Contents

Page

Introduction

The Algebraic Eraser™ (AE) cryptographic suite is an implementation of public-key cryptography which leverages the structure of the Braid group to execute a secure Diffie-Hellman type key exchange. The security of the suite is derived from the difficulty of solving sets of simultaneous conjugacy equations in the Braid group. The core one-way operation of the suite can be executed quickly on resource-constrained systems, making the AE suite appropriate to secure RFID Tag authentication for both active and passive RFID Tags.

This document specifies the security services of the AE cryptographic suite that can be used for an authenticated key exchange protocol.

SecureRF, Ironwood Key Agreement Protocol, Ironwood KAP, and Algebraic Eraser are trademarks, registered trademarks or service marks of SecureRF Corporation and used herein with permission.

Algebraic Eraser Over-the-Air Authentication

1 definitions, symbols and abbreviated terms

1.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts) and the following apply.

1.1.1 asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item

NOTE: The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.

[ISO/IEC 9798-5:2009, definition 2.3]

1.1.2 hash function
a function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:
* it is computationally infeasible to find for a given output, an input which maps to this output;
* it is computationally infeasible to find two different input which map to the same output.

NOTE: Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000, definition 3.5]

1.1.3 private key
private data item of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity

[ISO/IEC 9798-5:2009, definition 2.21]

1.1.4 public key
public data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity

[ISO/IEC 9798-5:2009, definition 2.23]

1.1.5 random number
time variant parameter whose value is unpredictable

[ISO/IEC 9798-1:2010, definition 3.29]

1.1.6 response
procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant

[ISO/IEC 9798-5:2009, definition 2.25]

1.1.7 secret parameter
number or bit string that does not appear in the public domain and is only used by a claimant

NOTE: For instance, a private key.

[ISO/IEC 9798-5:2009, definition 2.26]

1.1.8 verifier
entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication or for engaging in verifying a signature of a given message and signer

NOTE: Adapted from ISO/IEC 9798-5:2009.

1.2 Symbols

For the purposes of this part of ISO/IEC 29167, the following symbols and abbreviated terms apply.

PUB_i	Interrogator public key
PRV_i	Interrogator private key
PUB_t	Tag public key
PRV_t	Tag private key
CERT_t	Tag certificate containing PUB_t
K	shared secret between Interrogator and Tag resulting from AE key exchange protocol
H(K)	hash of the shared secret (K)
s	Column Vector used in Ironwood KAP
L	length of data used to authenticate Tag to Interrogator
B_N	Braid group of size N with $\{b_1, b_2, \dots, b_{N-1}\}$, the Artin generators
$CB(b_i^{\pm 1})$	N-variable colored Burau matrix associated with $b_i^{\pm 1}$
F_q	finite field of q elements (where q = p^k, for p (prime) and $k \geq 1$, e.g 2^r)
S_N	permutation group on N symbols; $\sigma \in S_N$, can act on $CB(b_i^{\pm 1})$, the result is denoted ${}^{\sigma}\left(CB(b_i^{\pm 1})\right)$
T	values, $\{\tau_1, \tau_2, \dots, \tau_N\} \subseteq F_q$, a collection of invertible elements, the notation $\downarrow_{T-\mathrm{values}}$ indicates replacing variables with the T – values.
$\star$	E-multiplication as defined in Annex C.
M_*	The seed matrix public parameter used to generate private keys

1.3 Abbreviated terms

AE	Algebraic Eraser
AEDH	Algebraic Eraser Diffie-Hellman
AEKAP	Algebraic Eraser Key Agreement Protocol (aka AEDH)
AEDHP	AEDH parameter
AEHash	Algebraic Eraser Cryptographic Hash Algorithm
CCR	Commitment challenge response

CRC	Cyclic redundancy check
CS	Cryptographic suite
CSI	Cryptographic suite identifier
EBV	Extensible Bit Vector
MAC	Message Authentication Code
RFU	Reserved for Future Use
RN	Random Number
TAM	Tag authentication message

2 Cipher introduction

The Algebraic Eraser is a group-based cryptographic tool [1] invented by Anshel, Anshel, Goldfeld, and Lemieux [2]. Like other group-based cryptographic protocols [3,4], the Algebraic Eraser uses non-abelian group operations to construct secure keys. In particular, the Algebraic Eraser uses the braid-group, B_N and has a Diffie-Hellman type structure. An introduction to the underlying algorithm, the Ironwood Key Agreement Protocol (Ironwood KAP) variant, and the defining parameters of the protocol follow and additional description is provided in Annex D, with test vectors in Annex C and specific protocol parameters listed in Annex F.

