INTERNATIONAL STANDARD

ISO/IEC 11770-4

Second edition
2017-11

AMENDMENT 2
2021-02

Information technology — Security techniques — Key management —

Part 4: Mechanisms based on weak secrets

AMENDMENT 2: Leakage-resilient password-authenticated key agreement with additional stored secrets

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 4: Mécanismes basés sur des secrets faibles

AMENDEMENT 2

Reference number
ISO/IEC 11770-4:2017/Amd.2:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 11770 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Information technology — Security techniques — Key management —

Part 4:
Mechanisms based on weak secrets

AMENDMENT 2: Leakage-resilient password-authenticated key agreement with additional stored secrets

Introduction

Insert new list item e) as follows:

e) **Leakage-resilient password-authenticated key agreement with additional stored secrets:** Establish one or more shared secret keys between two entities *A* and *B*, where *A* has a weak secret and a (possibly, insecure) stored secret that might be revealed to or altered by adversaries and *B* has verification data derived from *A*'s weak secret and stored secret. In a leakage-resilient password-authenticated key agreement with additional stored secrets mechanism, the shared secret keys are the result of a data exchange between the two entities; the shared secret keys are established if, and only if, the two entities have used the weak secret, the stored secret and the corresponding verification data; and *A*, *B* and an adversary who has obtained and altered the stored secret are all unable to predetermine the values of the shared secret keys.

NOTE 4 Here, "leakage-resilience" means security against either compromise of stored secrets held by client *A* or compromise of verification data held by server *B*, but not both. This type of key agreement mechanism is able to protect *A*'s weak secret from being discovered by *B*, as well as preventing an adversary from getting *A*'s weak secret from *B*. Also, this type of key agreement mechanism prevents an adversary from performing online dictionary attacks unless the adversary obtains *A*'s stored secret. In other words, an adversary who obtains *A*'s stored secret is restricted to performing online dictionary attacks, and the security level in this case is the same as that of the other mechanisms in this document. A typical application scenario would involve use between a client (*A*) and a server (*B*), where a client user employs a portable device such as a smart phone, USB memory or smart card to save the user's stored secret, or where a client terminal shares a network-attached storage device in an office environment.

Clause 2

Replace Clause 2 with the following:

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 29192-5, *Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions*

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO/IEC 29192-6, *IT Security techniques — Lightweight cryptography — Part 6: Message Authentication Codes (MACs)*

ISO/IEC 11770-6, *Information technology — Security techniques — Key management — Part 6: Key derivation*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 19772, *Information technology — Security techniques — Authenticated encryption*

Clause 3

Insert new term 3.40 as follows:

3.40
Hamming weight
number of non-zero elements in a bit string

Clause 4

Replace definitions as follows:

H	a collision-resistant hash-function taking an octet string as input and giving a bit string as output. One of the hash-functions specified in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5 shall be used
$h(x, L_K)$	a collision-resistant hash-function taking an octet string x and an integer L_K as input and giving a bit string of length L_K (in bits) as output. One of the hash-functions specified in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5 shall be used
$mac(k, m)$	a message authentication code (MAC) function taking a key k and a variable-length message m as input and giving a fixed-length output. One of the MAC algorithms specified in ISO/IEC 9797 (all parts) or ISO/IEC 29192-6 shall be used
G, G_a, G_b	points of order r on E over $F(q)$, where the relative discrete logarithms of G, G_a, G_b are unknown
g, g_1, g_a, g_b	elements of multiplicative order r in $F(q)$, where the relative discrete logarithms of g, g_1, g_a, g_b are unknown
K	a function for deriving a key from a secret value and a key derivation parameter. One of the key derivation functions specified in ISO/IEC 11770-6 shall be used

Add the following definitions:

$\oplus$	bit-wise exclusive-or operation on bit-strings of equal length
AE	an authenticated encryption, (reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. that provides data confidentiality, data integrity, and data origin authentication. One of the authenticated encryption methods specified in ISO/IEC 19772 shall be used

Clause 5

Replace the last sentence with the following:

It is also assumed that the entities are aware of a common hash-function *H*, one of the hash-functions specified in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5.

Clause 9

Add new Clause 9 as follows:

9 Leakage-resilient password-authenticated key agreement with additional stored secrets

9.1 General

This clause specifies two mechanisms (LKAM1 and LKAM2) for leakage-resilient password-authenticated key agreement with additional stored secrets. These mechanisms, specified in 9.2 and 9.3, require one of the two entities to possess verification data for a weak secret and a stored secret known to the other entity.

The two mechanisms share the following initialization and key establishment processes.

Initialization process: The two entities involved agree to use a set of valid domain parameters, a set of key derivation parameters and a set of functions, all of which may be publicly known. The two entities also agree to use shared password-based information, i.e. one entity has a password-based weak secret and a stored secret, and the other entity has the corresponding verification data.

NOTE In the initialization process, the two entities who only share password-based information can establish a secure channel by performing the key establishment process. In the case of LKAM2, the server first sends an RSA parameter *n*. Through the established secure channel, the two entities can register verification data and stored secrets.

Key establishment process:

a) *Generate and exchange key tokens.* The two entities involved each randomly choose one or more key token factors associated with the domain parameters, create the corresponding key tokens, which may be associated with the password and the stored secret or verification data (a key token associated with the password and the stored secret or verification data is called an "entangled key token"), and then make the key tokens available to the other entity.

b) *Check validity of key tokens.* Depending on the operations for producing key tokens in step a), the two entities involved each choose an appropriate method to validate the received key tokens based on the domain parameters. If any validation fails, the entity involved shall output "invalid" and stop.

c) *Derive shared secret keys.* The two entities involved each apply certain secret value derivation functions to their own key token factor, the other entity's key tokens and/or shared verification data to produce a shared secret value. Each entity further applies a key derivation function to the shared secret value and the key derivation parameters, to derive one or more shared secret keys.

d) *Check key confirmation and update stored secrets.* The two entities involved use the shared secret keys established using the above steps to confirm their awareness of the keys to each other, and to update their stored secrets. This step is mandatory.

9.2 Leakage-resilient key agreement mechanism 1 (LKAM1)

9.2.1 General

This mechanism is designed to achieve leakage-resilient password-authenticated key agreement with additional stored secrets, and establishes one or more shared secret keys between entities A and B. In the mechanism, A has a password-based octet string π and a stored secret s_i, and B has verification data W_i corresponding to π and s_i. This mechanism provides unilateral explicit key authentication and, optionally, mutual key authentication.

This mechanism works in both the DL setting and the EC setting.

NOTE 1 In applications using leakage-resilient password-authenticated key agreement with additional stored secrets, A can play the role of a client and B can play the role of a server.

NOTE 2 This mechanism is based on the work of Shin, Kobara and Imai[35].

9.2.2 Prior shared parameters

Key agreement between two entities A and B takes place in an environment consisting of the following parameters:

— a set of valid domain parameters (either DL domain parameters or EC domain parameters) as specified in Clause 5;

— a counter which stores the value of i (initially $i = 1$);

— the length L_K of a shared secret key K;

— a password-based octet string π and a stored secret s_i, which is an integer of L_K bits used by A;

— a verification element derivation function J, used by A;

— a verification element $W_i = J(\pi, s_i)$, used by A and B;

— a key token generation function D, used by A and B;

— an entangled key token generation function C, used by A;

— a key token check function T, used by A and B;

— two secret value derivation functions V_A and V_B, one for each entity;

— a key derivation function K, used by A and B;

— one or more key derivation parameter octet strings $\{P_1, P_2, ...\}$, where A and B shall agree to use the same values.

9.2.3 Functions

9.2.3.1 Verification element derivation function *J*

The verification element derivation function J takes a password-based octet string π and a stored secret s_i as input and produces an element of $F(q)$, written $J(\pi, s_i)$, as output. Leakage-resilient key agreement mechanism 1 can be used with either of the following two functions J_{DL} and J_{EC}:

— J_{DL} is suitable for use when the mechanism is used with the DL domain parameters, i.e. it operates over the multiplicative group of elements of $F(q)$. Given the DL domain parameters (including g_b and q), a password-based octet string π and a stored secret s_i, J_{DL} is defined as in Formula (40):

$$J_{DL}(\pi, s_i) = g_b^{\text{BS2I}(H(\pi))+s_i \bmod r} \bmod q \quad (40)$$

— J_{EC} is suitable for use when the mechanism is used with the EC domain parameters, i.e. it operates over the additive group of elements in an elliptic curve of $F(q)$. Given the EC domain parameters (including G_b), a password-based octet string π and a stored secret s_i, J_{EC} is defined as in Formula (41):

$$J_{EC}(\pi, s_i) = [\text{BS2I}(H(\pi)) + s_i \bmod r] \times G_b \quad (41)$$

Function BS2I (Bit String to Integer conversion) is described in Annex A.

9.2.3.2 Key token generation function *D*

The key token generation function D takes an integer x from {1, ..., r − 1} as input and produces an element written $D(x)$ as output. Leakage-resilient key agreement mechanism 1 can be used with either of the following two functions D_{DL} and D_{EC}:

— D_{DL} is suitable for use when the mechanism is used with the DL domain parameters, i.e. it operates over the multiplicative group of elements of $F(q)$. Given the DL domain parameters (including g and q) and an input x from {1, ..., r − 1}, D_{DL} is defined as in Formula (42):

$$D_{DL}(x) = g^x \bmod q \quad (42)$$

— D_{EC} is suitable for use when the mechanism is used with the EC domain parameters, i.e. it operates over the additive group of elements in an elliptic curve of $F(q)$. Given the EC domain parameters (including G) and an input x from {1, ..., r − 1}, D_{EC} is defined as in Formula (43):

$$D_{EC}(x) = [x] \times G \quad (43)$$

9.2.3.3 Entangled key token generation function *C*

The entangled key token generation function C takes two inputs, an output W_i of function J and an output X of function D, and produces an element written $C(W_i, X)$ as output. Leakage-resilient key agreement mechanism 1 can be used with either of the following C functions C_{DL} and C_{EC}:

— C_{DL} is suitable for use when the mechanism is used with the DL domain parameters, i.e. it operates over the multiplicative group of elements of $F(q)$. Given the DL domain parameters (including q) and two inputs, the output W_i of function J and the output X of function D, C_{DL} is defined as follows:

  — compute $C_{DL}(W_i, X) = W_i \times X \bmod q$;

  — if $C_{DL}(W_i, X)$ is 0, 1 or q − 1, output "invalid" and stop; otherwise, output $C_{DL}(W_i, X)$.

— C_{EC} is suitable for use when the mechanism is used with the EC domain parameters, i.e. it operates over the additive group of elements in an elliptic curve of $F(q)$. Given the EC domain parameters and two inputs, the output W_i of function J and the output X of function D, C_{EC} is defined as follows:

  — compute $C_{EC}(W_i, X) = W_i + X$;

  — if $[2^n] \times C_{EC}(W_i, X) = 0_E$, output "invalid" and stop; otherwise output $C_{EC}(W_i, X)$.

9.2.3.4 Key token check function *T*

The key token check function T is the same as that defined in 6.2.3.3.

9.2.3.5 Secret value derivation functions V_A and V_B

a) The secret value derivation function V_A takes two inputs, an integer x from {1, ..., r − 1} and an output Y of function D, and produces an element written $V_A(x, Y)$ as output.

b) The secret value derivation function V_B takes three inputs, an integer y from {1, ..., r − 1}, an output X' of function C and an output W_i of function J, and produces an element written $V_B(y, X', W_i)$ as output.

c) V_A and V_B satisfy the condition $V_A(x, Y) = V_B(y, X', W_i)$.

Leakage-resilient key agreement mechanism 1 can be used with either of the following two functions V_{ADL} and V_{AEC}, and either of the following two functions V_{BDL} and V_{BEC}:

a) V_{ADL} is suitable for use when the mechanism is used with the DL domain parameters, i.e. it operates over the multiplicative group of $F(q)$. Given the DL domain parameters (including q), an integer x from {1, ..., r − 1} and an integer Y from {2, ..., q − 2}, V_{ADL} is defined in the following steps:

   — compute $V_{ADL}(x, Y) = Y^x \bmod q$;

   — output $V_{ADL}(x, Y)$.

b) V_{BDL} is suitable for use when the mechanism is used with the DL domain parameters, i.e. it operates over the multiplicative group of $F(q)$. Given the DL domain parameters (including q), an integer y from {1, ..., r − 1}, an integer X' from {2, ..., q − 2} and an integer W_i from {2, ..., q − 2}, V_{BDL} is defined in the following steps:

   — compute $V_{BDL}(y, X', W_i) = (X' / W_i)^y \bmod q$;

   — output $V_{BDL}(y, X', W_i)$.

c) V_{AEC} is suitable for use when the mechanism is used with the EC domain parameters, i.e. it operates over the additive group of elements in an elliptic curve of $F(q)$. Given the EC domain parameters, an integer x from {1, ..., r − 1} and a point $Y(\neq 0_E)$ on E, V_{AEC} is defined in the following steps:

   — compute $V_{AEC}(x, Y) = [x] \times Y$;

   — output $V_{AEC}(x, Y)$.

d) V_{BEC} is suitable for use when the mechanism is used with the EC domain parameters, i.e. it operates over the additive group of elements in an elliptic curve of $F(q)$. Given the EC domain parameters, an integer y from {1, ..., r − 1}, a point $X'(\neq 0_E)$ on E and a point $W_i(\neq 0_E)$ on E, V_{BEC} is defined in the following steps:

   — compute $V_{BEC}(y, X', W_i) = [y] \times (X' - W_i)$;

   — output $V_{BEC}(y, X', W_i)$.

9.2.3.6 Key derivation function *K*

The key derivation function K is the same as that defined in 6.2.3.6.

9.2.4 Initialization operation

In the initialization operation, A chooses an integer s_1 randomly from {1, ..., r − 1}, computes $W_1 = J(\pi, s_1)$, and then securely transfers W_1 to B. While A has the password-based weak secret π and the stored secret s_1 (along with the counter $i = 1$), B has the corresponding verification data W_1 and the counter $i = 1$.

NOTE Entity A can update the password-based weak secret by performing the initialization operation.

9.2.5 Key agreement operation

In the i-th ($i \geq 1$) key agreement operation, this mechanism involves both A and B performing a sequence of up to three steps, numbered A1 to A3 and B1 to B3 (for the steps to be followed by A and B, respectively).

a) Entangled key token construction (A1)

A performs the following steps:

1) compute $W_i = J(\pi, s_i)$ as its verification element;

2) choose an integer x randomly from $\{1, \ldots, r-1\}$ as its key token factor;

3) compute $X = D(x)$ as its key token, and $X' = C(W_i, X)$ as its entangled key token (if the output of function C is "invalid", go back to the above item to choose a different x value at random and try again);

4) make i and X' available to B.

b) Key token construction (B1)

B performs the following steps:

1) receive i and X' from A;

2) check the validity of i: if the received value of i is not the same as the value B has, output "invalid" and stop; otherwise, continue;

3) check the validity of X' using $T(X')$: if $T(X') = 0$, output "invalid" and stop; otherwise, continue;

4) choose an integer y uniformly at random from the range $\{1, \ldots, r-1\}$ as its key token factor;

5) compute $Y = D(y)$ as its key token;

6) compute $z = V_B(y, X', W_i)$ as an agreed secret value;

7) compute $o_B = H(\mathrm{I2OS}(1)||A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z))$;

8) make Y and o_B available to A.

c) Key confirmation (mandatory) and shared secret key derivation (A2)

A performs the following steps:

1) receive Y and o_B from B;

2) check the validity of Y using $T(Y)$: if $T(Y) = 0$, output "invalid" and stop; otherwise, continue;

3) compute $z = V_A(x, Y)$ as an agreed secret value;

4) compute $o_B' = H(\mathrm{I2OS}(1)||A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z))$;

5) if $o_B \neq o_B'$, output "invalid" and stop; otherwise, continue;

6) compute $o_A = H(\mathrm{I2OS}(2)||A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z))$;

7) compute $K_j = K(A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z), P_j, L_K)$ as a shared secret key for each key derivation parameter P_j ($j = 1, 2, \ldots$);

8) make o_A available to B.

d) Key confirmation and shared secret key derivation (B2)

B performs the following steps:

1) receive o_A from A;

2) compute $o_A' = H(\mathrm{I2OS}(2)||A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z))$;

3) if $o_A \neq o_A'$, output "invalid" and stop; otherwise, continue;

4) compute $K_j = K(A||B||\mathrm{I2OS}(i)||\mathrm{GE2OS}_X(X')||\ \mathrm{GE2OS}_X(Y)||\ \mathrm{GE2OS}_X(W_i)||\ \mathrm{GE2OS}_X(z), P_j, L_K)$ as a shared secret key for each key derivation parameter P_j ($j = 1, 2, \ldots$).

e) Update of stored secrets (A3 and B3)

A performs the following step (A3):

1) compute $s_{(i+1)} = s_i + \text{BS2I}(H(\text{I2OS}(3)||A||B||\text{I2OS}(i)||\text{GE2OS}_X(X')||\ \text{GE2OS}_X(Y)||\ \text{GE2OS}_X(W_i)||\ \text{GE2OS}_X(z))) \bmod r$.

B performs the following step (B3):

1) compute $u = \text{BS2I}(H(\text{I2OS}(3)||A||B||\text{I2OS}(i)||\text{GE2OS}_X(X')||\ \text{GE2OS}_X(Y)||\ \text{GE2OS}_X(W_i)||\ \text{GE2OS}_X(z))) \bmod r$;

2) compute $W_{(i+1)} = W_i \times (g_b)^u \bmod q$ in the DL setting;

3) compute $W_{(i+1)} = W_i + [u] \times G_b$ in the EC setting;

4) check the validity of $W_{(i+1)}$ using $T(W_{(i+1)})$: if $T(W_{(i+1)}) = 0$, output "invalid" and stop.

Entity *A* shall verify the entity *B*'s proof of knowledge of the agreed key before revealing any information derived from the agreed key. Therefore, A2 shall be done before B2 if the latter is performed.

Functions BS2I (Bit String to Integer conversion), I2OS (Integer to Octet String conversion) and GE2OS_X (Group Element to Octet String conversion) are described in Annex A where Annex A shall be referenced for the details of the conversion functions.

Numerical examples can be found in D.1.

