTRU", August 2017. In: Fischer, W., Homma, N. (eds) Cryptographic Hardware and Embedded Systems CHES 2017. CHES 2017. Lecture Notes in Computer Science(), vol 10529. Springer, Cham.

[K1981v2] Knuth, D. E., "The Art of Computer Programming, Vol. 2: Seminumerical Algorithms", 1981.

[SXY18] Saito, T., Xagawa, K., and T. Yamakawa, "Tightly-secure key-encapsulation mechanism in the quantum random oracle model.", 2018. In Advances in CryptologyEUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part III 37 (pp. 520-551)

## Appendix A. Acknowledgments

Acknowledge TBD.

## Authors' Addresses

Scott Fluhrer
Cisco Systems
Email: sfluhrer@cisco.com

Michael Prorock
mesur.io
Email: mprorock@mesur.io

Sofia Celi
Brave
Email: cherenkov@riseup.net

John Gray
Entrust
Email: john.gray@entrust.com

Xagawa Keita
TII
Email: xagawa@gmail.com

Kosuge Haruhisa
NTT
Email: hrhs.kosuge@ntt.com