The one-way function underlying the Algebraic Eraser Diffie-Hellman construction can also be used for other cryptographic primitives. One such construction is a cryptographic hash function, AEHash [10], which is also used in this standard. The description of AEHash is provided in Annex D, with test vectors in Annex C, and specific protocol definitions in Annex G. The Hash is used to protect against an attack that requires access to the shared secret [9].

The protocol describes a method to authenticate Tags based on *public keys* whose security is related to the hard problem of solving simultaneous conjugacy equations in the Braid Group B_N. This specification focuses on Tag Authentication and defines two profiles (which differ only in how the Interrogator obtains the Tag's public key).

Profile [i] (Tag authentication only):

The Interrogator begins the key exchange already in possession of the Tag's public key (PUB_t). The Interrogator produces a one-time use random private/public key pair (PRV_i/PUB_i). The Interrogator then sends PUB_i to the Tag and requests an authentication of length L. The Tag computes the shared secret K using PRV_t and PUB_i. The Tag then computes the Hash of K sends the requested portion of H(K) of length L to the Interrogator. The Interrogator uses PRV_i and PUB_t to arrive at K, computes the Hash H(K), and checks against the response from the Tag. If its result matches the block of length L, the Tag is authenticated.

Profile [ii] (Certificate on Tag):

The Interrogator begins by obtaining the Tag's certificate (CERT_t). The Tag sends its certificate, which contains its public key (PUB_t), to the Interrogator. The Interrogator obtains PUB_t from CERT_t. The protocol then follows the flow of Profile [i] however it utilizes the Ironwood Key Agreement Protocol as documented in Annex D.2 which adds an additional field to the authentication response. This protocol also allows for tracking the Tag via the Tag's fixed CERT_t.

Once the shared secret is generated it can be used to encrypt another set of data, which would allow for a secure communication channel in addition to Tag authentication, however these features are out of scope for this standard.

Issues such as the key infrastructure required to support the techniques described in this Cryptographic Suite are outside the scope of the document. They remain, nevertheless, important considerations when assessing the suitability of any Cryptographic Suite for a given application. As this Cryptographic Suite is a Public Key system it does not require maintaining a secure database of secret keys.

2.1 Asymmetric cryptography with the Algebraic Eraser

The AE Key Exchange Protocol (AEKAP) enables two users, Alice and Bob, to evaluate a shared secret using their own private key and the public key of the other user. For the purposes of this specification, a Tag plays the role of Alice and an Interrogator plays the role of Bob. The following definitions are used in the description algorithm which provides the security for this protocol.

The AEKAP contains the following public information that define a particular keyset (this can be considered the AE equivalent to a Diffie-Hellman group parameter prime, or ECC curve parameters):

– A fixed matrix with elements in the finite field, $M_* \in GL(N, F_q)$,
– A set of conjugates in B_N for each group, Tags $\{c_1, c_2, \ldots, c_k\}$ and Interrogators $\{d_1, d_2, \ldots, d_\ell\}$.
– A set of T-values (an array of N entries where each entry is in the field F_q)

This public information (matrix, user conjugate set, and T-values) make up the keyspace for AEKAP. The conjugates should be chosen with specific high order permutations to protect against certain classes of weak keys [8]. For two users to communicate they must share a common keyspace. This is similar to Diffie-Hellman where you choose a common prime, or in ECC where you choose a common curve. In AEKAP you choose a common matrix and conjugate set. The main difference in that there are two sets of conjugates in the set and each user must choose theirs from the opposite set (e.g., Tags choose from set A, and Interrogators from set B).

The public parameters are generally chosen ahead of time and published for users to use (see Annex C). For a 2^{80} security level parameters come from B10F256 (a braid with 10 strands and a field over 256 (2^8)).

The user private/public key pairs of the AEKAP are derived from the public parameters. User Private data have two components

– The Private key is an NxN Matrix where each of the N^2 entries is a member of the field F_q -- computed based on the public keyspace matrix M_*.

– The conjugacy set consists of a random product of a sequence of the user's conjugates, again in the case of Alice, $c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot c_{i_{L_A}}$ which is itself an element in the Braid group.