NOTE 1 A group element in this mechanism is a point on the curve *E* in the EC setting, or an integer in the range $\{1, ..., q - 1\}$ in the DL setting.

NOTE 2 In this mechanism, *X* and *Y* can be computed before the key agreement operation.

NOTE 3 This mechanism can be extended to provide synchronization, randomized ID and security against server compromise impersonation attacks in the same way as in Section 6 of Reference [36].

9.3 Leakage-resilient key agreement mechanism 2 (LKAM2)

9.3.1 General

This mechanism is designed to achieve leakage-resilient authenticated key agreement with password and untrusted storage using the RSA public key cryptosystem and establishes one or more shared secret keys between entities *A* and *B* with joint key control. In the mechanism, *A* remembers a password (denoted by π when rendered as an octet string), and has, in an untrusted storage device that might be modified or copied by adversaries to impersonate *A* or *B* or to reveal the agreed keys, the RSA parameter *n*, a stored secret u_j where subscript *j* denotes a counter and a random pseudo identity A' of *A*. *B* has password verification data v_j corresponding to both π and u_j, a hash value A'' of A', and RSA private key parameters *d*, *p*, *q* and so on. These RSA private and public key parameters shall be generated using ISO/IEC 18033-2:2006, 11.1, and the additional requirement and recommendations for *e* to be used in this mechanism are explained in 9.3.3. This mechanism provides unilateral explicit key authentication, and optionally mutual key authentication.

NOTE 1 In applications using leakage-resilient authenticated key agreement with password and untrusted storage, *A* can play the role of a client and *B* can play the role of a server.

NOTE 2 This mechanism is based on the work of Shin, Kobara and Imai[36].

9.3.2 Prior shared parameters

Key agreement between two entities *A* and *B* takes place in an environment consisting of the following parameters, in which L_K, *e*, *H*, *mac*, *K*, $\{P_1, P_2, ...\}$ are shared as system parameters among all or a subset of the users of this mechanism:

— the length of a shared secret key L_K which must be a multiple of 8;

— a set of RSA public key parameters, namely a prime integer e and a composite number n generated as specified in ISO/IEC 18033-2:2006, 11.1, where e is specialized for this mechanism as explained in 9.3.3;

— a cryptographic collision-resistant hash-function H giving a $2L_K$-bit output, that shall be chosen from amongst the functions standardized in ISO/IEC 10118 (all parts) or ISO/IEC 29192-5, being truncated as necessary;

— a message authentication code generation function *mac*, that shall be chosen from amongst the functions standardized in ISO/IEC 9797 (all parts) or ISO/IEC 29192-6;

— a counter which stores the value of j (initially j =1);

— a stored secret u_j and corresponding $v_j = J(\pi, u_j)$ where u_j is an octet string of random L_K bits and J is a password verification element derivation function in 9.3.4.1. Both u_j and v_j are set in the initialization operation in 9.3.5, and then used by A and B, respectively;

— a pseudo identity A'_j and a corresponding hash value $A''_j = H(\text{I2OS}(0)||A'_j)$ of the entity A, where A'_j is an octet string of length $L_K/8$ whose constituent bits are generated uniformly at random. Both A'_j and A''_j are set in the initialization operation in 9.3.5 and used by A and B, respectively;

— a key derivation function K, that shall be chosen from amongst the functions standardized in ISO/IEC 11770-6;

— one or more key derivation parameter octet strings $\{P_1, P_2, ...\}$, where A and B shall agree to use the same values.

9.3.3 Additional requirement and recommendations for RSA public key parameter *e*

The following requirements on the choice of the parameter e, additional to those specified in ISO/IEC 18033-2:2006, 11.1, apply.

a) e shall be a prime and $e \geq 2^{L_K}$;

b) the sum of the Hamming weight of the binary representation of e and the bit-length of e should be as small as possible, subject to requirement a);

c) e should be as large as possible within b).

NOTE 1 Requirement a) ensures that the e-residue attack[36], which applies when an adversary can modify the parameter n, is not feasible.

NOTE 2 Recommendation b) is intended to help minimize the computational cost for entity A.

NOTE 3 Recommendation c) is intended to make e-residue attacks as difficult as possible for a given computational cost on A.

NOTE 4 Examples of choices for e satisfying requirement a)-c) are given in C.4.

9.3.4 Functions

9.3.4.1 Password verification element derivation function *J*

The password verification element derivation function J takes a password-based octet string π and a random L_K-bit stored secret u_j as input, and produces as output an octet string password verification data $v_j = H(\text{I2OS}(4)||\pi||A||B) \oplus u_j$.

9.3.4.2 Key token generation function *D*

The key token generation function D takes password verification data v_j, RSA public parameters n, e and integers x_1, x_2 in {1, …, n − 1} as input, and produces as output $Z = D(e, n, x_1, x_2, v_j)$, an integer in the range {0, …, n − 2}. D is calculated as follows:

— compute $y_1 = (x_1)^e \bmod n$;

— compute $W = \text{BS2I}(H(\text{I2OS}(7)||v_j||\text{I2OS}(x_2)))$;

— compute $Z = ((y_1 - 1) + W) \bmod (n - 1)$;

— output Z.

9.3.4.3 Password-entangled key token generation function *C*

The password-entangled key token generation function C takes, as input, password verification data v_j, an integer Z in {1, …, n − 2}, integers y_2, d, p, q in {1, …, n − 1} respectively, and produces an integer x_1 in {1, …, n − 1} as the output of $C(v_j, Z, y_2, d, p, q)$. C is calculated as follows:

— compute $x_2 = (y_2)^d \bmod n$;

— compute $W = \text{BS2I}(H(\text{I2OS}(7)||v_j||\ \text{I2OS}(x_2)))$;

— compute $y_1 = ((Z - W) \bmod (n - 1)) + 1$;

— compute $x_1 = (y_1)^d \bmod n$;

— output x_1.

NOTE $y^d \bmod n$ can be calculated efficiently using p and q and Garner's algorithm[38] with $((((x_p - x_q)/q) \bmod p)q) + x_q$ where $x_p = y^{(d \bmod (p-1))} \bmod p$ and $x_q = y^{(d \bmod (q-1))} \bmod q$.

9.3.4.4 Key derivation function *K*

The key derivation function K is the same as that defined in 6.2.3.6.

9.3.5 Initialization operation

In the initialization operation, A securely transfers the hash value A''_1 associated with the pseudo identity and the password verification element v_1 to B, and B securely transfers the RSA public key parameters e and n to A. While A has the password π, the pseudo identity A'_1 and the stored secret u_1, B has the corresponding password verification data v_1, the hash value A''_1 and the RSA private key parameters d, p, q and so on.

NOTE Entity A can update the password-based weak secret by performing the initialization operation.

9.3.6 Key agreement operation

This mechanism (for $j \geq 1$) involves A and B performing sequences of steps numbered A1 to A6 and B1 to B5 (for the steps to be followed by A and B, respectively). Steps A4 and B3 and later are optional.

a) Key token construction (A1)

A performs the following steps:

1) choose two integers x_1 and x_2 randomly from {1, …, n − 1} as its key token factor;

2) compute $v_j = J(\pi, u_j)$, $y_2 = (x_2)^e \bmod n$ and $Z = D(e, n, x_1, x_2, v_j)$ as its key token;

3) make A'_j, Z and y_2 available to B.

b) Shared secret key derivation (B1)

B performs the following steps:

1) receive A'_j, Z and y_2 from A;

2) compute $A''_j = H(\text{I2OS}(0)||\ A'_j)$;

3) look for an entry corresponding to A''_j in the server's database; if it does not exist, output "invalid" and stop; otherwise, continue;

4) delete other entries for A that do not match with A''_j since they are garbage when communication is cut in the middle of the sequence;

5) choose an L_K-bit random string r_1, and then make r_1 available to A;

6) compute $x_1 = C(v_j, Z, y_2, d, p, q)$;

7) compute $K_s = H(\text{I2OS}(1)||\text{I2OS}(x_1)||A||B||A'_j||r_1||\text{I2OS}(Z)||v_j||\text{I2OS}(y_2))$;

8) compute $K_i = K(K_s, \text{I2OS}(11), L_K)$ as a shared secret key for the following communication;

9) compute $K_m = K(K_s, \text{I2OS}(10), L_K)$ as the MAC key if the key confirmation below completes successfully.

c) Shared secret key derivation (A2)

A performs the following steps:

1) compute $K_s = H(\text{I2OS}(1)||\text{I2OS}(x_1)||A||B||A'_j||r_1||\text{I2OS}(Z)||v_j||\text{I2OS}(y_2))$;

2) compute $K_i = K(K_s, \text{I2OS}(11), L_K)$ as a shared secret key for the following communication;

3) compute $K_m = K(K_s, \text{I2OS}(10), L_K)$ as the MAC key if the key confirmation steps in d) below complete successfully.

d) Key confirmation (B2 and A3) (mandatory)

B performs the following steps (B2):

1) compute $o_B = mac(K_m, \text{I2OS}(2)||K_s||\text{I2OS}(1))$;

2) make o_B available to A.

A performs the following steps (A3):

1) receive o_B from B;

2) compute $o_B' = mac(K_m, \text{I2OS}(2)||K_s||\text{I2OS}(1))$;

3) if $o_B \neq o_B'$, output "invalid" and stop.

e) Key confirmation (A4 and B3) (optional)

A performs the following steps (A4):

1) compute $o_A = mac(K_m, \text{I2OS}(2)||K_s||\text{I2OS}(0))$;

2) make o_A available to B.

B performs the following steps (B3):

1) receive o_A from A;

2) compute $o_A' = mac(K_m, \text{I2OS}(2)||K_s||\text{I2OS}(0))$;

3) if $o_A \neq o_A'$, output "invalid" and stop.

f) Storage update (A5, B4, A6 and B5) (optional)

A performs the following steps (A5):

1) choose an L_K-bit random string A'_{j+1}, and then compute $A''_{j+1} = H(\text{I2OS}(0)||A'_{j+1})$;

2) make $AE(K_i, A''_{j+1})$ available to B where $AE(K_i, *)$ is a symmetric authenticated encryption function using K_i as the symmetric key.

B performs the following steps (B4):

1) receive $AE(K_i, A''_{j+1})$ from A, and then extract A''_{j+1} from it;

2) compute $v_{j+1} = v_j \oplus H(\text{I2OS}(2)||K_s)$;

3) add $\{A''_{j+1}, v_{j+1}, A\}$ to the server's database;

4) make $AE(K_i, \text{reply1})$ available to A where reply1 is a reply message.

A performs the following steps (A6):

1) receive $AE(K_i, \text{reply1})$ from B;

2) if the result of decrypting $AE(K_i, \text{reply1})$ is not the same as reply1, output "invalid" and stop;

3) compute $u_{j+1} = u_j \oplus H(\text{I2OS}(2)||K_s)$;

4) update $\{B, A'_j, u_j\}$ to $\{B, A'_{j+1}, u_{j+1}\}$;

5) make $AE(K_i, \text{reply2})$ available to B where reply2 is a reply message.

B performs the following steps (B5):

1) receive $AE(K_i, \text{reply2})$ from A;

2) if the result of decrypting $AE(K_i, \text{reply2})$ is not the same as reply2, output "invalid" and stop;

3) delete all A's records $\{*, *, A\}$ except $\{A''_{j+1}, v_{j+1}, A\}$ from the server's database. The deleted records include old records $\{A''_j, v_j, A\}$ and those that might remain as a result of communication errors between A and B.

Numerical examples can be found in Annex D.2.

NOTE 1 r_1 can be removed if it is acceptable for K_i to be a function only of inputs from A, and joint key control property is not required.

NOTE 2 x_2 can be removed and e can be 3 if n is stored in a location in which adversaries cannot modify it even if they can copy it.

NOTE 3 A' can be replaced with A if anonymity of A against eavesdroppers is not required.

NOTE 4 The octet string of A can be the concatenation of an octet string identifying the user and an octet string identifying the storage or the client terminal.

NOTE 5 After the key agreement, the RSA parameters can be updated by sending a new value of n from B to A encrypted using $AE()$.

NOTE 6 This mechanism can be extended to provide security against server compromise impersonation attacks as in Section 6 of Reference [36].

Annex B

Add the following before `-- Balanced Key Agreement Mechanism 1 --`:

```
id-km-ws-lKAM-1 OID ::= { id-km-ws leakageResilientKeyAgreementMechanism-1(9) }

id-km-ws-lKAM-2 OID ::= { id-km-ws leakageResilientKeyAgreementMechanism-2(10) }
```

Annex B

Add the following before `END -- KeyManagement-WeakSecrets --`:

```
-- Leakage-Resilient Key Agreement Mechanism 1 --

verificationElementDerivation-9 OID ::= {
   id-km-ws-lKAM-1 verificationElementDerivationFunction(1) }

keyTokenGeneration-9 OID ::= {
   id-km-ws-lKAM-1 keyTokenGenerationFunction(2) }

entangledKeyTokenGeneration-9 OID ::= {
   id-km-ws-lKAM-1 entangledKeyTokenGenerationFunction(3) }

keyTokenCheck-9 OID ::= {
   id-km-ws-lKAM-1 keyTokenCheckFunction(4) }

secretValueDerivation-9 OID ::= {
   id-km-ws-lKAM-1 secretValueDerivationFunction(5) }

keyDerivation-9 OID ::= {
   id-km-ws-lKAM-1 keyDerivationFunction(6) }

-- Leakage-Resilient Key Agreement Mechanism 2 --

passwordVerificationElementDerivation-10 OID ::= {
   id-km-ws-lKAM-2 passwordVerificationElementDerivationFunction(1) }

keyTokenGeneration-10 OID ::= {
   id-km-ws-lKAM-2 keyTokenGenerationFunction(2) }

passwordEntangledKeyTokenGeneration-10 OID ::= {
   id-km-ws-lKAM-2 passwordEntangledKeyTokenGenerationFunction(3) }

keyDerivation-10 OID ::= {
   id-km-ws-lKAM-2 keyDerivationFunction(4) }
```

Annex C

Add new Clause C.4 as follows:

C.4 Parameters in leakage-resilient key agreement mechanism 2 (LKAM2)

Examples of the parameter e chosen to meet requirements a)-c) of 9.3.3 are as follows for L_K=112, 128, 192, 224 and 256, respectively:

$e=2^{113}+2^{90}+1=$`02000004000000000000000000001` for L_K=112,
$e=2^{129}+2^{127}+1=$`02800000000000000000000000000001` for L_K=128,
$e=2^{193}+2^{132}+1=$`020000000000000010000000000000000000000000000001` for L_K=192,
$e=2^{225}+2^{182}+1=$`020000000004000000000000000000000000000000000000000001` for L_K=224,
$e=2^{257}+2^{132}+1=$`02000000000000000000000000000010000000000000000000000000001`
for L_K = 256.

Annex D

Add new Annex D as follows:

Annex D
(informative)

Numerical examples

D.1 Numerical examples of LKAM1

This clause lists numerical examples of leakage-resilient key agreement mechanism 1 (LKAM1) with elliptic curve domain parameters.[37]

secp224r1 (SHA224), L_K = 112, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B6575736572314061697374 2E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
password (= zokang1) = 7A6F6B616E6731
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E 3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 038C9C85F629134BEED14A1665662BBFC7F517BDFE070C1E470D2BD921
s_1 = 77A29359EA58A369D5F49519334A91C82E2D04A7BA97D56B4B28F9E5
W_1 = 033440F4772CD2AA5BB8452DEA433A3308CE6CE8448148135E6E44DD1E
x = B7F03B2A8293504BCBE4D10593216B46E0FE3EC3DFA0474E041FE99E
X = 020BBDFA70DD45BC4C547E76CE7FF03B4AB32ADA12A52637F82F910D0C
X' = 039C4956146DF34530CB82503A0925497761402B7722C71F26C0B0D4FC
y = 915186FF1942FCC764FEA417CD728909F5C29419E59273BFC5EBE02A
Y = 034E5F87BEE7955E0AFF018DA0D77A12FFFB6C4B130E95602821252304
z = 020A386B68808E33B6DE6A5DF9AF8FA29D4765128CCC2D5E76D6C2FBF7
K_1 (= HMAC(A||B||..., P_1 (= 1), L_K) = B4988CC5943D6C8A1F8EF04866F43B6B89A70959681DC8A13C0AB494
o_B = E26DC0043AA90EBDF33CF4C5B1B1860348D56D2226D0383ED62B56C9
o_A = D2F7F179F71D62B9DA5033A5F1096F4EA75E5E24AA6D0A432EE8DD0A
s_2 = 05F627B8FA25380326AD512536BA467C8C5B989D4A7B7CE2A163F802
W_2 = 02AF9DFB335866BF68D391FBF0F791D195D2EBE6A0FB07AE514E483298

secp256r1 (SHA256), L_K = 128, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B6575736572314061697374 2E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E 3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 03836362FFB02357EFF24F4881D96618B2128F55791A445D67E301A5A67B57146B
s_1 = 08B637BA75234719211718326BE28CB3C45EF4EA366DEEBAD2A1738D6A77E327
W_1 = 03EDA13583FB00976FA641B29F1DA37D95EC4E38328A3E645A522637C635F7AFB7
x = 36B80344B46ACC4185A40A740D8008C47BCF6F5C183787DD3E8CFF1CA38A26EC
X = 025460E3BA90D478232E64786C016CDC1CA31B67F9C876CBFF5E59CAD80F417896
X' = 02CA2646F82997E01610F25B2BA8858557A193FEF31C4360DBE81537C96D4ECA03

y = 78574F0E3861B458291DF3D3935624E873FF9AB8FECD7FB731E8E4E28312C53A
Y = 02A509BBD2DCA18C790960A7D6A616A29E9361C5B3E8EDCD5474EDDC03F4FF680A
z = 02903FB52457300DC360EE8E29E35C8E2AF029EE2E552F9AC79C7D7414A09BFDAF
K_1 = 642B8E2BAF69CE15311D89111403F530239D324B597998C2E6468F153545BF68
o_B = EA9C1114DA052C9946016F3E13E5071F687C0F397FCE48395EB417854F13FA43
o_A = 7E44AC7A41F74B739B4119288C00117C4EF697E38E4B4CF9CCA75AF48A220633
s_2 = 8674A52EC629B2DB1CA283E9F3C1BAB79A060CA25F8FCB3EFC940EC3A5A6DEF9
W_2 = 02ECCBC141C0BD5663378F7F71DD846ADDD11DFEE0160DB8863583680A014A21E7

secp384r1 (SHA384), L_K = 192, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 032795D71E027B79FBD173E29AFEC1FEA012EA8E949261351B1B55A057BA2AEB486DAE7864567E295455102A36E80FFABC
s_1 = 172728FF24A8DACA76CB35CD452A5B2965566765284188B170432CB308087F694BA5BE9096646BD841A38CDBF303BA36
W_1 = 0387B53DFD61DBCA7B713EEE1CD97F906BDDDB5154560698 2047180ED861A334816B9280C680B7D006CE16A791E6D34052
x = 06E32720C444DB089B0FB133C4B76BCB999AF85BE2F0FEE00828F3D2C8F6F461B6C59DD6C50D221BF62893DAE34D170E
X = 024F7E422FAF3CE9B6C41D152810F1219275EF2609C2B773FDDA831042547079A81D6422C333176E4BBEA33B1177A91A29
X' = 0245E1A1AEF8670486F0CEB1B64365C6C880EF523B74ADB8FBA8E98E8B7262479342852EACBE59C97A5B443DA391F84DBC
y = 04AA9BED6A080FEB1AA1989C879EC789FCE09E0DDF31ACE2AD6AAF9B1B74801E5BF4A47FD5C88FC6D340AAA4510D3C2A
Y = 02D07170771E78C29960CD8F2C4BF84C680E0E634D626B4354A29E608746AAF6EF0EE8F6F3916D46AEE0542D0A64945539
z = 02CA358BBFC9048EDEA3F584105E3461F9DE6BE68F8D6FD36A35C206DF9E83AFC9D84D8EEBFC6A9B5AF26166D5324A2B93
K_1 = F053027E04824E247DCBD91922C523DB14936475839F0B5D03FE9D93A6D60129E5C77DEB2219BFC8404BE35805487286
o_B = 786C709D048E9E9CEAB0C2E032596E5E708ECE7AD3BA38CD998DE574DF65C413494922D50D2D869D572A5CF563EA65DB
o_A = 3E9928F723856EA8A9051C1C1AE5B9DBCBF5B71235874C03AFD9FF8A7119B001A87E45310899F4431442604878D50C2A
s_2 = 37926DC8F0C6DD5C833A9BAC88CBC7B10540C3FD6ED95522C14DF050BFDDE4A55B551D50747EBB03DDFBB231AD11FA8B
W_2 = 026B99C3D3216E128D04FCACFBE3BD54BA6D60226406EE9789B6040743302C6A916287178C7E0A9CE3AA1CBCBEF63BF7B7

secp521r1 (SHA512), L_K = 256, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB

G_b = 0301FC7EA5FABE261338268E4D869C85792F696FED0C4E8DF2C5CC2E1A058870AD34F2075F6AA9EB345E5C7E389A1F6DACDC69E7F2E23E2E6F4FE634B7AF04B96C0000
s_1 = 0145C5774E00ECF1B110F2830121B25AF54DC20AB69DCAB9EB178A8503F9BB0149584FAAF65643FEB5D3D7ADBAB368DCCD7F516D01B1225016EDCE45DD3D35A222A4
W_1 = 02001641396A47DF8E7904722C402F3CF28D0195A9E9F01C9F8587E21DF000EA8FE9F8F5AC190B8433A678D977802A06F54773D2D703DC7C70A31F86CFDE98456B7B6F
x = 3415721DBA0048D8FFA0B55AE61A5A26FDFED7ED27338B57CCB727821DAEFF7ADE71FF07696940EDE7C6F0ECE64CC528CBFA2B1719AA7EC87A7203701BF28974F2
X = 0201789EDE6B436290240CD0560C417E026CFC40189E01E7D60FA8B34104D841F59528A5FB26A5B5BA08DAA8E0731FAA9517D676E8CC6FD18B3423D472CD02417FB32C
X' = 0201E1254B57E3B19B58E5AC4E8C69951695B67B1A6F871ABE1A09F9EF22531624E6676136F8827933C6AFCEB6A9C8C2699FA52A8185A1387F061E51951322F662DAB8
y = 349E027B11682752968B5F81D2A0011AEAC948D879E059DD24FAC570459C431B742D6087ACF3707EF30D1BAAEC6312A799E8A4408B81BC5CAB320F543DF6B0F96
Y = 0300CCBD31FFF6AD192125F1166FA8315F0862DA0DDFA602A4C16AA285042C1357A91412F8BF94F1AAA23096807205CEC8A88F7E49CCB3FE3E2E99687BC000036A0381
z = 0201DCCEC1D4104F63ECE5733667130E51994AD9AE3326E90778C4D033F24881C105D129FE7188D2A809ED6A200B2B889A7A10FEB2EA1CB6B66C20A61BAE34D29D5FCF
K_1 = 784C12720D21CF9ABE1863130308C215E77A48F33885DAFD0418C18CA5BAF48DBB77B4D1C6CAD146E84BAAA09397C4396375A6203C00E658B99680BDF7483442
o_B = AE16DBDB229E54E861BE925F5FA454348D15DA2268D323FE98F8B5907B35FF938F875130116C41672F4AFFF74E93769A1FE092A71BC04C5868F4C2139E798E86
o_A = 3EEE9798B58D8416432B59BFE2718EDE5B928FC2FB2879883D81B5965ACFC470D3DA3620CB9A4B5C74D563779F116651AF7EE10D6EF6E4FA3B006F6D4909CC58
s_2 = 01460B413E44AC230CAD3226FA37EF303AC5F4BBB25374FA4D6164A74410F89E53B4DF5F4AAB621EA58765738FF1D622D06CC8D092BC11549E4F457A799A09B6C50E
W_2 = 02009C79B87EB0FF1AB99F4E58EC7D73181B675021FEDA0CE34A60F2AEC8FD7346F6156454C88D473120A021C45EC1105487FB4A5FAD01DCF081455E1F05CC3AB6B462

sect233r1 (SHA256), L_K = 128, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C72706C16B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C72706C16B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 03001C0CBE86CE4859A31E30AE144FA26FBA67A84B9430DAABD6EE81608D2
s_1 = 80CD565B13979070999D2B733B7C67F8998C8DFCE1CFC7AA2ADAC34ADF
W_1 = 02017FD21812430AE35D6F95604E7D31DF4B9F1734F8618507CAE552E7AC4C
x = BEFE05840C788DB83D76A374442F9D83E473E87E7583A57D41E3860DA3
X = 030121D46772E77EDE102BE7F0D87FE4554432B72B418DC4640F28C13DCB04
X' = 030038B925C51C0FDB139A3B9C983A182271AE94B03186AB76C92E0D0CD615
y = 8B58498C6E9C433DE2602BDFDEBCB501D67C54A418D53DCA5A2D39F5AF
Y = 0201A7B1C1E33EA306523FBAC0978109606B3801C9EEF25F06EEF79EFC4074
z = 0200EFD59D2776243486B7F8A6D70C48901A12737CC8524F016FEB89FDB138
K_1 = 0E3BBDCF9C27AAC8157485433D96CEA88F1195645A7C6B86C79D8B2A4DA8AF20
o_B = E7A8215C6C8113E86197130021D1B3510624B2ACAE5168B6833B143163C92D5F
o_A = 9CBF4ADCD3FC4DE526F520DA805520526AE4162562B8D279AC4F8191953C2BCB
s_2 = 5EC18601AEEC38217E68A867C2FC8F66A0FD6E065F246792C2AAA3F07C
W_2 = 0301ED6A3947172912BC8DBB893691DDFAEAA8AA3CE378F6DE825838B09782

sect283r1 (SHA384), L_K = 192, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E 3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 0300A28B50B8139FE286B2D2E2C0472F226C08A73E5B46410DC3A855A95E51FC5936EE4CBA
s_1 = 0189B967F2E0578BFF8FF7A91E86AB06C5B8FEEE98755F650C785858977F4CF1EACB3566
W_1 = 020134C6F0D6432C45E17344F56AC1BD32E4773EE5E7FC154B615F70E9232884A6ED89AFCC
x = 6D6EA2F06155FB6EF0A501F700E2D5564168A42A04D0982313155CA99F0DE873858272
X = 020797C2BD11D4B68D95C9339B844137C7271121124DE28EFB74591E8E960DF00CBD0DDCD8
X' = 0304A03C7473B46D6BD7F317BFDE936D12840118C33CF87CFD42EA5D6C05929C6E4C58846F
y = 031C8259C15815B83B5821D6769DE7D1A5749B8F336914EDBB073EB67F26CA36B4F6BED4
Y = 0200D87675C56855A645233E8732CBCD2D0AEFEFB7F432887517A10186A69E6D750B0D3A13
z = 02077C8D10FB2EC7E26F5A25DB4875D9C31B89C90D5609BD0EEDDE9562059AA5DA42371E4E
K_1 = B54951F161350F5DB64CC5C9BA5D8B504C8D11F53622779AA75BFE705582C647D288FADEE074199A038EE 88976EA8093
o_B = 8A410DE35B583BD661518CF98D953684E97CC0FAB6149452AF277F842D25606C5485C20A27662EBC06F2 97C37329BC2
o_A = BD7CD009CEE8185B7C6D22513F2BE610A69C9AFEADA6BE24936EEE61073CFE6B5D6E5FB22A865F1F62808 86745AD24AC
s_2 = 02805D7E24ACBC7677DA4489A68EABDD7649FEF32C9369BF2CAAA17A7619BBE65135DFD9
W_2 = 0200B77B97EE94A9D75530C47059A6B3BC88D871F86ECC2B7DD4611E7C0B02619CB6501

sect409r1 (SHA512), L_K = 256, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E 3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 0200708C13AFA264704D56E9E96049E700352D76249BB30AC28EFAC3046B62A03D909FBA4D0B0416A1A75 EFB48EC1DFEC46A480C99
s_1 = E22E2D8868A7331EE6C9DDF3A5BC71D5833D48ECB2AD63E30C0B3F3242F4AD712AE3AB5325D5A3E22474A 536E0A7522AB1EF22
W_1 = 0300E2AB649F26205F689C2C8C860CA3B95A2DAFED5867C306D3540A9ADF1BDA229BCFBA6BAA46A0BDC1 0FD3E506393B472639538F
x = 88B91481A83B9C19CD4C3DF3B029419A2DBCFA934AB26594981206629F3C6EE9B6110EE91B547A5C85E0BB 501D8A12A65548FF
X = 03010D5C610DD654DD3A39ED05CAA6CBA5B75E720F06AFEA0D54CC31C93414230E7673FFD945C755873B55 CDA040530460013313C3
X' = 02017330B65524EB502E5C818954320AFE000C39DB6E9CFDDC57E73E20ED5BA0E6CD3F8B8E4EF8F3EA0DB 15D62025FD16E52ADFB1D
y = 6E67CB1AE43571006FD3005657B8409926F40BBA28E1E3FA171B31D125C9AEA35F6374D95821526482EE57 B81CDDCC4DD2CFA2
Y = 0300879FA3A9295CA8581F878B7A8945868C223F00E007B2C587A0ED727BD06CB845D2D76F9F0B3113E0D8 40A94B685851C8F944DF
z = 03005B1A6089322D7754BE58303F775967263E113DBA277A12F485FA067FF93139F78F526B58AFB5E54B4E 81E4D85CB85BA6C306E3

K_1 = E30D0863036B3EBF9E271AB0F8A32219368E5D946054F57E97DE368F8CFB3D23519BCBB16B3CA09FC757B EC803877FCD44703F2346327F319128F6A7F923CF95
o_B = 0CA98948D9D7F2A9A05EB156AD51B4CA6389D78AB2FBE3069389C3BBBDD6D290C275EE504E50C4D4B2FDB 709954B9BECCBFB65F84FD34036CD0CB294AEE513F4
o_A = 14E97AC5FD6F0C4A43E107E70F505E6CBD70C1F7ADE5E8B4E1EBC6CE8CEE883E14E65AD49A154E2641652 35D9E15BF0E9E5BF34024ED3124D10D80141D6BD863
s_2 = D95C91FCA449ED36273C6708A132DB34C7F93DF3DDFCBEC1D21C99313397FB308E8D4CAC53D9F8CEF4BD3 85E91BD2DA8BE7766
W_2 = 0200986D96C4D23EB65C8915EC257C29A0F35A2EC5B4D07B6EC0F80175636421BC023AD2FAA3F6CAA297 868D5F5D6E09500A71191F

sect571r1 (SHA512), L_K = 256, HMAC
A (= lrpakeuser1@aist.go.jp) = 6C7270616B657573657231406169737 42E676F2E6A70
B (= lrpakeserver@aist.go.jp) = 6C7270616B6573657276657240616973742E676F2E6A70
$H(\pi)$ (= SHA512(I2OS(0)||A||B||password)) = 64C0F6239CCA16866612D8E1115B5ADA038D88B2A1376CC24E 3B54F308DCBF18256A008ED70342EB5F32BAB141717BEB59B46EAE36D8E50EBA514287CFA66DDB
G_b = 0207BBB9AB624978D634EAB74C381AE69EDE5377095CDB8F68E111FBCB4DCE7898C37E32A8E50B3CC1AF5 177E6876EC5A56C953C493DB21603EC8DCBFB210F0354824B6173D2550FDD
s_1 = 0260AC86F64047E56070B76A0345DFB594AB33BFDF233554AA8B0B9413FF6620A2D4E50639DD0886FDD17 7DA5E7DC7353E5AB8A0B3B31699F0A0697742DCD2C60CEE20C331219780
W_1 = 020349A54418ADAE8F71EB4F5339023FEF1922C2FB5AFF86AF7C01AFBDC9FAC2AC82ACDDCEB259BB740C 6EEE530B189777215CD4AEA995C7060A15D795042266DAAC4B03608FFDFBC8
x = 017E33C05B015B4A1E7ADD458C08BCCBECA494525987BF81008BB2F570E28AC50C9DC1A6E1A688F9D7E4CB 21DE6177C8EC4B88DC293FD6E36684B0FFF91163133E4935400A75761E
X = 0204E4685B756105248DB2D31870E8162C3488B620BE9CCFA9A484EB15677582036132B21C1099A20BE927 221F6BD070CB26C53584A5BF9CEC2C6FA7AEAF0B48497F266FA3E99EBAF9
X' = 03013417D0989691E426E081AF15E177518AACE9B37A57496B6342616BD5968CB7DBC47F40A24451E018A 61F3F73A56C4E816C784D6F3712018CCFD1F8C8A6A75618E36B81FEB6B7F
y = 025A9F76667645F39A4B2EBDDEBF55249E9135D7EDABECB69C8E2089E5BC2B17E16FBCDF1F61F4C07F310A AE6FAE4236FF2FB5B01870777ABAEB0FF8E6C6FF65CCDFE9FDFF05E3E9
Y = 03004A4DF3A5337772EAC17E0B4DB1D4AF5293C74868C8EA0859FB1867FA9C567A8B49EF877646420A8230 39E446D2EE4EC461A577FEBEFDC43E74016A37A258356FC95AD746D56786
z = 020252EE40059B7DF364A605776EFADD349495D85DAADBAF82C3340E369AD6A520053C2BB1E0973228D521 698F83CE83E6856C90D8B05AEAC6CD9877299226769CB1BB807D6DC7A01F
K_1 = BA7D494A386089990A39C5C2064AFDD263AFB4038B5A2E2AEB9875F0409A5606C8B18064C1F288C4FACD6 436FCC449FCACE685626B8DA5C3C635DB50FC79AEF4
o_B = F3BFC7CD8CA2BDF01EABE89BDE570D524808473DE20C6A679FF4C142D959BF47EC76F06E83A9E5854F054 05966FAE07FCADDD2D3DE3A1887C42A70A4D8D5C4F
o_A = C715CE1E8EA379F71AFCE59198128184A51FA2EB31F621317CAF0B248F9BAD30D0C65DA73814F2BEA5458 3DF970C5F8D988195CF97440EFA9E06C5ED84ABAB8D
s_2 = 0260AC86F64047E5C18A0497B18FDF47BD60F821B7BA96A7F6D18E26D1FF09CEAE8CDC1756BDCA316DAEB 2E01885525BD9AF5DE7140F4944872604FA1DCB1E556369203B20C3834
W_2 = 0206390807781A7BC0C8BEE076C88B321DEDCAD6BCAEDD76BFFA6EB67011ED4E77B950B3C040A615C482 1A2257C4CF304FD0D606859ACABA891BD4A2810C2292B4C261F1447F99CADE

D.2 Numerical examples of LKAM2

This clause lists numerical examples of leakage-resilient key agreement mechanism 2 (LKAM2) with the parameters in C.4.