In other words the user randomly chooses L_A conjugates (and their inverses) from the user's conjugate set in the keyspace and combines them together. This combination can happen in real time, or, because the result is just another entry in the Braid group (e.g. another conjugate) it can be pre-computed and reduced for storage.

To compute the inverse of a braid you reverse the order of all the Artin generators and then you take the inverse of each. For example, if you had the braid $b_1\ b_2\ b_3^{-1}\ b_2^{-1}$, to compute the inverse you reverse and inverse the generators resulting in $b_2\ b_3\ b_2^{-1}\ b_1^{-1}$.

Alice's public key is obtained via E-Multiplication of the Private Key with the Conjugacy Set. The result of the E-Multiplication is a pair: an NxN matrix where each entry is a member of the field F_q, and a permutation of N entries (S_N). This is the composition of the Public Key.

Obtaining the shared secret/exchanged key:

– Alice receives Bob's public key (M_B, σ_B), an NxN Matrix and a Permutation, and computes the shared secret by a combination of matrix multiplication first with their own Private Key and then using E-Multiplication to iterate down their conjugacy set. The result is the shared secret, an NxN Matrix and a Permutation.

– Likewise, Bob receives Alice's public key and computes the equivalent computation, performing a matrix multiplication and then an iterative E-multiplication down their conjugacy set. As before, the result of this computation is an NxN Matrix and a Permutation.

.

2.2 Encoding Algebraic Eraser Keys and Shared Secrets

The Algebraic Eraser uses Matrices, Permutations, and Braids. The following define how these data structures are encoded and transferred between Tags and Interrogators.

2.2.1 Encoding Matrices

An NxN Matric has N^2 entries. Each entry is a member of a the finite field F_q (a number from 0 to q-1). The most compact method to encode this matrix is to "bit pack" the entries. For example, if N is 16 and q is 32 (aka B16F32) each of the 256 matrix entries uses five (5) bits. Therefore the encoding would occur by taking the five (5) bits of the first matrix entry and combine them with the first three (3) bits of the second entry into the first matrix octet. For the second octet take the remaining two (2) bits of the second entry, all five (5) bits of the third entry, and the first (1) bit of the fourth entry. This process continues until you reach the end. Any extra bits in the final octet must be zero.

Note, however, that, not all entries in the matrix are used. In particular, due to the way Algebraic Eraser Public Keys are generated the last row in the matrix is always all zeros, except for the last entry. Therefore, when packing the matrix you should elide the "row of zeros". I.e. you pack rows 1 to N-1 as above, but then for the Nth row you skip the first N-1 entries and jump directly to the Nth and final entry in the matrix.

2.2.2 Encoding Permutations

A Permutation is a set of N entries from 0 to N-1. Packing a Permutation uses the same "bit packing" process as with matrices.

Like the matrix encoding, the last octet of the encoded permutation should pad with zero bits as necessary.

2.2.3 Encoding Braids

As braids are not transferred between communicants the encoding of braids is currently left as a local matter. However, it is recommended that implementors consider encoding braids in their own "bit packed" format in order to reduce the amount of required storage space. Each braid element contains an Artin generator (a number from 1 to N-1) and an exponent (+1 or -1). This can be encoded by taking one bit for the exponent (a value of zero (0) signifies an exponent of 1, value of one (1) signifies an exponent of -1) and then as many bits as necessary to encode the generator. Note that there is no Artin generator b_0, so we encode b_1..b_{N-1} using the numbers 0 to N-2.

For example, using B10 (N=10), the braid generator requires four (4) bits; adding the exponent makes that five(5) (NB: this is true for all braids where N=9 through N=16). So if you had a braid of b_1 b_2 b_1^{-1} this would be encoded as the binary: 00000_2 00001_2 10000_2, which packs into hex 00_h 60_h. (Notice the last octet is padded with a single zero bit).

2.3 Required Algebraic Eraser Parameters

This specification requires implementation of AEDH parameters for interoperability. To conform to this specification a Tag shall choose and implement one AEDH parameter keyset, and an Interrogator shall implement all required keysets. For security level 2^{80}, Tags and Interrogators shall implement B10F256. The exact keysets (Matrix, Conjugates, and T-values) required by this specification are documented in Annex C.

NOTE: Security levels listed here are derived from the calculations of security from [2] and are based on the work factor to break the keys or messages. As with all asymmetric algorithms the security level is not the same as the key size.

Tags and Interrogators must also implement the same Hash function. The specific parameters of AEHash are documented in Annex G.

In general a Tag only needs to implement a single AEDH parameter to be compliant and expects the Interrogator to determine that either by the certificate (in which the keyset parameter used by the Tag is explicit) or by other out-of-band means (however the Interrogator acquires the Tag public key PUB_t). Interrogators are expected to implement multiple parameters in order to authenticate multiple Tags and discover the keyset parameter via implicit (profile [i]) or explicit (profile [ii]) notification.

The parameter in use defines the exact sizes of the matrix and permutation to be sent by the Interrogator to the Tag which means an explicit length parameter is not required. If the data is the wrong length the Tag shall reply with an error.

3 Parameter Definitions

Parameter	Description
FN[7:0]	The number of fragmentations and last-fragment marker: • [7] : last fragment bit (set when this is the last fragment) • [6 :0] : current fragment number
AuthType[1:0]	This shows the authentication type in the authentication procedure. The values are as following: ▪ 00_2: reserved for mutual authentication ▪ 01_2: reserved for the use of Interrogator authentication ▪ 10_2: Tag authentication ▪ 11_2: RFU
AuthStep[2:0]	This shows the step number in the authentication procedure. The values are as following: ▪ 000_2: Step 1 of Authenticate procedure ▪ 001_2: Step 2 of Authenticate procedure

Parameter	Description
	▪ 010_2-111_2: RFU
AEDHP[Variable]	AEDH parameter. This field consists of the packed public key matrix followed by the packed public key permutation. The length of this field is dependent on the agreed-upon Keyset Parameter
$Cert_x$[Variable]	The digital certificate of x. x can be Tag, Interrogator or TTP.
Profile[2;0]	This shows the explicit profile to use. The values are the following: ▪ 000_2: Profile [i] ▪ 001_2: Profile [ii] ▪ 010_2-111_2: RFU

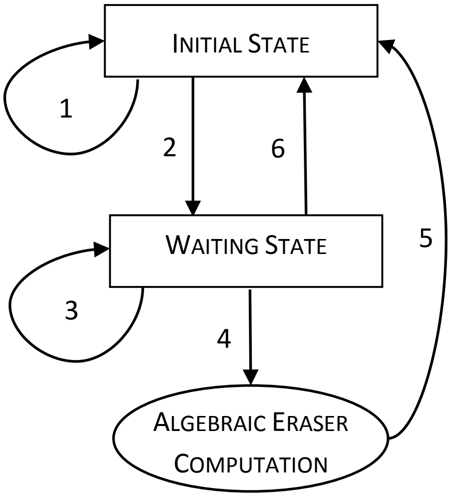
Table 1 -- Definition of parameters

4 State diagram

This part of ISO/IEC 29167 shall implement an INITIAL state and a WAITING state.

The Tag used for the AE cryptographic suite will be powered up in its INITIAL state, and return to this state after a successful or unsuccessful authentication. Timeout controls could be added to the key exchange at the discretion of the implementer for added security. However, the Tag will resume function in the INITIAL state after such time. The WAITING state is used if the Interrogator fragments the authentication request message and shall be used to wait for a complete authentication request. Once the request is complete (all fragments have been received) then the Tag will perform the computation and return to the INITIAL state.

The transition between states is specified in Figure 1 - Tag State Diagram.



1. TAM-1.0 CERTIFICATE REQUEST/RESPONSE (WITH OR WITHOUT FRAGMENTATION BY TAG)
2. TAM-1.1 REQUEST
3. TAM-1.1 RESPONSE (REQUESTING NEXT FRAGMENT)
4. WHEN THE REQUEST IS COMPLETE (ALL FRAGMENTS RECEIVED), TRANSISION TO THE AE COMPUTATION
5. TAM-1.1 RESPONSE WITH AUTHENTICATION RESULT
6. ERROR MESSAGE OR TIMEOUT

Figure 1 – State machine of Algebraic Eraser Crypto Suite

5 Initialization and resetting

This Cryptographic Suite does not require initialization. The behavior on reset is to return to the initial state.

Implementations of this suite shall assure that all memory used for intermediate results is cleared after each operation (message-response pair) and after reset.

The cryptographic suite shall be reset on power-on.

6 Authentication

The authentication protocol of this crypto suite uses a challenge-response protocol described below. In particular, it describes the use of the Algebraic Eraser AEDH key agreement scheme to establish a secure channel and simultaneously authenticate the Tag to the Interrogator (Tag Authentication) by using a Hash to protect from disclosing the shared secret computation.