e = 02000004000000000000000000001 for L_K = 112 (RSA-2 048, SHA224), HMAC

A (= lkam2user1@aist.go.jp) = 6C6B616D32757365723140616973742E676F2E6A70
B (= lkam2server@aist.go.jp) = 6C6B616D32736572766572406169737 42E676F2E6A70
password (= zokang1) = 7A6F6B616E6731
H(I2OS(4)||password||A||B) = 45AEDB90B740E9DE9CA7526A7EFDADDBD6E40F6628BF15DE14288687
A'_1 = 87E73FDEF41F684342D1A1B898AEFB7E7D5CBA39AC5AB757EA194B36
A''_1 = DE1AD38862B96C40FB702F3539644EAFDD5116DB4D32C60A81F6110E
n = BB0DDDDE835EB966C0F03A215ABFA7998AAC98B9C2C72245C6FEE4C1B71C0BA39BBF6D20D3CA39CD62E0DB EE89A490D0ECE2DF87CC6FF6F9DCA313543DB3A61E14FBF4C10187A15A4C6A69E7B35B3211C1A3741234F94BC 26C82F665B27F70122F40CA0EDB13CE1D04809FB2DA53D4BFC11065696DC36A2F8466E7DC7C741D3F01474F3 66BE172757350A3C15D41FF78EB163101414DDCBD3001BE93B0B348D4FCBCF59C902CC76893FFC1BED277F6C5 FE86BE9FF69CEB0C05648977ACEB60F169741F08B64F7983B2331364C0EE274FB521BB6BAD4E1D0B3B9F6EC65 82B61B6636EBAD9EA8A77247E16E80C4BB228D4A5B62BACAD716EB249343E683CA3E81
d = 900BC7F2D740FC02BB42204DB6DA1465BB8782C28EB66F070D8EF151B9A3BDDAEA77D8EE832C5DE693118E A4C66F3F4D252E6FB47F6997E7C0E0232251FD6AD0F363CD53AA4BE2BE7C60ADD8F8B803D76B9964F7999E586 EE7D5B49B43F72887A4D917EBE5C96DA5D22D7B7BBA6D26EBAA687FD7AD7B24A563C8EC403D29F475C3705AAC F39331E39A6876F85D621F5853D4BEC23198100CBEE39417A4593CEFB97A64DBBC244F4FD237CBEEFC8DCC649 4BE22952DAF68F64543C347D090A8327A5A66183CD1E8E5DE86C7F59A67C5F0FE923100948563693155 34F94 025AD3E731467D241B301D56DCD2A3CAB0F12379E1E72E82821247A4F570C4E526CD99
u_1 = DEFF10A3DCEA53B9CDA7C210C1E9AA0DF590FF8F96A4E280772D29A5
v_1 = 9B51CB336BAABA675100907ABF1407D62374F0E9BE1BF75E6305AF22
x_1 = 90A25DFA4B7011F513794F8DC539CAF8296D1AC5734B032621A3015F1BAB4B95A06EC95046C4E15DF0FC6 7D67E63EAD2F4A85DF121481944CED4CDBDE8FF4DF40CC0FEE82B34D16B4017E1D49D86AA29B34EBBBED4253E 9A516F4D2DD17D6FE9D92D6782497A45F583AE96F708588EBD436A2382E7AD520786A6C1FE398F9038984E5C6 FF76DAB893002A2197C41F7D6768F6E24E69EDA12336FCEBD7EF67C59E64016B88C26BAC81D443A6B92378B8A5 67BCB38840801CE3C10B2CC1E14D27FEA87E724A1E60DD99EB066A2E46858629C827D0526BD8F981315A34A4F 226C31C9E3D782722BBA6394650ECE5E186F77F31541C33352EB408C7215A5AA860028C
x_2 = 49BD832F7E7782027BD193619BA875A472CF60AAE58EBFA08E49FD74A382D858366D199922743817D72C4 DC628ED3700FEB4A00DB5FD78CC871E48941A1EF09EDD5A242317F7D7288A43FF791C31BBD6967A1568E0777 39781842A5307082471117A3452E8842F7898C9CA5AD01CC57B28AB0EF92B3942EB3ED76856074CC8DC428B97 E1ADEC4CBD8CBEB4F86D4285BAD8FF950F3D7286D4188FFF9E6381CB2BC463E4463E413F01B77AB969D7B5627 A61BFE88F541EAC8B89A8549A3926402C433777AC57A5978C89B550FAB723E09ED04849069092322 93AB76EAA 935ED4A50959D6AD2A307FD6E04542798EEC24D0785E4911FBB83822BAFB5C7F0CB931F
y_1 = 96E8259D67F21A85678E8C1E5D5DE247CC4E29562A8838C18409A94DF453FC72EE02ACECDC7812A5E4BF5 E31CBE6595B76269C0E9F5DF5BCE86D05625C7822F41B4569A57E10DB612FE4127275E59BEE0F80BF34B9DFD6 5846A65E87BB9D33250E57952DBC24994A9B3F236F3A1DA1C84044183596A464C61C2F9BD0C95E221C4987861 D7197F6B35FBE14B9B7B5B4F2E537813EAC3D8264A762D2FAE28A1BD0D94DECF98CDAA954BEA25AE9621A4054 3301FF9D35971C83928B5F2AF27469ABED085141E834CFB93910E50CA238CD289F105210033778DDD836B8B96 35B821260BB73B002D78F6F2C4A870D7DB253848AFD0530BC1FCCC5E10ADE7713C4850A
y_2 = 7DF9DC446A691B3C3514A502DA0F733A6EE3C3C59899A8E6345BDED78B8A0C737D564718042D95B055575 6868010E2A63DF17BAD02B28D585F96E6F85DF7976ED8B2713D61B08E0817225B4EDE3BEE7791A0947CA4D4F0 61281AED58BD0CA3B3E850D64841AD322AB9DCD4BC3083D490F1A9B8E5CF75CF0FFC999139D3716BCA406111 C3B1AD7F6D563CE0F710061C442E5FB10A09F279CF210CE499D19241529E380CC4BD5930B5D8B888110F096 8AAFE1EF2FBD79746B2059997B8437ED77A0A17987D2AA874BA753C3B82F7AB12DB242FA1B9C18317ABE4E61 DB93522C940A68A274F362699FC87AAA9D454EDEBDD13C1E533805FD1831084CF858745E52
W = D07DEDBDE93A7E376A50B05417B35C62E92C5777CBDAF44FBE90926F
Z = 96E8259D67F21A85678E8C1E5D5DE247CC4E29562A8838C18409A94DF453FC72EE02ACECDC7812A5E4BF5E 31CBE6595B76269C0E9F5DF5BCE86D05625C7822F41B4569A57E10DB612FE4127275E59BEE0F80BF34B9DFD65 846A65E87BB9D33250E57952DBC24994A9B3F236F3A1DA1C84044183596A464C61C2F9BD0C95E221C4987861D 7197F6B35FBE14B9B7B5B4F2E537813EAC3D8264A762D2FAE28A1BD0D94DECF98CDAA954BEA25AE9621A40543 301FF9D35971C83928B5F2AF27469ABED085141E834CFB93910E50CA238CD289F105210033778DDD836B8B963 5B821260BB73B0D3557D2D15850544E80303D8A2B06193A54C243DACE5D2C6D2551778
r_1 = 30655322A2C0EF24383D7C067E5604C31734F2496ACCE4B82EC69367
K_s = 987D985F935BCA9B8A8A9B957FE86E17A54258C6709B452FFEE98ABB
K_i = 8A8DA8F8E2A5A423D7241ED5A75A098FC2BA4A5AE4F4BC6F03F915F02CEA5ABC
K_m = 129E32E1A344038C10A4C0F362F8EE88E4EEB17D060010E56E62D415A7995060
o_A = BD5031C6826659E0E67B013D14BEF2A46C235DD8816B9564DABBE2F2
o_B = 1822C7497A6D1C62001ED42017279C28430BF9259E7E9D16DF75CC9B

A'_2 = 336340FCA1772464BC92C7FA5FA634EA8D57C6D2C6A8FA537DD3A267
A''_2 = AABE1BE5A6C800EAC7F35671C5DEBC6B7106A23F65C1BDA248FE35EF
u_2 = 7D2C7C1F5E92D8797D41DD1A3C5ECB54CFA3A5432D2E1988737A5933
v_2 = 9B51CB336BAABA675100907ABF1407D62374F0E9BE1BF75E6305AF22

e = 028000000000000000000000000000001 for L_K = 128 (RSA-3 072, SHA256), HMAC
A (= lkam2user1@aist.go.jp) = 6C6B616D32757365723140616973742E676F2E6A70
B (= lkam2server@aist.go.jp) = 6C6B616D32736572766572406169737 42E676F2E6A70
H(I2OS(4)||password||A||B) = E8F2C5A73E78E95ADE261F29CE9ABB008E4BABD2B8B1CA6EA2C52005CB2C705F
A'_1 = B83D73D145CA980A5C4D69D83236205C58B436668CDAE250E26DCC073475F9A2
A''_1 = 8F3B63C968E2E24BE9AB40677BFB7D3F1EE68FEF9B16E8C35F23B101C13FD0DB
n = A9C583F716E704397B805A482B4C150223D1CEA6BBCDC878D8EE254D6A10B3111C322C97C89057CD5AAF32 6E75138227FB6D0B7FB5DB3CE202A34D5461EEE7813B4DFA356E9890C4843369B93D787CFB01D7F62C752A4B5 0F9B194AC36D19ED9CB64B29F30E795572F9354785876597F71B03FAD997CB57499B96498C7CDDF4DC236DAAE B52BF3087107FA52749DC354DF60AC4A96C9012CDDD6E7FF07203B3578D3CE716B787E911044D0FE289EB7794 2437B88DF6ABF9859FB33A53725C4AD36F03328AD07F7459BC82679CFD109FC2BC44D4812380CAE9152D8D453 CAACB8F85F6FD0293803F745739FB65417D5E732DE54478762A5D68261A03E30BCE7C24880B1501BE7728F340 5A616CBA966B56BA210F340FA16784EA41FD0129BA2AE915FA8C8C7FBCC9BFB3E09FE56A08A6A3FEDB4B1A29E 08BEF0461F10A53B5B3E998AB0928094038C5B4A18F4E8D89694857ECAE8FFEBB110E1110E06B33000F3DDE6E 6CAD39DF905E1D57C0C382333778D36BD5C247DB02E25017E2232316C2
d = 77CE26735E4EFEBA4C0C542F42CF47CBE56454739C991AFD85405DC1655733BD7EA1EAAFBC7964DEE11FC6 66CE4A56416B0E0FD4C5F3635B29EE813E9D1947C8F3CF8922FFD4483A238026962652AF6EC3A14F70D801385 EF99E056285E3C42E7E5A10A7E9B69521C837D29624BB2B09E51BBED8927E005597D7A0A03F39AEBD4D23BA33 1CFAB88D2D4188757F3B1B89BD878BB7CC2D88076A41279262E9457B047CA9900FAE7258388DF6CAD36A3D3A8 FD44619DB02EC54C86369E44122B4CE6098E3A769BE44406FE93C1E50DC2AF99E9F19F2F66F07AF47716BC0FA CD712CC84A3640D6D5E0AA66773D3BA7AFE0BE3AB4B5EACC8E643121D716EBED7C40380EA23F3DAC0949C8FF5 6EC419AF19598F616A75A6AA8423F7028509D2222E89B8A155DDE689A508EDE33468B0E8B7964730AA8B54488 7CA1FB0B4CF8E6B43311F89C096F92D5711FBFEDACE7D974DED09182A7F6B9C1A4B35A393639F0A6DC3A302DD A491E0EA73CB74F4813F4487686A5051FA36F6E81E1B38702B1380003A9
u_1 = E66117C724A338F4BE799CBB62BDFF59840483D56071125D6404975ECE321015
v_1 = 0E93D2601ADBD1AE605F8392AC2744590A4F2807D8C0D833C6C1B75B051E604A
x_1 = 5C6FA7C304D3963962F88FBD931649BFA6AAC95C119C548FAD411390D09E864BFEC3D5565992D805599F5 0B85B13A51BF2AA57BCB5073AE3ED01C05B4AE09EEB0E6C9C7F8250985462DBF6327A99115D582C832F4C86B6 A840B3594D48B0D4E08FB0780D75A6B1E64CE4244C95DFFC09A4E73AF0F142DF8FC0BDA04223A11A71316F9E D89794B02F8D5A83B9CAA65C22D0C066B6CAF7DE69F1DE1BFC9B2BA3F84F300C444293477AC85A96740DF758 0F3EF90E207129F1A2AE8E7B9E7BB319DBDD90348AD28088BC4C26CE70B6B5058009FF0847EB1EF223EE0B87B 972A7CCAE0DFEA345595D1120AA6A4BEB967EB4798A89F9247EBA8F523AD7F48A469844A9124FDCE243CD4E92 3AFC24AD0B87EE380991B45D4AE3F49867C936F8EBA75EA7550FEEDE221A6FBCC2ED4A746B139BAAA2DD5DC73 749C544FBC356C7F976D3E5B8775F4689C41EE1E74CAD1B649CBABD35747D76694BAD48F0CDEBD5AAF362BDC2 540A97D7EC74801D89B16953E263339A278C619421CBA4BE698A5B177272
x_2 = 98FD69C9B7EC99BC3BC5BB8654A05F2579275817F7623C327BEE5E1ECB6380A709905BDE1F13678268E07 554C099C6E06BC9B6751C994AA2B6064CDC3812CBE2ED0D98C9CEF00741ADFE1E982FEB3E20775AEF65416EC 43289FDA3020A88FD630413C79F232CD5E553B2EDEC978710EBAC9A9B687A7E0D396591322BD89DD99027379A C3B5FEE8C073749344EF23D5EAE39664B07ABA081B87074FEDE1E3F547BDA679DA472B2E7490E8FD07617CE8 765C1E1292CD540089FFFCA1155B98F8E97D686144D3F2A2793E08E417A4848881980153303706 5B1FFCFC6BF 5E5582A912FA06564FEF4A21B1B5DF62262BE274F6B375280DF05BC904D32D5D6D86BF1FBE898D18C0D1947D2 F39E8D997BD3B48C3A1790BCB37D9A31A48DCB05EB6F08244EF44AC8021FF2FFB277F66352A8CACEA5403DAA5 90B2ACEED664A1E8D757D3050023E5050EEA050B4EB0A65084DACA41BA7EB5FF557322E8CD36DA51B27CDCEDE B483DFA3F73D7A7523E30405BBE584FB0B245DD079B7DF38EFDC7F1561BC5
y_1 = 7D8EAC856546CDB16684FAEC8E07D4A0D84B9DA80077CC27ABF42858805DD6CD65FDD3D5747D5FECB9A43 FA1D2F465240657248A475A0979A1750888729289841A0110DE638A2EB09C68FD93552B9FA092A22DD9A1A2F 94E95BF426303682C6B2E6D1107274C767D43DDF6C4081BBB3400026ABAB3FD81FEE601166ECE7DC15E60878 825842068DB34D161F6312A371F727BE9D75B0A99E8E2C31433ED48F905ED7D727C81DCBA3F4D2FA3147DB71 FC7B9EE8DD0C8621F617ED58DB6A5C2C14DA4556329F08688230C1321EAEBB3A7BA571D45B70CE65485555F81 0C91912DBFF2887468BF3AF37F9D41999500BDD67F29ADD95C23486EB0E0589B14EC675B54BF5D836F1E23C3E E2F2D681631B7B7AB12C9B59DFDB5460C611F35D8F2A38A97E0F90B6D1575D475F09CF973512F6F60B49DA9A1 F30378007B65FD4CD54D52EA6FFAE7DCC29B5C02E320A629D25BAF54AD1EF108538A270F2E70256E8853F1D76 D186928E2A15420FDC80A23825F25CC449CCEB2A8B0DD46D6FAF68FD2C9552F

y_2 = 2C8A6DF1B203B2E011B1C8875E1596C2E6B1DD84B6F4534F6636A4AE78344166713C3BA96C84A3CD7D5FD 54191A67C41A0BB1FD139AC6ED732B728B702EE2621AA4434090540E4C971CA4F8514B7C64DA680993492725D 82CDE2CB54EAA5A3751D2535B0FBD6954B9C9B77A0B8E58363831CF46150CF93387891C562CCA0354E802C91D D4639D09F82B790CA716D93836B6F7C1EBADD28011E81A70A64B336A7D7BDA82669593BD120BEF1A129883BBD 1A74FA47FC7010EDE380540F6E0B2AE84A2DAF2103A21CD96DFC6ACA012A02E80AC2A4811543E54B1BC747D11 9BE086EAE06FFFD846C78239AE5B7913E528D884AE07DF5E4F79BE93CC2EA5C64E11E5043392E28AE35A3D841 06E0852B912A7E9F671CEA4590BB374371A15D10454E7DDF110108EB45BF9E8A5B4F8DF9C3AF014212D30913F 97F482AE05138A9723006038DB326D797D2224849B38097FEF6F36A3907E460E0FA797EAB74EA2912ACEC7082 A22705AD750AD001777A45565910DE3BD7519F371486858154FC5A7AABFA
W = E1FEA7B6D80C4B5A13D0D98EF24DB4C9D9D02EBAE38F2705E8FA45ECFB3D6366
Z = 7D8EAC856546CDB16684FAEC8E07D4A0D84B9DA80077CC27ABF42858805DD6CD65FDD3D5747D5FECB9A43F A1D2F465240657248A475A0979A1750888729289841A0110DE638A2EB09C68FD93552B9FA092A22D9A1A2F94 E95BF426303682C6B2E6D1107274C767D43DDF6C4081BBB3400026ABAB3FD81FEE601166ECE7DC15E60878825 842068DB34D161F6312A371F727BE9D75B0A99E8E2C31433ED48F905ED7D727C81DCBA3F4D2FA3147DB71FC7B 9EE8DD0C8621F617ED58DB6A5C2C14DA4556329F08688230C1321EAEBB3A7BA571D45B70CE605485555F810C91 912DBFF2887468BF3AF37F9D41999500BDD67F29ADD95C23486EB0E0589B14EC675B54BF5D836F1E23C3EE2F2 D681631B7B7AB12C9B59DFDB5460C611F35D8F2A38A97E0F90B6D1575D475F09CF973512F6F60B49DA9A1F303 78007B65FD4CD54D52EA6FFAE7DCC29B5C02E320A629D25BAF54AD1EF108538A270F2E70256E8853F1D84F171 0DFBAAD9F7B1198E3B274ACDA961E6CFD6D8C40044CBFF53C7CCE06B894
r_1 = 78C97D9136553807560C4875AC2BAB38C5CBE606475B6E44FC1E8D1CAA704430
K_s = 7450EA83A3FAB147F53FFA4BCF60559A9216B9273C57747133C0BEFEC7C565CB
K_i = C1D82EAE7028BACB6C948C381F7D9D175F8A4688DA71E194781E4EE9319965AB
K_m = E51AA895087F407A2F3E42AACD0AC15DBCF9A7CED6545838E88EFE9BFA9221C9
o_A = 4A488828E5B4563C3DBEE507EBEC1D83BA1DE591807AC808B496C0CC8A4CB79F
o_B = B6DED2C0A85FBB790B101B4C465AC7C93A4BEE12FB53813348E9CB550F1DDDA4
A'_2 = B9F9FBF632C9F7244B3F011E37A5C1FEA6998A8DF5B440A6727727DDE316998F
A''_2 = 8F6468143D5844391E03C681079AA8F49C76B679F7B4350722AA8320A4A84E3E
u_2 = 651B0E50B6BDB1E1504EBF55AF3AFAAB7D6EB7B92B768E896A53D98E0CB3D9A1
v_2 = 0E93D2601ADBD1AE605F8392AC2744590A4F2807D8C0D833C6C1B75B051E604A

e = 02000000000000001000000000000000000000000000000000000001 for L_K = 192 (RSA-7 680, SHA384), HMAC
A (= lkam2user1@aist.go.jp) = 6C6B616D32757365723140616973742E676F2E6A70
B (= lkam2server@aist.go.jp) = 6C6B616D327365727665724061697374 2E676F2E6A70
H(I2OS(4)||password||A||B) = CB908AEE4BD284D7C19B8F43CC7C74C1B931321BC6E32E56021917BD1E23775 58542A89F683B269533A072056C2EE1F9
A'_1 = 2AD88DFCDF78FB6E2077AC9CCE6ADCB6270A4DFC00B1A79045B87B8FB9F2B09AA3D25291663F52514AA5 DA873D938ECB
A''_1 = 460898F3EEB2D24D181AB66F4E58EB847B6C6A4F729F8113F37ABC538CB3C5DA85A4449CF6BF496153C8 1AF36FFEFD82

n = B5A4678602A7AA2B1F3290854AF40C8B99ACF9BC5787B9CE1349E9F27A8A845ABDE5693FF9C1446CE08B14 B2CEF444028948E5171F485B99629D2EABA6826EC328A82F424741F84E5E57E70B7555BCFF538AFB2EA4F7E8B 64FDF9EC8466A4A03AAE81D1952517AE982F162FD5D4B63FC5C468DC024F7064A76FE64E763C77235B9447770 0931A56D034716E182B7061308D858BBA54AF8DEE5DB6DA3653B6951D31D74AD313D4BE3F99ED3CEB6734C972 D97710AC8E1A07AB2ED5BD0879CC52EE108686E450C4649D392F765712C362F25A8A9936BEF3E928478D44970 8F0FD2705D26914DB7035B7A6A108F1AF04408CA1A801BBF8ED38FBBDC2CBBFB7166562FB18BE0E1A1733F124 2DD0AA17D955EB4D631858AB8107677DCC5682F64FFFF11F4AB14EFDC13ECF3232E2D7C6D44DE15382A0E4161 7DCD8CD7B046849E69311A505036C82576F45DF7C53AE7D30D07CEE6091DD925399F3E3D97915164A1C015E95 4EA5B696C680284B6311294D4D0E4D56E8F26347353943FBEB113124569409027622133 8B8DC5B7DE61659381 85C0DAF25E440655E792B7C8E413861571FDFA80935B0250D7E33B3290C61CDB3B2D90C5F9347D8889741117A 1F2163F290CDA615136203C90AE82B40B368AED0FEF88045CBC68AE4814FF9AFB717AB58529D196A94D2D44D7 DC9622E632CCA0DA76EB4837410A6991F880CBF7B20C99C1B0AB82A25B95C3C2E913C0B6E9FB12373B479CE42 D60AC9E673EA6A6B6FCD9886039D483BA59527F4362FD39F3833AA1795F843B4D425798DF8FA2BDFDC5761100 276B94D7CD5DCBC5B58CDCC3CD7B3566F030FA52A64D6B5A16A9D4141175B262EF2B2174120EDF213DB08A7D4 AE3D507AAB8F624AE7FCAE75CB966336661130FE04EE087AD68A28CFF8FE269106F269583065EC75261 8CC9 801166ACCEE90071902D259EC6CFB87925016381C34549DED12F8467960371F9B17FD88F9E047B45DB8C9F1B3 3AE194649A24FEDD9C3D7DC04A122BDF11E681FC66293B324C064DF227A690117462FF3CDE7777B732886DCCF 8CEB6B1A948F99420E25CA3F226EF462FE311AC6A9BB2DA0C35D5E219FBB1D73973226D21346CC7B5D50A893 F33E8DB6251110A42034B967FFA2ACD8C546EBE18603E2473166FEFA5D7F1CD2419D23702B52CDBD4B524808E BCD93B83D69CE182F0F4E8BF94FF2799335083736FA0DBE6B92C08D4004C3B9E2043DE86D37F77BE65C48A3F 7C24DB17824297C70C15E7DF1C926CAD52954D7DD3125C028D9F0466BCAA105D462A423FB8E81EEE348826F1 FA3DF3AE5931CFC435E8D82022641AF3A7BDC18916C4B6CE41313F
d = 9459A737844885ACF7F22D576CB398C424BF9939EF09A54EC32BF858934E646ABADEFC356B620869E9CA05 F00DB29150D6DF24917CAB34BD562E123CC9AC3DBD3FA3A8E67A7DCB8562311EB49BFF3B3FDEBA1D21D616501 980EBF981FED57A57FD8EB1BF8DDC32358C9DBA0F1A5FB4AB52C0D5B293E0BD27FA55780BC91284C0413AF593 4385B2A269650256CEDC4974E8AB44D4C9CFD15BA337A186C145CDD608F8B83D5D0F82F95D4E867362C91AE1A 6BDB746A86CA44F9D76A05EE8CBC6051F3ACA8AAB133EAE8C1117336CA6EEC387384809235D2C456DF1C44D99 97DE5138B1957C80D9F0270699CCE2812DC0DD4B3B6A518277DE5489C4A5D54314C88083F603F3779B49984D3 C9745A50DE4C1D6E0F2543431A260DCCE81883DC0830B4BFB6739F1599 8994B64A0C04FAB82BCDF0801A98DC 3A6E7A9EB89ED00E4D69E7CD3A27A43C46E9C8ABDD8ADE77EF7D053E18C398ABFB21BC320B7A100D377580B0B 11E43EB3D364BC9D32B2BCD443BA79117301B89F7AE9A3A597D685B2CF728B3B2B1D1AC3AC4866627F54E7396 9AFA64407FA3189F80344B863878D4AEDD9F56C6F799192231 43CD47BEB04FEA271B91F255A668F44A6503335 596AC532FC82E43E5557ABA77103FF01C9403FF3C94981306B8047639AE1B9399F1E04C85146BD785B75F2DBC 2230409C59D2BAFBEF49D26257573E9EE8817B6C88B7690 DB40A04D4C67597AC1741BE172D929FF425A713B7 33839AD13639AAEB814ECD53306AF2C3E0CCC17AF199714121D8E7BC111501F1A98188A12BE01F17D41F8E619 D43E14ECEF720255DC97EEF65CF70D79F44F6046BD0A06A14DDC80617E01F8C792CD71A03EF23922966F8B3C3 4BC6DBD4A484CE2C90E858099DEFED5AD4D2F0352B45D252F9136F28E1539FC9464ADB398AD51D19901C24CE7 FCE6372088C1CA64628DDB1D8C96E963359C9F 06A8D024CB897E82D0965473C3BB1644DD8B97E65C9710C4 A597E34D47FDCB6DB3B9E3A7D348C71BAB4CC 94BB225F9DEDCA1D83E685A84CB3F0870348723AEEC2E567A3C 93B0FC855865D2258CF5ED26B943586FC8FCB 46E0410674EAC0DA76794F9F6BD1E80381AFEC23662780E9B26 DDA124B606A2DCB05582092DFA73915D725 09B9209A967BE7BC37AEFC58FD9E499CF7A85B09C57959B957C90 1D3515A47EC7C67E7C95A3164C4B95DF1B7ACF382570AB716BF39F557B4D4B8FE9DFB5FF9CF4F10470F9AAC49 32D194B67BF8D789CC8D66526FFBF1 E989DE61BD772B864168A89A527B574D16BD0A618BD0E854EF8828980 3929AEC2A0EEF14AF99280F11BFF 16EE389EDB3D063226249749
u_1 = 5A62851B9A0CB2D2AD34BE3332BA68CCD1B239BE00DCBB4EF6864FA48F923F55EC3D4CFB92E15309D4909 599E4B5E81B
v_1 = 91F20FF5D1DE36056CAF3170FEC61C0D68830BA5C63F9518F49F581991B14800697FE464FADA759CE730E 79C889B09E2

x_1 = 93A8601D782445DC1EBAC0F9120927A8A4182F8FEA6911242919B07E8DC865A2E606AB07D090F9E770D64
1F90B1E3136B4DC212843C54C901198779F35EB480C196BB7B6E17E0B510654CB7A979B3F59B7B21C2827ED76
F34A4D61FAC82DCEF80B2AD83A527A60E92544F0C4DA03179ECE2E6FA80D8626E6BB43F3D92C7211FB28E0546
E00A93B7F4105DCE30BC9E63CA4F1A0E2244841686D9CD4BAD169502F7988A68D872CE3E2E44D0E8677CA3047
5F54D68A84B4985AE5D27C9BD32D494656A44D9898D848BFAC2066CB090CC38D6FCEF2ED35F61FAFAB1DC86F6
E4D53CA50B716C2C2E0285A8AA93268A4144BA3CCEADBF7E62233391D42836978EC81D24A9D10FD435353C968
5030E8D84D373674AA11E6AA946361E57DA187591B32B138CD0262861990528F19A73E40DB39D48790A2EDAD6
074C211532321BCDDF3EFAA2BE93018C24E17F4459A96D0CFCAAB1189D10FBA5B871EA0AE8893AE5922F92114
43DBFBC755CFF226DFF30CE54B17DB4270C8ABE0712CD36015831A9BA2CD6545516175C5858FD6FAFFAB36DCA
8DAA230406A3B85FD992B30E4FA45B365A8A6ACFD821E303290C70173E34ABFB26E08D9A55A697469740C8C7E
4F55AFD8EEF47C2E23779F9BC4764CB187A362D6D2F60399E42E8BEF3942F635824BC2CE81571DB744DDCD1FF
3847A4469F81B1BB7FDE2071E0745A9D43ECDD6D707C2947199AF6C79D72DA85DD7C3E90FB628F6EAA2C7B28F
8C3F44C88F594B216C61E0CAC0724BB775B9F6AFBF987BF37875B0F0A9C8783AD0BCBEA756CF8837C7F30B8D
74C5E6F385399F27B5E230E85D4C6DBAB6C0451DAA9E185EB521B08CD86D63CF41FBE9B32AA262F3E81ED0CC8
6E25DAF990ED48D00ED87D3C3C2E85739F2D76F46A42F1526C1D0B33C194C04D0AE664FB4F6DDE5D943012CC
CD2AFE3DB6DB950119605EE07907AC4361ABB49CAFB014DF323F35B62274D30FEC629CB7868793341516371A16
C9EBFF05575B96329B02A91B2B6BEA6616261FC2F0DD1FE3466126FA97B4001DAE95D98943A4DA388014AEB79
BFC3707F2CACC5EC2BDEFB0B7712C190B8893AF2511412074BB68A51FE89D0AA126870CCE4362BAE68662BBD
72EDF83E74404EF5615E57BA72A7B4844C582501AE808AB5415189CB386C9DB6D59BE3C2375C6F15A455550EB
57FD9EE31D98BA85EBB09DFC6979F4065D8DFADED7560CD90E489E4827DA6D72C05B89001F9C4863AAA7182D9
C1A6350BD51E81A9B4E80ECC75051AB785B13B358B951ED404B80BBF310336698BC6385FF2FBF8266F86C2AF7
98AAA0956F7A6C061964BCDABDC42B9302921474B4D78F40454B538

x_2 = 09FD33030A7821B9E43C16C7557C87DFC6E98F1A4A671668D6C7F92EAF9ADC8F39ADDE212F41719249B16
A01E3702F9F0857185FBBC7B20066E2EAB57CC718C362007B2B4EB797A732BBF9DD3DCAE5612A2516C146E628
631319FC5D97F0BEBD2B7CBDFE5DC191C4947FAE15BA95D3EF47E6B054D3A23CDD7152F4834935590ECF4A02
F2669B276E73E466B3073BCB862B5BA027793FB6D81F9E044521731C0C497E88B11FA790134C9E53919D80ED5
FC826511062F2EA8747B499FD472D7D41848EC1A7D5B56C6AD30875F3EEC3910C6678FE1934C758CEC76E062
CACE36E1F098F91C99ECECFF7D53D262344C38E4CECFD095766A55AC7364A20DC1CC8FAED16D9A2EC682B657
BE551F6EE9C3825929831E6A4C05EDF85D5676121C451C6BDD9A20D7D8DA26580DD647AC1930D9664FF3853CE
9AA1A9D41758DD30B4ED4BD2470C8C0FAFBFF8E1D67BEC7EE5E898E81D029B5D71C16F581975E9A776C1FEC40
CF1EA152B1A0793D0A86BF8CC1B6DF947D35FE1537A44A1B1D2812C74BBC16C8D302F42A5971719003BA73AC0
C16BA6B269BC98C6242EFEB231549C7CC805BD99349883DB967994D87A32EB249C03CD7CF1E4F81C5A4BB6D55
E2778EB54339794481A93B0A8E754E4E49B78D12308A0400E6E425AE21EC9242F5F246B5888CD20DA459DAB42
DA89ABCDC850E6C9BBEFE15BB5E55846282EB2179E9CE47461C08F50C24F786EE4C2CB6E91FE67A0671EABFE5
84A4511CF2A0D78A19E7AAF10CDCB1C964CED1182A1EA396196EFB4DC71AE509D5A5EDC65BB8C16175D85A005
B448B464FB405004151CB8FABE169CF269D40380E3F8FAE875BB46E9195210F2D2832CCB2AD773D05671C5AC0
69ED0DA9EA02440C12029FAAD71DA18EE8B7850FE58985905ACD33D36BCEA4FCA7871578550A2C6E4FB5A13E1
782878BE16FB6D8C6C639780ECDBDCBAF7DDA221E2FA2ED10C47ACC172017A0945923F0A01FC17F532B5EB2FB
5132C9F77EE75DF32B69513A70CD7B04DB0213BD0457D54E6A3D7D2657D7CB96A8B31E8CE759D965F8C7593BE
1703F63C4D0D07C7D6471B98D0232D659182DA59B371784F2681A43C375056D63A7B084A022CA126E8CD7D387
346432A3548858BF32DBA9B026A6AEC7E09E292F115F41E330E60924C84EBDBC0ABC0634A9EB1B97C5CC083D6
BAA55DC94E4B8A18FADAE75D2C17B25D7DB8BD7BB9987ADEB6A89570886ABBD4E4D12129379751898E2C94651
5A29F82743E1A180D8C61F62EEE97A3E4ED8595C53556C47E783C8DE7C88B006A9F34B763F11494FB5D5C3DEB
CFE2A9A2B7C548A12E9C3BBCA133F3BBC5B011EADB25E89659D4CB5

y_1 = 0A97F7C49E6D6AC4F496B7971C842F549D10CD350F34B69132F055B938CF1A7FF95B4B17993D0256A777F
B9A5186F18A53F7D04FE32F6879E3DDD947B2AC53A58FBA85F7C37AC98059F43CC5D35071D7C9FF6327B04DB
D060B742EF2577C09A895E0AC08E7B37BE7FCB717A423B691055FC90A40B29BF848996D39233721C65953E25F
CB8B2AF5F92890D164DBC208A559830131E2590C7CE900376CF0963812F17E14FF67C0CD8B26FE616CFE26AA4
0E964DDA848438A3E3E16D63A703FBBCAA7DDB73A04A665375C65E394AA68B602626C0C31394B4B7C1F57F63
1F581B9BD6493AB103C59A08EDCDBCC587484D5724A7511CB551334EC2DA897779D7D8A2EA9986DD790BDA15B
30F96140C3C0AC5F40A318E171A44D02095F0ED08FDF5954BE62EECAC41227A5D5428FA149D70307C1043A9AE
FD72A3AE7A6EF8E139286DC7CA952AFD95F478B0E71B91303F234513DAE34CA1DC24A13262A8CB621E86A1D17
3E08EB5A236E6DC80E2710C31502A6031F83C18B7986FBFA9F9D29D172AE225665901040001FB260AF13404351
84BE606B560DE14F73FD6F7ED021A6D12CFB161CF75F324E81923BF3F4616302BB6970A4743D2AD9AC29F12D6
CEDC9B855424C40F9187843A2AB368A6BACA0BBDD1530BF24DCBDA410F50177A791A78E1ADF4778292F0A7824
533CAFBD5D6526197AD24E5BF5B3D99F24093D26398751219A642AE54E54B879D8E135B33D9934D90690E3E08
604B1442A415AD0BB02F3693F7D55F6135637BC653645AF830939B12A2BCC539A4CD72D04D84716D60A642C38
C24A4653632BB863B01FD2C3806452E34267C2ADAF369ECCC5F5B6B1F749B3BD9BB48D02C7337077396ECC40C
F2DB77F92C4F8474907EE87C607C9D2BC5A8F39DBB2AD2CF6754FA5836CA88EC1320FD020014142CAE9DA9F57
44392F92B9501B9D887507089BC4369B125EDDA068078254C57F08E76807B1DC2A9F1DE52A32D58119FAD45FC
2626AFC7F07F9273C11161164EECF7AD8F5B40820C25143D64954E6BCC9B983681228F2791D99E1331534D92B
DA50FD529685072D071A851E4D484D2E2DE9BC34E127EAB636F4DA07EF365086C1C7B1BDB27E6FDF603CA24E4
4DD4224FE0DC6DF6BE969D2255E8CA224D328BBB710B45F7CE5D6A0D3459BE9127112E6DA86B0063DC8978803
16E78E3DC13C729DD65DD0A0A14CB93FD582A88846338E94543CC1909FFCB0DE7B3653DF434C7E1B174463B4D
E7C90EF1EDCF57CA0F088C997796956BD21CE5CD5743401BB0AA979CB142937275FCB64672CD12109DB06215A
234BE7C9BAEA365FFECE59827274848BDE94D1089D063832F3762A34