6.1 Tag Authentication

The Tag authentication messaging sequence (TAM) of this crypto suite outlined in Figure 2. This TAM is used for all Profiles of this mechanism, with Profile-specific details included in each of the following subsections.

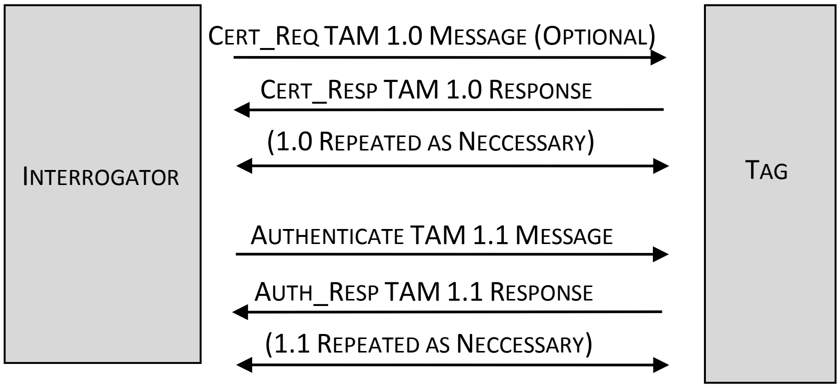

INTERROGATOR
CERT_REQ TAM 1.0 MESSAGE (OPTIONAL)
CERT_RESP TAM 1.0 RESPONSE
(1.0 REPEATED AS NECCESSARY)
AUTHENTICATE TAM 1.1 MESSAGE
AUTH_RESP TAM 1.1 RESPONSE
(1.1 REPEATED AS NECCESSARY)
TAG

Figure 2 - Message exchange for tag authentication for all Profiles of the AE crypto suite

6.1.1 Certificate Request (TAM 1.0 Message) (OPTIONAL: Profile [ii])

The Interrogator may have the Tag's public key (PUB_t) via out of band mechanisms (profile [i]). Alternately, if the Interrogator does not have it, then it must request it from the Tag (profile [ii]). The message consists of the AuthStep (000_2) and next fragment number.

	AuthStep	Padding	Offset	Length
# of bits	3	5	16	16
description	000_2	RFU	Offset into	Length of requested

			response	response

Table 4 - CERT_REQ (TAM 1.0 Message)

The fields of the TAM 1.0 message shall have the following meaning:

a) AuthStep: This field shall be three (3) bits in length and specifies the step number in the procedure. Each authentication procedure requires a pre-determined number of steps. In the TAM 1.0 Message, the value is 000_2.
b) Padding: 5 bits that shall remain 0
c) Offset: This field shall be sixteen (16) bits in length and specifies the offset (in bytes) into the CERT Response message to send back to the Interrogator.
d) Length: This field shall be sixteen (16) bits in length and specifies the length (in bytes) that are requested by the Interrogator (starting from the offset). A length of 0 implies the Tag shall send the complete response message.

NOTE: The Interrogator completely controls fragmentation because it is best able to ascertain bitrate and transmission losses. As the TAM 1.0 Response (Certificate response) is a static message, the Tag need only send back the desired portion.

6.1.2 Certificate Response (TAM 1.0 Response) (Profile [ii])

The TAM 1.0 Response consists of a Length, the response profile, Padding, the Maximum Fragment Size, and the Tag Certificate.

	Length	Profile	Padding	Max Frag Size	CERT_t
# of bits	16	3	5	16	Variable
description	Message length	Profile Version	RFU	Maximum Fragmentation Size	Tag Certificate (or fragment thereof)

Table 5 - CERT_REP (TAM 1.0 RESPONSE)

The fields of the TAM 1.0 response shall have the following meaning:

a) Length: This field shall be 16 bits in length and specifies the length (in bytes) of this response. This field shall be the requested length or the actual available data length, whichever is less. The length is only the length of the returned data, which includes the Profile, Padding, Max Frag Size, and Certificate data (or portions thereof). When the data is fragmented the Profile, Padding, and Max Frag Size shall only be sent in the first fragment in which they occur. I.e. consider the Profile, Padding, Max Frag Size, and

Certificate data as a single, constant, static buffer, and the fragmentation and length break apart that single buffer.