y_2 = 02AC72611D95F6D5043F9B94D7C1E3BB9AB9C7B82AB41DAD21C99AD81B21A90DA555308D548FEAA9FFB745A92BF68A704F5BBD6C804B9357C05D0A3B48FBB45DAE68E2092FE066692E7E61CE10D8E161136D46E6D3A4E50A5AF1234CB26D439BBEB2F1588ED369DBDD1C42E93CB40766BF4C0F506B499B36E34110606BD150DAD9A14DA0F8D6C8445CD128A25AAC4D88BE4774D3485BA8B5498E5CCBB70A68344D02E6DA82E650BD6DCA9034D82D7A63C61DF9E41061791DE306F1A30C01C5178DDAF8D2A77B093CEF7BBDBD77CCB7ADAAE057F4261AB4CB4BB2EA29DBD66C22CA666389CDFA4569A5FF597EE6D7138B46323E04A358C0EB89BC234D01C026AB72A8C500CC4790E7E3C2A2D84C581EFB27C86D9AA68B77F079699E79D76C7A6B221404257205C679FA3FBEDC063AD2CDFE5A61E383FABAECF5D2C2D34434D8321D2C48AC520B716C0C25BA5EA710FE6CCC266C9F26C495F56D6EE2F3D9A7AD03DB6EECCF4B678D10AC0ADF952780CA07375AE1B1F9559B45E240DF2FEB4C819CCEBE1D21C9FEE88C053776C9565E699C6AC12B491296DD851DFB84602C2C81548838358360A0B0A53E643B5B116488E8A43F1DF26E1B4FE374A85DA2C9874E939128B0E26C32B3E61CE5995A48CEE1A956F8FFA90C8747CD4E6075BEA8A1CE91D32E35141139023
W = AF166E359F433B2EF82CFE0AAF61C20256578692F108F1277E3B255AEE41F87CC1FB181093D4A29BD40B29EC2069CFF4
Z = 0A97F7C49E6D6AC4F496B7971C842F549D10CD350F34B69132F055B938CF1A7FF95B4B17993D0256A777FB9A5186F18A53F7D04FE32F6879E3DDD947B2AC53A58FBA85F7C37AC98059F43CC5D35071D7C9FF6327B04DBD060B742EF2577C09A895E0AC08E7B37BE7FCB717A423B691055FC90A40B29BF848996D39233721C65953E25FCB8B2AF5F928900164DBC208A559830131E2590C7CE900376CF096381CF1E14FF67C0CD8B26FE616CFE26AA40E964DDA8484328A3E3E16D63A703FBBCAA7DDB73A04A665375C65E394AA68B602626C0C31394B4B7C1F57F631F581B9BD6493AB103C59A08EDCDBCC587484D5724A7511CB551334EC2DA897779D7D8A2EA9986DD790BDA15B30F9614063C0AC5F40A318E171A44D02095F0ED08FDF5954BE62EEAC41227A5D5428FA149D70307C1043A9AEFD72A3AE7A6EF8E139286DC7CA952AFD95F478B0E71B91303F234513DAE34CA1DC24A13262A8CB621E86A1D173E08EB5A236E6DC80E2710C31502A6031F83C18B7986FBFA9F9D29D172AE22566590104001FB260AF1340435184BE606B560DE14F73FD6F7ED021A6D12CFB161CF75F324E81923BF3F4616302BB6970A4743D2AD9AC29F12D6CEDC9B855424C40F9187843A2AB368A6BACA0BBDD1530BF24DCBDA410F50177A791A78E1ADF4778292F0A7824533CAFBD5D6526197AD24E5BF5B3D99F24093D2639875F219A642AE54E54B879D8E135B33D9934D90690E3E08604B1442A415AD0BB02F3693F7D55F6135637BC653645AF830939B12A2BCC539A4CD72D04D84716D60A642C38C24A4653632BB863B01FD2C3806452E34267C2ADA369ECCC5F5B6B1F749B3BD9BB48D02C7337077396ECC40CF2DB77F92C4F8474907EE87C607C9D2BC5A8F39BBB2AD2CF6754FA5836CA88EC1320FD020014142CAE9DA9F5744392F92B9501B9D887507089BC4369B125EDDA068078254C57F08E76807B1DC2A9F1DE52A32D58119FAD45FC2626AFC7F07F9273C11161164EECF7AD8F5B40820C25143D64954E6BCC9B983681228F2791D99E1331534D92BDA50FD529685072D071A851E4D484D2E2D59BC34E127EAB636F4DA07EF365086C1C7B1BDB27E6FDF603CA24E44DD4224FE0DC6DF6BE969D2255E8CA24D328BBB710B45F7CE5D6A0D3459BE9127112E6DA86B0063DC897880316E78E3DC13C729DD65DD0A0A14CB93FD582A88846338E94543CC1909FFCB0DE7B3653DF434C7E1B174463B4DE7C90EF1EDCF57CA0F088C997796956BD21CE5CD5743401BBB9BFE800B36C725657F86271DC32E30C315DA7ED1454D8F139255BBAED1051FF346F9C9C726973A47111621F13DFFA27
r_1 = 4309185486A772069D990EBE263177A7D7C04C0A5F6EA68CD47FDE6418CF2E61A4A88A0D82DDBE329CEBA8428B570FA0
K_s = CEE44B1E0A9526F24896D8A6DDAAE1BE32119AFB1778F3D2E9B8FBE3777F33D191D6AB5B5CD1602B2BA534D0D8A4D0DB
K_i = 3D91FE92FEEF4E0D5DF7216BDD1195AE79B7117AECF310803DA7CCA3E6A7653D
K_m = 0A7C69591AD386DD260AD9E9646172FCB8F7ACE21D4C3365E35734F96849D94F
o_A = 9767 0EDC5E22426AA6981937D58BE6958D3B924AC0ED15BD6002B569745BBAF8AAA474CD4BF2137B85B819F00AA7D430
o_B = 00D9E7420DA93D12B42B1BA67283FA4FD83BECED41E31AB9A8514775118B561AAD7555F04B87C2E82B4C5C550DCBFEB1
A'_2 = 5F0E2CD39855B80A7429EFA92393EC249F07DDC3639943AF14306F08874C32F44E02CBCABDF2F986028246BFA9BD5BEE
A''_2 = 8C0244895B7594E9092C487D5C2BE85B4C68DE6F76EECD8B1125FA5E72F050B538E8F4FE5FD775D1A7063BF0A6C52A0B
u_2 = AAC834DB0AA695B18FBC70F7BC2D763181386B992B7D5D2F32D6E175D8E43443BD329D4F507A166389BDF73F6B63F2B6

v_2 = 91F20FF5D1DE36056CAF3170FEC61C0D68830BA5C63F9518F49F581991B14800697FE464FADA759CE730E79C889B09E2

e = 020000000000400000000000000000000000000000000000000000000000000001 for L_K = 224 (RSA-15 360, SHA512), HMAC
A (= lkam2user1@aist.go.jp) = 6C6B616D32757365723140616973742E676F2E6A70
B (= lkam2server@aist.go.jp) = 6C6B616D32736572766572406169737 42E676F2E6A70
H(I2OS(4)||password||A||B) = 403ACE79AFC2A31D2C84DD89BA6DDE18F0173827CB0FE94EC5DC04E31BD934900BAEC3BD98C205BD1AFB34EFF4686CEF8376D72A8C0DDB61C27936AE2D5F13E5
A'_1 = F2ED23688D292688B6F9884F99ACB0BD5F57B7820BAB2732F1EC8B9E0C734791DF2764E5BE9C59CA87627C693FE1FE7B86FD688018D25964EF455815BA4632AB
A''_1 = 32A217F531944B5E315A07C6439BA2BBAAE2338F4A80E79A2A17B0E62DA906D34628CD21D3387DC315DF25784BB5BD4C8F03365648F2045DBC2DBF8003F9D385
n = BCCDA660BD5655CD1CA173652995A4B36CA2B0C4F77CE2117C858E5D6FBA6BFBDE00EF540B33BAE3B805D EC0C0A7C529CBEEBAEDE6E27EF631840EF91A9BFE4BFCF48283C104F2F9925B685F6BCB15252B526DC4CE9660 E4DDD4DCAF65927F5C2A370DC5AB2EF34840826C472FF9A5C2996ED2DDF1B7DE71C0F8C9BBB0C9DE7C503415B C2CFC1A0E70695BF88E55530355F865A64065C16709AE9096A9B0E805E60F08BA4173697E5270BA5CDAA82FC9 92D9AEF0338C6F47D580A73BAE409D086FC488263224CC7C8C23AE1A7B17121FFEBA501A357740FAD98BE7670 DF257DD50EFBB5E6937A7D9FEAEA34CC4F0AD19CEE0D79EC2A706748EB783089786115EA28BF13FF2656D35D2 9E73A117F8043AD43F69EDF648999A20A7801D79AD7455E96F1F1FE37DAE8844CA0BD1303E993B4CD3EB3357A 5ABE71D668D97DAB98BFF62DE6949A03EBEF5E774AC047A083095E14FCDC0FE7A90A7F9A2729B46A69DE28E4 D2BCEB0A479BA256F49312788EBC6158A4E85C3EC889D304E7D9C87790EFF581B6F3ADC6248399F64EFD2A70 DDA2867445DD631A037462F2A892272A65BD1B599092403F8A96A1B51537C12D9CB1CEEDE34603E4147613919F66BCB48193462E39085148022E540B87B556960484C1A53585EA1E4B57205F8A9F84345C96DC54C75B132C63038C629533A47F267597AFFA1AE24883AD2608252B44EFAAC6F29F4041DD20150B098877995A0ED983C56A85F16B6A8ADE550A3C1FBFAA17F32CAE7925A0C3C426A2430B6C7692469A6BB07F8C810D1E7AD0A6C674D5FDC88384B26B09E6B024440639CD70C1ABB4DEB535AD0809EA7E90450B6065AEC05361E6D5222A04F9F4F2B6BFE29854BA06E10D86AFD71158191B59D7FB83806B628292A7D4E32228DEE84220830616E57B46F8284C53C4975223003B986B23E62FF858DF284B76BC958B71ECECD7184A806C90F0FBFD678E8B65C9076CEFC05A28A93F5CACE7E3C72A693D7C992546063098E53C581CA5E2DADED544CACB0E803A591B6CBCB580CF7BC12945554AEE11D980E5F68FAE76322B1B71641060534FB1E924AC45EBAE903A17B1C88164C3448C1632C2BE3E61930BAEFB85C9FB5900D19FE7BCF1DCA19CABDCC9DF35170C6228B271A7C770F99CF5AAFD245DB7AE1ED3DF773AB9285DA63DD1183F499951E0A9752B3343D9863C8F80A6BB32D85675ED49D2814253B09B7F0EF034F196E271CD87F43D86EB6CF19448DDB51F40F41A7F6A62837654E0DDC30DAC90040E0299461471285F9F87E3917DD8D90ED210764CA5654A301B2418975F321F14068B3DB20516EAF234CD9AD7E6D14E0B2BD9D94472A24D54ED5BB83F0323242862BE797496B2027B8E4EFE4C0DFBB08D3C18D658C6135AE67AB7A00B3D8395146B89CE7B8A17C4CF5D34FCE96B19A4D3A4AF183250F1F9AA99A911600BC7A67A10F605A4E4AF04A05AE62E6EB86060F2BA6587FE8BF3BF3348DFE544129C50F3FF2D3BF1A2E269BA55577C217CD718A576D4E9030A45A44012D3ED7134331FCD2A9F037E6653F42DEBA1B55A7760B2803D9A6C98185143570E7C5F975DD8CE0F7BC83385A6BF433959AB8255B04268DACDCFF84335CCFCC6B9B035378C61463D4EABF2C5CFAC92974C1C492722242E73F09E838418F6AF01571A45E556E657F2D2266793D8452DFA03794340EED30FC32610432F1A630C10337A55153503FBB114969AA851A2E2BE4EA78F9F64D0B14E9C5CADFC770DB7D65ED714573E9882903558CE9D502CE3ECA89B19BB08A3D5A111DE3998E89DEED5AB4185EEBB9F9AD13BC8E42EC20320D601974DC162DA2B2FC28190E1C7E3CCF065A4C574C0FF18E5357F0CB1217E14B213EFEFDB17E5AB4F2D9441117C7C3B726666ED4ED10110CA102DD129CD6BC38D0DF6819B0F8920A65A9C13B4DB6B20805361B1DF25D826A81C9BE2B9108C5D740214EE4479BD7311F57A19C0A3C069BB325C34BFAD5F8DD52F02E51D534F5210573CD7C550EE0429D6BFFE749AE03C21C7B677DF5BFBD2EBE9E5FFF338049D31BC43C81574A368B1DA2B5C3734A6711BD5C4C0C8FB69C4EEAA2A4CF245FD28E10D25643B231A03C2297726AD4E1D6F3C8C4BD65B436C362EE0B6CA30E7CD524FDDDB68763A90BCD0B994205F232A1C4E65427B2D39B8670FBAEE847908F7B38C6A88883AD3142A7DDFF0EB9A289A7C6FDDCB324343283D157755C0A1D6E525CF2C0F169CC00250B37EAC2C8ECA6C195421D5855851FE5C38A7B65EC930FCBAF286DA2F23E213ADCA00A5B379AE22A7ED1E50DE3D0AD917702DB0BE86BBFFF30E7D6FE4D1953CA96451C65E01C32F41200B493299767A8459AAEE9EE01240E92887ABAC7B4115551E5F86C49CEDC9116F6A2F8C947AC1344D59DE437AE92CCC04D7C7A9B99B5F474778E1C3A8BD295CADEF85C5147B7DAE01F414CA3F71E3C87BF2D9C6881244D198F11804709C73F42B97899D343627C630795BB5BB8BEB69F6BFC37E33B0C81ABBA4A954C562DB5D7FEE26229FD351A36BAD3098C5972874D65DD39ADCFF7225074193C406E388A0AFDBEBA91CBD48DD04D76ECD7528089147E6C4CD4771BBA96967D34DFA98E40C1E781C6E87CFB61269E394688C51C333C36BAD3D10035AB91D2265964AC66616776CEDA0DEF01675FA0B6B12CD70E013D13F56DBE365A970AD07299

d = 7038515FFACAD2B32EBE019470882E44EB3C32526713441F23C1DED845B214CDD001839429C0867BB1FC2
633EF0FD17A34F68C44C9DF0211E6FF5B8FC9D130572B5275A80170EC971125B9F1A829AD4ECE4CF7FFDEB62A
E0F6B1CE4404E2E4BBF55679E31F099272F2C6068FEABCB090BB75D2E8940D280A4F8582404674BAE256CA378
9C82687135DB9C0F2E5CF8F2EAFA015E225A541FF0B293F1F3593B42BCBFEB2F06715BB7B042FCC4EBA3BE16E
232A42BCE24846E910D92D8F4CD75BE762318F80BBACB78CE2BF78EAE7E75BB618FDF7E30723615126A43B1D4
4154BDBA34A97086B8D89B5CFAEAFE14708571BEEC84DFAB48B4E4478F03306A5D36E2DBE090FA515A21B94BC
036FB848E9723DA0AFFE72027749F924B5150B8B7A1E02B38CB0E45D4157543B95FFABE3B6A9FEBCD720726AA
38756E037131AA39B2C860F5FECBCEBF7A4A49554B94948A9287FDE9EB4961AE0F4E97B432FE2B405CA8A34DE
4ED97C7A22EEFD08A6003677818DFC841FC3F8551106CA1F16C3B3084E97A636B495B96603FBFB583693AE111
294BDD40376F20093D0CE92281D5E24C7025634971DCF1C152C48D8CE01D8D70F047850B0FECDAFEF84405510
C0B56D4308750C1A0E57DD8FAC2E288A16562CA630154BBDEEE0BA900A5A5462312B978E625C93B89E7CEABB6
7845F708456F455F3822E99837B1C8C2F6C29A4F1E40976FD4DADC3C3341A917425E87CBD43534631B1590BD8
F77190526E24C88B11AD818500867FA51A6C242D7F4B3A3036542AF651E37BAF0A052A6096375ABBD63BFDB84
ABDB65D78EB552898921821B1B8FACA9D4FA619C823D5DF91F85273A883C8897E28BFD4EB7DBC2F6EDF977F62
CC34A93BC5DF34D83065BFB954BC31601D840B0C45E7335C112B751DF768914588DEC9F6C413E04D015726AE
7C87B343B19FB5D7C6C8E82CD32FEC52617F4A133350FCF3910A14FA9F38E9E4859A89BD1660234EA33CD23EA
C98A63DF97F16A88666989D969D6400606D7A13E45FAB4B21225396C2A6591CB6C06C4EEE44F3435019CDB1F1
CBB85E4D775D7FD9F0E52FE52758BC7A77E27E2CF2D572AF1BA7BCF3212C41390CEDE862AE934F74110CF2CFD
509243F544ED7B22167CB0376B58BA1522515E49CA19320FF0E354562A773388F2C1F4FE032262E8F642CD492
2D99F82141A8850C7AD129431FA5FF7DF75A1EBAC5F8BB67A378CE130C9D30A5C5F91C464DDBBFFAF6699E48
3E2ECE55BFD597134428BA955999F79E424EA2539B578DF6CC7FAC3059D789A4D128598EDD42C6F6BE635FAAC
7F8F6B6E50C6936A29B3A94A2D35AED6362B4B7F11091C60D817FC04D32C6391D1A46016C636B88686B4FBD08
58453CE8E9C22D1E6008DE98922736FE148012302F581031A1E7A4ED1AA13FBC93FCA96F6471D29F23C06C581
47528B72F38A47D381179C8FF27C9FC93FF4A3BBDF3BB4AA599574A0810F7DE5F91B207C350B5610A374337E1
50B0A589D4584D92783AF135245BF65302C18DE5E57868F146C01C65C4CBB895F9EF96162362A311A421040D4
5C160414BE4FE48598E34ADFE60B1B746816A52872AB4F6851255379797A88A50F853D14919C6FC688782C7CC
3D54CB295145D6B5DD07CFCA02AFC90C8C3D596FFBEAF21A8E051CEF27D1934 0A158C9379E13D9149159C60D2
D05A8FC2763794332F53EB25F604F8E64B33AB4E779E850FDB18DCA52035891D5A4C67CE64A40A4521E39C9D0
468247D6CF8501B99224E53EAB13DB24C10578BB1AC8B6F2A462C196895CDECC1078A5CDF3FA989928A33145
5735674FF97841FCE495D67E79491658C20A32AFC47DE1E365C8D8E72EF3AF415B63B2FB161714D2D199F9DD8
758A4D6A342CF8E59AA3CBC249F9ECF2159F60AF1F6FD8D8E6FFB56000055AF776697E59A6019605A43C6C219
0290E0948D71403DBD13D6A82F29541C1217967A6073439BEFAD954B61645403715D2C8E9B0F73AD3ECB07A7
FD564B04FC347B24DC4B2E1C19F7B6568D6B43C40F9EA307060C4DD698CA13C11161B6ABE344E2730E1816AF3
D3664CAB494CFAB9D90263C63DBF09ACE05F42112A77A8035C258AFCAD2DE2784D98CF43C7EA07E76DEA233EC
716CFE98B68E2E1B33A0223828BB9907E1534985A5BE90F6955CB8D9A3C2ED68ABC98F19BF9CDD68EB42A6B88
7CDE08227B20EEAA3A641E5A65A226F2F56C688B50B3F6DE95FF97FE3F1B294A16E041AF6971EDF2EDAF6005F
7BF111E640346338B7FB86DCB237DB81E472329CD0CF0CFAFD79EC436DCA4E5A8D4679A0E76645B21C289689B
498F1F582160C92F27882D86F507EB07FCF1A732FFF89B8311F1B29EF4BD97435EC09BD21FB07C5AF43C1D351
4F81C62B2F2F671428DCBEE12E8155B0BDFED2DD01B57AF755615DA5CA9E42EB5A2A89C0DAAEA57694EDF8A32
6F8B508A0FA8EB13BAFDEF502A03F9CD225FA14DEB27814AC62FA0815ACACB4B4D74713EFC6F918030FEE8D79
27CEFF74B421BA6B93F9C1E09D07F2452166CFF312EADD857CDD80E04808C6D30278D4E08A7A289E4BFEE2304
E272486E08A7661EC251672A93AE8954B2 2670E9C5A2F849D8078668179FA1106C4BEB1DDE8CEED8E688A3A2
59D9D9833D7A0B0CF6C032606FF4CEBEB6EB799D1F6D4C82958CB5E63DE331E5F9949E80B302281A363850C44
8A3A708B7FD9E3A40601

u_1 = 92768C04926084AD2D2C109140F6D66A53A5DE776A149B248FB06757EED8B2A62F94174531D594CA24472
00D9F6DBA4D2CF5983099DE36290A05796A196DE6EA

v_1 = D24C427D3DA227B001A8CD18FA9B0872A3B2E650A11B726A4A6C63B4F5018636243AD4F8A91791773EBC1
4E26B05D6A2AF834F1A15D3ED48C87C4FC43432F50F

x_1 = 94CE793F64C3CD5A6A948418D855C9094468ED6EF31F30EF0E5E2D19C84D2D3932B6DC95EE5CEC6D16240
12185A07DF2EDFD6EFFF701CCE0B55508EF40B7933B88B3734827880EA5F81958C608E1DE7ABED428B4F3D43
B48A82DB7E53F5B790F3A3BB6218EFC735B1093B90DE40478B3B7980223695F9F516D7A0C3DE56AA8D111F95
9D83EA4232C98AEF122B8F9E545B4E49ED79EAAE08C574268A55E65A5B9F285509B5666B8B7DB8C0D9EC79250
16CC490E30D821EA4B71DA8754C11CDC19462F93EDE819612CF9A791CEC3F78933FDAEA421341BD47EA438668
1E94192875BBAB19718EFF914624413DD10DD9BB2540E3A2A600E27A27B43C5E6779797AE95E423993C480CA4
4D6088FBCE6FC8BB3859C81535C4425859EC4354037EA901E4791D5C0EA12E87EA35B2696113E479065D2B3FA
F2C4A8AA0AA6E6269B6134D35ABF51B352965C4AC3FBCF507A0700DBB027B1C4848475D7023171B6407E04339
8AB517C01926A8281360117F3DAB44AC34BDA48ED343985DF1D4861E46D77CFE8F6ABC51AF419EABF3D69B90F
B1BEA5131A14F2749D9DA82976631CCCEACF0AA873B4CF88C3B7550856AB10D4B38B1A29C1F1058FC61F1379C
010C820D1997457BACD791E6332C04C8A68D705578E056FDE483C5859D2ECE487042CF39ABEB98E6F1D9188AF
0BEE85A4138CD0CB2F864194024544E451253F986A221486CA7E9650E4E75413C0441F773A9D69B90ABCA0F80
745C251CB13589D9593BBEFF6753A786C763F123C8C845C603063439EC0952FE13574A2044185C2C9FDF4070
DA9F39A838EF83584554B51BAACF56B8D8C1F6FCF26DFF71A9AA0675704B2C43864EFAE67626452962237CAF5
51F029D6223B6A7A3561A9BC35A50910CD376FDBA919BB0E3E738DF7AA6BC84F62A193508FC155CB51A6AE258
38C4973F0ECBB901FD95ABE88999624458A20D55B1A50D36D1C4B090B500FC977DE25022BC645350305B54F1B
C6C34F5785842B60195BA2F96B9FF970D9AE66CF112CAD014D768E70A283FFC2EA525A24D565A655B8859051
ED7C7D8E9A534C67D0943474DF55B5839E50043B09F77F9CE768C56B88DD61FC52524AAABC251C6B745AE86A
4239AACE7AEAAA5257C555E22FB2EF6FE60014744A3FDBE562DD9D947FD9BA82DB3A7816E61D230D1EB57B0A
77BE16D18A57289BBAEB2B9EFA326D69B17C76FB252E5E580577A2B61550FFDC563C04A4CFECCBF4757F9857A
F69E39F750D7714D1E1CA6B7E77354EF224A712CEBBB31BC82ADEF658417D09B14DB2DA974B83F9F33CB2695
DE175E04EFAAE5089DE4CDD2C79A28D1B23D5A2B8053147150857689ABC6BAB059B5821E0C2801BD7FD33B67
8FD6E6C85486FA691DE11B116A1C29B6958551ACE0827DF884F5ABEDED5E82B5E7A8F9DFD459FD1B28E8CD50
6B1BA03C7B3EEB2C8B61FFFF488F92E36D85AEBD35A8946CBBCA74F0098D20363BEB24452BD93B18647F1A21
AB70C970C044DDB093CFEEDA3CD01BD4543C2B0492BA7A43A02AA6BDB4EE10A13244D25CED44B58CEB43D06B
0CEDEB5B46C3C81BF2E07B5FCB306C95713263B4EAD78430C34424EA0CDE6683C91404DBD12AB039019643A7
B563762B402B3A898676A8228A62B6FF32478A2860928A392B94C853AD8D27B911A0FEB810FDF146A688E5A4
BF138191451CBCAAEF0382CC311E060B3277E0177698D2FC3D4D6234BFA86117E818D08CB7800B68C5EAF2
384175C855C18F120155513D3210C5A00B4929C9BAB4BE5AFF7A6217EC9A4F023BF374864D7B92197F8A97723
ED67FD450C8E7426E07FA2CE3A1120A51F4B28B180C269FDCEAFEADD17A6781195D4D566913F4412ABE36C368
BD4CFBC9A8457D9BF043BEC9D677B1F96CE8389D1E7056006D73A98F79E510D898F4DD125C5800CA98ABE163B0
23C38D9DFC39304F1D4564F724CD50BDF71A0FAAE011230ABE75FEFEDEBBA6681B8499E93B8CC583E90F8E956
B27AB0857788AD2A9E4BD3513A6BEBEFCFEAA269192F199FC5CBE886BA7E68D12F4100E45303D785F4B086936
9EF5BF8BF448ADA2D275E2CA5F875DAB6A6B6962FCF55A6702AE870EB02BD8DAAE85E0C69407F3DAE653D101D
ECD3307E4FC5D0F87E3786050806CC72EAC8AB0027C84953B447DE8766AE01D599CBB5B1403C247B3CE03A338
389503A6D25A2D18C797F52EF3A1644F3DA971N7091CA209AC90845540348D4C8DD712E57DBFA403C5F425144
782FC84BAD3F20AEE2FAAE0813E9A25A8A65FE92ECBDFA1E08948233E56D14A8B301AEE5AC61E1D83594D2BD7
F8D4AEF2B7D293C77E4EB0DEDE66BD589FC30F014F152900A53612AE65BE52E60079326331AE826D8BEA43A7B
F63B809C85737E7BF633419798C60DC7739234614447 2D964017A23FFD0947F713C06E8E36E92319884AA74D5
A8428A7CB2F46037D59C6992CE90C7A6CD844215C1CB85E7A2D0B60CAC25C2DB2B91B30D2C3A2ECCC72609B64
20A36049F2F61A54671C758AF3B3951CE4E418556818FAA7B698563B66323DCCB66EE8E05E815D08B6204984
9D04CEA4374E462051DB254713D04820B10D72FC99F85A2D98541C6AB1B23426241D88418F07236800FA464DF
1FCD5BF5251941F8D01B7FF87017393AF96D9BFE4065B7BD9FB518F4C2072E189C5B8D527D9FBEA0EDD56BBB3
FA6E055E3B79816AFB79DE01E3C0

x_2 = 07CDABE711450305B7A0F9B058D5E184B87607FFD4067E86A7B5CD86F143955C26C8BA8E3DBE015D862E5
E77A1324DE8725AC296B142B788C7B797543393D1F616EEACA90EDC2FA7B58580CEC684283DFC27287A71118
62F0C82FF108448A62931361602E1E670219FEA84A9FD4B56CB4A90F5219CF6B2667CE3F0A5B1B9C698D23E0F
CAE62E1A5A163C63555B6073F05EAEE3328D48B7DC3936BCDFE2DAA9F31B5A31FE33254C571549AC5A306D1DF
FDE7DCFF0EF5A879737BAD92C4C2A2AE0FB8CF297998AE4D0CAA65C38EC8238B58A70E40A050DC4F403D2815C
FD67302CE4AB79975D9916BAD9B11D108F5F78F6B86414C6CFE1D98FF6EF9C481767AF02FFB6A9395090E22EB
4CCA18C6CD3329CD23E3199F166677D5122488C36B70D63A85897131B53CF7C1D45DCE9E11B553A1202F40AD9
308C199A312CD3AFBE54C8D670FEE93A33F2904F758C0DE88A5A563484210202408D28AC728CE8D3C6FFF9BB5
5BEEC15A7605CFF683B3E70FF68F32A01B5AB3E3A2EDEFFBE2387306A4D14572BC626021AEE7C376D67538CD3
8B396CCBAB03D451924EF9DAD7B8F6F0C1212B0DEA3404E7AC7E4D1C5E1C87DE1E7D5724DA3C4A52B610D7D93
06870E53E92A81427FE3E50AD1694B8BFBC13FC9800F1A308DB7030B775EDE0B7E5F9DB9EAC0F6D8ECD7252FD
E509B03A3C5CBDE240C1AAED235A5B32D89DCF75845EE45846DB7492CC75DF6E2930FC5A91B9BE1AE4367524 3
45129C9C49DE17CED179927CC0AFA40041484A54BCCECDAA2430223A73142F47C2451BB219C87A74E81B96EFF
23940FBC6E7796A49A503D83EF36E1AF7993B1A8BA8FB45F6BAF2A8D99D7A18E6B4539543A655300B100BA10C
3FF545842AC61EA954673B49B23790138930602E80A1E9667A062C2578ABE6E419A52575510916CF44ECF9D3D
2637CB671233074F5AD193DC30191A1A9B8F15D28AEF8CE26A8ADAAEF658F4FE97C9F666819F592A408F28835
4086A119AFAD502C6B46462632D0B8CDF102F1DED0B18D4ADFFA2EEAA52BC8269A8B2217F7B3D8083329557 7
2F05B898B187769E50E31903053A8F08215CE763855C0307CB3F06B644B372F1C266B3E7CC4CFF0C2B87D5A91
1DCF9203D1FE104BD73D89FFEF54ED0FAEEABCEAF8390C1DC3B810782737260EA761F64BAD3E19079B167B9CD
D69726A384DFF4A0A077A3055F52FBABD4658925DC9642F57440EB66D66CDC42E64B0E7E3867C2502F1670E9
85DAAE8ACD4252492EFEEDB0DF58EBEF2F7DF71C4076A5093819C653E4BF3CD0E6FCC3105CF32C4155772EB54
235A50CB376C1577D953F2533F98AE9E1D87666C89F0D9772F97649DBE054AB7FEE5AA7A5DBBCF1316E242603
F68DC474A2E16C24DC0B1214383A69EBE0F6B061CB653155CB8988A05E10379D8CD9FCFEF4A611AD400EF24D9
C0613F887BE7BEA83561511ADB7D4F257484D403B1E2492371DEC1AB2B826B03A2AD35CA677D6CEA65F49E5DB
CBFB1CB8C77F48A44E7C3AFF04F605A685EC7A1BC11219E9F5C06D7DACF8423855255D8E3A83F81BC2A72355B
5B35181588DB1909BD0B1A06721465C97AE589F4D4AE82EF2B4E33A8994683929B28F7E1930F8CAE967BB7233
5610A8B5CAD131EF6A6754E37D2D466EC2688D7A4EBC36A331E42688C008C740EE19C4F79780EA547919B2D02
CD9E114A64D9D79919D58FB5FBE3421F1237D346B4F6906773D7791019BBF4582C17F41587514DA786C1CB43
F52A3DB4F3303D27CC1117E9A80F74151A366287276A0B19332E6218C35CCB71CE5FD03E3AA667A38296E1294
1D258A234CBC2BACFA599017823D65A9C357D855F5487362192BF2C561EC91D259FF21CD917D85CCC0725CCF7
6601DEE8C4C8F58F885D8F7D567819934E4B1CCA4C4F2676624BFE345C9BBD45132BBFC0F7758F37B6B173EE
A8B63706666D5E3ED56A92B0782879CDE2169E746AE7F6F2FA6F03BA33426FAF1B98CB9D0B29A64E4C4839B4
4A7488FD57C052B9040D0D63E12059F4DB4A9BCA5469FF9A09862406D22F901EC4DF68E257B24DA8611D16F54
49F9A84E6F1A8591067DCFE414C61E74D03428BBCF652FD71A654690DEC1FABA51695547E52D02FD4087165B2
A14E44797428E2AE45CE0314AE840335C10645999A0DE0C414485D7749D3DE66F05AF38085E47E82E3608AC77
7E4E292D05A1185B62EC3FD4331A8BEF81C95EC4193F6AEB4AB4F60788CB1EB2479BBA68DBB8D08C5F049ADB1
A0B4B2787A4022DD7CC03FE42346C1EA955F1C2E14C4AAE219967B43BFF0618CF37F618C2C2FB12E2DEE52CA6
FAD8FAEBD6B77F5B15BD994660578BFD5D7C9EC4C0E25738291D3F2F5F5E295F031ACCB456EC12526DFDC6EC8
8D662C745AE5C160E6A70E6ECB36071ADA0BE985355901C4578CB3F8EDED693F00D65A5C1FE39FDEC69C4DFFDB
4C6353AEF71688BB7CDBD7CA64E40DA5586691398B04964C04407F593E2D58038049C29C823E7018A3B992222
BD49EEE42A7786E8F80CB24AFC3E7D50A41E94AFF9AE7AFFF04EF927FEA7BEFC0383E77CAD341AB005889CBE
6DF2262840DC28F2EA555AA47957136034FDC58879E6A970F9A4104B6483B252ADBC5639EDB1D9986C3B4FE75
F3415CAAB63475241A99499C83BD9E7B675676A32277B7641C8EB966395AF639E052ED49AC60CAA170E6DA45F
9EEE59F1B5F04767D763

y_1 = 8CC4BADCC047A06B396C4EA13D26E088A7C6F91E056EBBF3B7B4A131C17C8DB5F886A78562F27AB72B931
B3F55DBC65023BE9BCB24931BB26163D444D04216A5F2075A3F632AB224D33BFD99AC1496763BABC33EE6542
0810FE7CDE3C69371630B2EAE4F7AB30D23B4A38B5303A6693DE0C6B4D6A358B66F4E17834A2939EA9169B09
D945E2670A879D501533928623AD717148D3FF2F769648F22D7E39907B48991B8ADA001811100B5A95F7301A
608181C09D3D9AA9DF90C35B37E367805B7C8FBE1677774EC67E5D0F85E4B59437C3A18D71F22128E5787827D
8E27990788661BE6E41E516B76BA4235A33B85F6D2B41788A1DFB272962E371797B3123F480EA1AA1E98F3133
68EE0241980A27B013AB14C00144529EE2C665E1376AD0C901162334881F1CEEAABABD687AE0244BE98D39100
576932FB9F83599A2F6E0C93EBF7883CBAA7BD9196ED86B61CA686C0A456DE62FBF247EE997B9CDAD7FEA51F3
6DEDEF28BE5BF74E7CB2ACCDB2471FAEFADE5259CF8FDA580CD11575B6443CEE53D8E1A683538EC20EE6FB44E
D9F1CBCDB3C281075397CF6880216B4443A8E7F38D9A6FE5F724373EE077A59632E661058FC77ADEFBD902B39
6CCBCF72AC94BDF6B2AB0C43DC994228BB51EAF62E156D068834E6D10E8E5A9CED3ABAB7D4F89F86A09A51593
DE28033A5BA3772406509D307FD8D925DB095C61E6B892C43AF1E18130E2FEBD9142764818C6C9665203CFC2F
86F1A5E6A3CA8E64405DF929F5B64307E0B4475125B7DA14512192F4E4AEBBAA2F8DB7248D96ABEFDB375B4F
C8FACEEB96ACA326D8668484451259D5625B8FEBC9C91CFB67728D6149A0D1832FE29747AFE4D8C9237292E46
6ECF5B38ECF52DA9C0AFDA624A85F52994700346C419FD8C6DE7CEE5F5821702C8CC85CBC331BD258A767AE0E
71CA6F0E719BD08B9A930588A41570580B241789EDD420B50A8480E909D6B05DEB1FC382A0A7C13B9540259E7
2666747CB3A6282B29B2E56658B866976DF5A4A88777AB094528C5474BA2FBC14C0CDA5DFE47B3DDBDE7A4BF7
9000BA6CF71635F752E8CA7062EB96FAE66D0C22CD13455F8E3C43B420E0DADBBE25E9AA9338DDD4BD1501A19
B104E2AFD8B04F6FAD859188364533C2656024DD7827E802B6E9409A6F6C9654AEF63F6AE9C8DF692968B5D6C
AF4C866CD195FDD30F5C7EEDA2F3336A9C07AA6487353C725D1A8C9B81FEB15607808D15C09B04C79BBB64C1
A894B2053CF7FD91E91C2C270450D80947C6AE956184F83E816D67ACFA4D2C5308F70B82DCD44F90F68A7271
3FC70731D437C22D2B016CCF8BE156D325974BFA3C4EB53F643A0CD7E92AD2DC05F6BB596F2B63C21BE426B8D
9C734BA154DD274478C5E60D275032B0A348967448F3136A4F88ABEAD5E43DBB6C4F1E5CDD22062B0759DC88
81CB9B56F29C36832FE911BA9B171E45A9C109C95E876685247C6EDA92B7C015DA05E90C219477D8F1ABCF35
F2FE82C89F474BAF70F84851B7CFDDEC318CB7EF76CE5E962E6FD4EC200826ED59E318C8FE2C6BDCDB445C13
40AFB69E95C5D66FA6967BC8C53F244B3E2EA1A3B80125582689B7916A4053F87AA1C86DDBDCE2C79250CC5F
96B1FA11C6B5E4B05DA526BBEE5F43FC432B9D67093A705F4C4449D2D9FACB014CBF6BD09D7933FCF3582D09
CB980034E4F68FC405FDADFA77DBC7B93198CBF65B51D254CD2A7CBDC860462BC8FFF2A616C1618585E57C72
ABB9A48C53305B664D0A779DE9908322A805A121550C530C2C99F01AD1397C307470596838E11746F2DA3CB6A
AA7F66DE2115DC8B9DA5D549960F3AE98E0D02BD43DEA3FF9B5F61140A576C87DC66194F8F3C0B8F9923EFE6F
BF4FE78981045E18341FEDD5C540D24D36CD04D4D7061C9ADFB94F4BBA64A605EA93D02B4C2952AC38650CB32
A32D25E61781165995980EE0DA8998D116C5E195BCF13DD31F61E5879A8D391558D7567DD54960DA0C8E02CCC
F93453A6767399647A2D576573FBFE77AA0E41DA1B1D90AFCB7E3FCF7D1E256FAAA716F43E637417B1231B499
42FF9A5E3399A15F48EADEA90D0810A39ACFAE4E3662C7B61C9F834CFB5F889D38DC222C5A91E69660D1534D9
270A2B1958188A7B09C27BC65DC05C1F08033AD6B2B881D5D4A63783EE5B5131994B2EAA14E3259941394F379
E7D2373A4A35BE8FA2773A551E51FD6FB209F3DCA5F6923EA1496CF3C136282425E7EA848C32800AD32B98250
35FF023445BE2E9E394E6750B7424BEEA531ECE67CE9220463265C82342515C626E89DB8940402AEAB744F77D
A6141B149FF2D282873CF3A3D4EAE8BF33D7DE5A67C906B740FA6DA2393C32C8A1CEE06530D27221EEA27C8F5
FC7C68B0D18EBA16F8C025D8DC4013815233396FD4432E3054463B73D61F6DBBD4529404BCFB4127428F7172B3
6FCEBD495C19B10DBFAB629025F6C55219139D66DA304982D468311C28820B1C826552557257925902F2991F0
11D22F3C7478560A09431B2209F42CF60C2C5F9277D4B53652903FD33B11ED4EABAF1E4603683F390E5CA3EF9
BABFC7D6098D300A8AA3EB8B9061A34C2CD34DA1DF407C5DB2311CE22A7F1348A3D46F8B937F8A68165CDB722
1B105BCFD5A1174C05C63FA04EC8EB99B74B4272857900DA9D0287A8F99FB011D928EB4AAD62AEC5D3C322BD
564122014878F0AFA4352E54F6E