b) Profile: This field shall be three (3) bits in length and specifies the AE Profile in use. For this specification this should be Profile [ii] (binary 001_2). It is sent only in the first fragment.
c) Padding: This field shall be five (5) bits in length which shall always be zero. It is reserved for future use. It is sent only in the first fragment.
d) Max Frag Size: This field shall be sixteen (16) bits in length and specifies the maximum fragmentation size supported by the Tag. The Interrogator shall never send a fragment larger than this size. If this size is zero (0) then the Tag is indicating support for any fragmentation size (including support for complete, unfragmented messages).
e) CERT_t: This field specifies the digital certificate of the Tag (or fragment thereof)

When the Interrogator receives the CERT_REP message it reconstructs the CERT_t data for processing. The Interrogator can immediately determine the keyset parameters and PUB_t by parsing the certificate. It can also verify the authenticity by validating the certificate.

Note that when the Interrogator issues and completes a CERT_REQ/CERT_REP cycle, this indicates the use of Profile [ii]. Therefore the Authenticate request/response messages will use the Profile [ii] data instead of the Profile [i] data.

6.1.3 Authenticate (TAM 1.1 Message)

The Interrogator's authentication request (TAM 1.1 MESSAGE) is composed of an AuthStep (001_2), AuthType (10_2), the Interrogator's single-use public key (PUB_i), the size of the block H(K)[l] requested for authentication. The recipient Tag will use PUB_i as part of the Algebraic Eraser Key Exchange.

	AuthStep	Pad 1	FN	Length	AuthType	Pad 2	PUB_i	Size
# of bits	3	5	8	16	2	6	Variable	8
description	001_2	RFU	Fragmentation number	Message (or fragment) length	10_2	RFU	Interrogator Public Key	Auth Size

Table 8 - AUTHENTICATE (TAM 1.1 MESSAGE)

The fields of the TAM 1.1 message shall have the following meaning:

a) AuthStep: This field shall be three (3) bits in length and specifies the step number in the procedure. Each authentication procedure requires a pre-determined number of steps. In the TAM 1.1 Message, the value is 001_2.
b) Pad 1: This field shall be five (5) bits in length and shall always be zero. It is reserved for future use.
c) FN: This field shall be eight (8) bits in length and specifies the current fragmentation number. To prevent retransmission of the complete message in the case of a transmission error the message can be broken into multiple fragments. The initial message starts at fragment zero (0), and increments with every additional fragment. When the final fragment is sent the high bit (80_h) gets set. In the event of an error in transmission the Tag will respond with a message that will cause the Interrogator to resend the same fragment (which implies not incrementing the fragment number).
d) Length: This field shall be 16 bits in length and specifies the length (in bytes) of this message or fragment. The length is only the length of the following data, which is the Auth Type, Pad 2, Public Key, and Size. When the data is fragmented the Auth Type and Pad2 shall only be sent in the first fragment, and the

Size shall only be sent in the last fragment. If this value is larger than the Tag supported Max Frag Size then the Tag shall return a FRAG_TOO_BIG error.

e) AuthType: This field shall be two (2) bits in length and the values of the AuthType field are as follows:
   - 00_2: reserved for the future use of mutual authentication
   - 01_2: reserved for the future use of Interrogator authentication
   - 10_2: Tag authentication
   - 11_2: Other

   This field is only sent in the first fragment (fragment 0)

f) Pad 2: This field shall be six (6) bits in length and shall always be zero. It is reserved for future use. This field is only sent in the first fragment (fragment 0)

g) PUB_i: This field specifies the Interrogator Public Key to use in the AE Key Agreement. This is the packed matrix and packed permutation. The Tag knows exactly how big this data is because the size is completely defined by the B_NF_q in use.

h) Size: This field shall be eight (8) bits and specify the length in bits of the authentication reply. This field will only get sent in the last fragment.

The Tag, upon receiving a complete Authenticate Request, will read the PUB_i and compute the shared secret K, compute the Hash of the shared secret H(K), and respond with the requested authentication response of Size bits of H(K). In Profile [ii] the Tag will also include the column-vector s in the response. In the event of a fragmented message, the Tag will respond with a TAM 1.1 Response signaling whether the fragment was received correctly or not and wait until the complete request is received. Note that an implementation may begin processing PUB_i prior to a complete Authenticate Request being received, thereby limiting the size of the FIFO input buffer required. This implementation choice will drive the size of the maximum supported fragment size.