y_2 = 7E573802A7BE63BC93758B8CF1AFF3215AABFDFD2392F912C3103D5D75557D3A124CD54641A5F601D164E
38AD2830E3959F7AC83C68253088CCED2EC0BD2EF2A6C40922628AC5479E31E345CB7CF1D30F7684BF059F55E
D7D4C6663391E289FB414A132BB8F5815E328CF40209823A7328337D513B29571CC7002617D5EEEC9D25A0D05
FF8A648B3CD2E25E79FE92873AD1504340A400718F21F44E48D265969410604D0120A27A9FA195A470F863EAC
0AF5C909C922C25419F7A556D5BFCA7454BE524D639F7A2B365D3EF05201B57F0E5706DDC11A3BD43BEE55F9F
11B5CB7215C7B16C4E94FD9FFA767DD244787E05057C92DDEDAEDC99BBF7153E79B5F88AB819E4F92C8F85B2B
225A5200C281F25B4FF313AC9D14AF53EA2EC963E74F0E15513C0900E97B66F74C1798512EAB62EC3DC00BF7
32794FC0FD195A9589E5F85FF7F5C04E0E054720BFA685D1C966B0B14A23817C0504C0A4A819ABC992BDD18FF
55BE0B51E49DDA625589447850E22C7BA335A3B26AEE31BAFA90B6DDA111E62F1DD97F097DD9EEC027009DD36
5BE01B892E2BEAD915EF07D0CA919C473D03B00C2BF3692B5FF330E86FA0C544D53F16DAD6E5E6216E667BC7D
E3F92D0D3892F349A9CC152AA81B2D5566E661B8AD46921A31672167CD3F1D6F281CAD8A8875DB805F4B5A67B
75912269FD4CC2B2CC3A3FA05F9BFF1A0A5CA51748F16DDFCF81712F30E64B6E666519E7B7FB40B33BEB870A1
A7A3EA355962F2AAF3B9A7A3D51D6DB2B242B4725E7FBEC352689E89B14D73EBE49B52AD3B555546F22B6CB3C
92F4BC8199F3749780547E2FD517A89C09F58DE59E4F232AE2B86C9079D2742F2F28F67543789159C40A6F213
19697CB0E373F286D66D8A9C41956BCA1D76A8A223FB32E9C4D06B0D599BC4A6429F16F3030DC3A9A19F4A408
B62311EF8492E0039969A9F9855AD70709C7069478F6E987C48EE7491AC2B977DD1BD708F15C594EFD3B0BAA3
6081A8D79A4E2574104B4AA2087D3678151B9834257BE1AFD9376E94F185C6CAE96EB15603BDC770473BE999F
C3C3F164CC41D395FFEBE639F501A520228ADCB29A0766DDF903366DDD76C9E38D1A4C7A93337F4FC8D51C35F
9222744A50479981D7B3EC62156DDC4E7854CC65F1CC346D41257FEA4BA76FA958A1BABE1EEBD0A1424EB8FEC
A39564A82A6397BC5F4E8F2F57057EEFC0167E45B0307D765505D6F3A59931F26E1F5A461ED4AD4D28719B93
96C1823A10061F252450690E8682B096ABE38B88B32AF56355B495FB7C476AE1B42DED73B04115B5DD2E6D128
B13AC87ADF93CCB0D4A1AF08B716E994555A817A8140983404FE1721B56B8FF27A861AF4D1C1B33B68DED15B9
EE3F2853504B6868C2D2E42DAFF8009DB3B1E502DD2C538698B5E9082A7BB7D85817B530321D81E47F805C5C1
DB2F94A2F33DD69C6545D74B4DC657FCAAF381CD0C0C9D612D607E9FFB4A357D5B99FFF1A62FB8B1E31248FE5
B3057CB1461DBB2A675F049DC4563E904313586798B1100A514E356DA1DF97834EFAD461537128EECAA26D996
02CD887DE69685FF4E475D831B1CE5DE0BE2AA0A2DFAD1D687F8BC22EC267E168288003F4067E12083E4763B4
164C28F7806945157B56922ED4B8F3B8320F68D48F92F7253F323FF09429AC6E0167CB45E13072AC1B6CF8A37
BED49CF2AE526B370EC01DA889610965C455008FE39788C04218F5DD9888888EC71FEE3462760E03A4770039
EB88BFEEF081BE4E05DBAA56B46419611CC2C3ABBC958476AAC4D626CFC465A0BDEDDC38AD93B238CF4F06390
4EA76BBAB4BEDB3EC88AC9738CDBE91082B23D2E5C3219839758EB8F4EC5F75E2650C422B04347EA1B8804029
0B3F710C82F48B285D8A2C2622CFD626A2A2F30156CF59AE95088D4A5E9881B91764A3884EAD2B4E554219D67
10D09AF296BC29677BAD142008AC505DC442E24DA8ABEABABD4D7BA9E7A835FBDEE0AF9225CBE2E0AE933119
1D92102884ED8203AEA50E57E4042A897AA95B0EF0A7DE57141B0C3E0B803D7C587E80760427DA83CD06E70B0
99779F5208A1F1A496F3DFFF8C14DADA812866A0457B37CDA62893799156A557C914FBBAE7FEDE079BE8A7981
7A39606FD512F227022010FF4196AAAB8E15C24BCA32C64778387F75A505F18428A5D4809F7BD14FC34B2185
518A9ECCAF98AA7E7247A51AA65F1212B496EFB6AA3B37F0BAC8997D73730EC630E90812D8F80A2CBECD55EFF
47EBF578CF87C92D7EEEC4863CE0D21D06CC26BD3CA67A396168AFD09A5F6097587C34E809A8A6E6480E8EC41
02FC9DDB9CBE9A444A0292C1BBDB28A010223D11E38ECCB13AE613B1648370C108DD3EF191413EEA037B77AB7
E63F8F267286B4DBCB20FF90EB4FB4E5C6CB9266E1C579F6B1586FAB628A603AF3A49251447DC806A4901EF31
74C1EE9EC0A397BDF2FDE5624B97C4332C0D88EF74F2991DEF5CC065C9B8E949A10BC9E3CEF7CCA2BD9976595
F5DF814C769669157E10377E9015E2582088941619FC4B3A09EF8F3373D5978C85742CE4660D75C35617FC749
66A40BA8FE7D71CF7DEAB4F7AD987A3AD4170FF96C84DB083A3E1D368A51160D40EE6CE55CABA01D28A1419BA
CD5E92FB3B702F8571956F649D9EA922BDF6CD98365126D15A4CD27BF3CF515BBCDC8600593BEFFA4B7D5977C
7AF77E0050964E3612E

W = 1E44DD50F00E24D170C7425ADA4004B67F5784BAFA47C7E93BB2C9F64922711CC65998BAC411611F5D9E0
46B4295AC32494244C87BF3314DF13411F02C316F7F

Z = 8CC4BADCC047A06B396C4EA13D26E088A7C6F91E056EBBF3B7B4A131C17C8DB5F886A78562F27AB72B931 B3F55DBC65023BE9BCB24931BB26163D444D04216A5F2075A3F632AB224D33BFD99AC1496763BABC33EE6542 0810FE7CDE3C69371630B2EAE4F7AB30D23B4A38B5303A6693DE0C6B4D6A358B66F4E17834A2939EA9169B09 D945E2670A879D501533928623AD717148D3FF2F769648F22D7E39907B48991B8ADA001811100B5A95F7301A6 08181C09D3D9AA9DF90C35B37E367805B7C8FBE1677774EC67E5D0F85E4B59437C3A18D71F22128E5787827D 8E27990788661BE6E41E516B76BA4235A33B85F6D2B41788A1DFB272962E371797B3123F480EA1AA1E98F3133 68EE0241980A27B013AB14C00144529EE2C665E1376AD0C901162334881F1CEEAABABD687AE0244BE98D39100 576932FB9F83599A2F6E0C93EBF7883CBAA7BD9196ED86B61CA686C0A456DE62FBF247EE997B9CDAD7FEA51F3 6DEDEF28BE5BF74E7CB2ACCDB2471FAEFADE5259CF8FDA580CD11575B6443CEE53D8E1A683538EC20EE6FB44E D9F1CBCDB3C281075397CF6880216B4443A8E7F38D9A6FE5F724373EE077A59632E661058FC77ADEFBD902B39 6CCBCF72AC94BDF6B2AB0C43DC994228BB51EAF62E156D068834E6D10E8E5A9CED3ABAB7D4F89F86A09851593 DE28033A5BA3772406509D307FD8D925DB095C61E6B892C43AF1E18130E2FEBD9142764818C6C9665203CFC2F 86F1A5E6A3CA8E64405DF929F5B64307E0B4475125B7DA14512192F4E4AEBBAA2F8DB7248D96ABEFDB375B4F C8FACEEB96ACA326D8668484451259D5625B8FEBC9C91CFB67728D6149A0D1832FE29747AFE4D8C92237292E46 6ECF5B38ECF52DA9C0AFDA624A85F52994700346C419FD8C6DE7CEE5F5821702C8CC85CBC331BD258A767AE0E 71CA6F0E719BD08B9A930588A41570580B241789EDD420B50A8480E909D6B05DEB1FC382A0A7C13B9540259E7 2666747CB3A6282B29B2E56658B866976DF5A4A88777AB094528C5474BA2FBC14C0CDA5DFE47B3DDBDE7A4BF7 9000BA6CF71635F752E8CA7062EB96FAE66D0C22CD13455F8E3C43B420E0DADBBE25E9AA9338DDD4BD1501A19 B104E2AFD8B04F6FAD859188364533C2656024DD7827E802B6E9409A6F6C9654AEF63F6AE9C8DF692968B5D6C AF4C866CD195FDD30F5C7EEDA2F3336A9C07AA6487353C725D1A8C9B81FEB156078C68D15C09B04C79BBB64C1 A894B2053CF7FD91E91C2C270450D80947C6AE956184F83E816D67ACFA4D2C5308F70B82DCD44F90F68A72713 FC70731D437C22D2B016CCF8BE156D325974BFA3C4EB53F643A0CD7E92AD2DC05F6BB596F2B63C21BE426B8D 9C734BA154DD274478C5E60D275032B0A348967448F3136A4F88ABEAD5E43DBB6C4F1E5CDD22062B0759DC88 81CB9B56F29C36832FE911BA9B171E45A9C109C95E876685247C6EDA92B7C015DA05E90C219477D8F1ABCF35 F2FE82C89F474BAF70F84851B7CFDDEC318CB7EF76CE5E962E6FD4EC200826ED59E318C8FE2C6BDCDB445C13 40AFB69E95C5D66FA6967BC8C53F244B3E2EA1A3B80125582689B7916A4053F87AA1C86DDBDCE2C79250CC5F 96B1FA11C6B5E4B05DA526BBEE5F43FC432B9D67093A705F4C4449E2D9FACB014CBF6BD09D7933FCF3582D09 CB980034E4F68FC405FDADFA77DBC7B93198CBF65B51D254CD2A2CBDC860462BC8FFF2A616C1618585E57C72 ABB9A48C53305B664D0A779DE9908322A805A121550C530C2C99F01AD1397C307470596838E11746F2DA3CB6A AA7F66DE2115DC8B9DA5D549960F3AE98E0D02BD43DEA3FF9E5F61140A576C87DC66194F8F3C0B8F9923EFE6F BF4FE78981045E18341FEDD5C540D24D36CD04D4D7061C9ADFB94F4BBA64A605EA93D02B4C2952AC38650CB32 A32D25E61781165995980EE0DA8998D116C5E195BCF13DD31F61E5879A8D391558D7567DD54960DA0C8E02CCC F93453A6767399647A2D576573FBFE77AA0E41DA1B1D90AFCB7E3FCF7D1E256FAAA716F43E637417B1231B499 42FF9A5E3399A15F48EADEA90D0810A39ACFAE4E3662C7B61C9F834CFB5F889D38DC222C5A91E69660D1534D9 270A2B1958188A7B09C27BC65DC05C1F08033AD6B2B881D5D4A63783EE5B5131994B2EAA14E3259941394F379 E7D2373A4A35BE8FA2773A551E51FD6FB209F5DCA5F6923EA1496CF3C136282425E7EA848C32800AD32B98250 35FF023445BE2E9E394E6750B7424BEEA531ECE67CE9220463265C82342515C626E89DB8940402AEAB744F77D A6141B149FF2D282873CF3A3D4EAE8BF33D7DE5A67C906B740FA6DA2393C32C8A1CEE06530D27221EEA27C8F5 FC7C68B0D18EBA16F8C025D8DC4013815233396FD4432E3054463B73D61F6DBBD4529404BCFB4127428F7172B3 6FCEBD495C19B10DBFAB629025F6C55219139D66DA304982D468311C28820B1C8265525572579259O2F2991F0 11D22F3C7478560A09431B2209F42CF60C2C5F9277D4B53652903FD33B11ED4EABAF1E4603683F390E5CA3EF9 BABFC7D6098D300A8AA3EB8B9061A34C2CD34DA1DF407C5DB2311CE22A7F1348A3D46F8B937FA8ACF3ADCB804 68276843FB4EBB4C512E35189A7901635DEFD9F24DD9301AECEED42854BF127EB1EC52AF416D82096E7B6E1 A2C8E1345D5803F0C337F16BEDC
r_1 = 0F274329DE32A41AB862AA6F2A133003999DDABB4EE9B9DA184C46159429C90BE93D43B365E8C6D4709EB A73F9095CB34CD9CAE216B6581F700E8F698C6E4806
K_s = D411C17E9EE99AC3C9EA219444EAF16C98E6C501E66EB8F3F9EA44371E623A90A3574484217B720ECAD52 209C61A1A25A76B112B2E2C483E7CD49B459261E8C2
K_i = E532EA72755FBAE2EE90F898BF74DEC92B8C0CFE583AF0EC667AA11500949C9A
K_m = 350FB5D79B79A7E52696FEC3E393781FE33B4FCE47D5237E30DB1C9A3E414641
o_A = F81DF642047CB3E6839B74C90769F11A877BDC2F8E0C8422AA306342E1DB8322DDFD87E99399F8E7DA97B 19FA0AD1F57C30FE9EB552094D33B9D68F21FD237A0
o_B = 86823B6BD9A3B05632D596CF95A2DE0B6F7390E6674F89C0799C2ECF1E2A96AD011F27C0C54AFD2E14811 E3D91E681F81D76BD227055968EE7DF0E9E37152110
A'_2 = 9828A952FC383373C545645A0F55566563E6388A7E4C4B4B9A2CA6B9D44FED5C5E43515FE3FAE29F8454 52F415EB747969C9116209B83D6A2B3F4FF0B9A0AAB7
A''_2 = 2A3A220C175BAF8CD0992F74E7932FA1A358D57EB5E23466D7542D5C430F344435E61830CBB6F18263CD C8892A8B7A803DD59DF3D6508B2799A3F3BE2D95A0A4
u_2 = 2548B0FDCBE747981F69F7B49839F0F08D18B797C3D1D3071DCD969EC504A864FC5921A6DAC5D4743412D 115F360A7604BDC0978875352377D54B4B0820B51AF
v_2 = D24C427D3DA227B001A8CD18FA9B0872A3B2E650A11B726A4A6C63B4F5018636243AD4F8A91791773EBC1 4E26B05D6A2AF834F1A15D3ED48C87C4FC43432F50F