6.1.4 Authenticate Response (TAM 1.1 Response)

The Authenticate Response (TAM 1.1 RESPONSE) allows a Tag to authenticate to the Interrogator or signal that the fragmented request message was (or was not) successfully received. Once the Tag receives a complete request message it computes the shared secret K, computes its Hash H(K), and sends a block of the hashed shared secret specified in the TAM 1.1 Message (H(K)[l]).

	FN	H(K)[l]	s
# of bits	8	Variable	Variable
description	Next requested fragment	Authentication code	s Column Vector

TABLE 9 - AUTHENTICATE RESPONSE (TAM 1.1 RESPONSE)

The fields of the TAM 1.1 response shall have the following meaning:

a) FN: Next Requested Fragment. If the request message is received correctly (the air interface received it correctly and the fragmentation number is the next in the sequence) then this field will contain the next fragment (i.e., if the request was fragment zero (0), this field will contain one (1)). If the request message is not received correctly (an error is detected or the fragmentation number is out of sequence) then this field will contain the correct fragment number (e.g., if the request was fragment three (3) and the air interface indicated an error in the message, this field will contain three (3)). This rule is true even when the request specifies this is the last fragment (high bit 80_h is set). Note that this does imply the tag needs to keep count of the expected next fragment number and shall verify that the correct fragment was sent.

b) H(K)[l]: This field contains the Size bits of the Hash of the computed shared. It is only sent in response to the final fragment (the fragment number high bit, 80_h, is set). If Size is not a multiple of 8 bits than this field shall be padded at the end with 0 bits until the next full byte.

c) s: This is the s column vector of the Ironwood KAP, included only in Profile [ii]. It requires $N * \log_2 q$ bits to encode the packed column vector, which shall be padded at the end with 0 bits until the next full byte. This data is only sent when the Tag is using Profile [ii] and is only sent in response to the final fragment of the Authenticate request.

6.1.5 Message Fragmentation

Some times messages in this specification can get very large. In order to reduce the amount of retransmission that may be required messages can be fragmented into smaller pieces. In the event of a transmission error this allows retransmission of only the fragment instead of requiring retransmission of the entire message.

Fragmentation is always controlled by the Interrogator because it always has a better capability to detect the environment, however the Tag may signal the maximum supported fragmentation size in the TAM 1.0 response based on its implementation. (Note that an Interrogator that acquired the Tag PUB_t data out-of-band shall also acquire the Tag max fragment size by the same out-of-band method). The Tag must be capable of handling fragmented messages of any size up to and including the maximum supported size reported. This does imply that a Tag must be able to accept a single fragment of e.g. 100 bytes or 100 fragments of 1 byte and all points in between, however the Tag controls how large this can get (based on how much data it can buffer during processing).

When messages are fragmented all fields prior to the fragmentation number and message length are repeated in every message. Every field after the fragmentation number and message length are only sent once. This effectively builds a single message payload of all the fields, breaks it up into pieces, and then sends each piece as a fragment, starting with fragment zero. If a fragment is received successfully then the receiver responds and requests the next fragment; if a fragment is not received successfully it responds re-requesting the same fragment.

When both actors (Interrogator and Tag) behave correctly the fragments will start at 0 and count until the last fragment; which is signalled by setting the high bit. For example if there are three fragments they will be sent as hex values 00_h, 01_h, 82_h. The responder will notify the sender whether the fragment was received correctly or needs resending by incrementing the fragment number when it was properly received and not incrementing when it was not properly received.

A bad actor could send fragments out of order. This shall be considered a fatal error and result in a reset to the initial state.

7 Key table and key update

The Tag shall store in memory the following values:

– The private data value PRV_t which is used by the Tag for the computation of the response. Note that this is in two parts, the Private Key which is a Matrix, and the conjugacy set which is a Braid.

– The public key value PUB_t which is used by the Tag for communication with the Interrogator.

– The keyset T-values

– Optionally the signed public key value, CERT_t, which the Interrogator can use to verify PUB_t.

This cryptographic suite does not support other cryptographic functions such as updating the key.

Annex A
(informative)

Test Vectors

A.1 Algebraic Eraser (AEDH) Test Vectors for B10F256

The following sections show examples using the B10F256 keyset in Annex C.1.

A.1.1 Tag Private Key

The Tag Private Key is a Matrix that looks like:

```
213  34 151  79  72 107  97  59 164   1
 79  73 138 230  68  86 173 115 132  71
123 184  36 190 157 171 120 169 193 219
  0  15  75  59 133 166 202 144 143  48
 55  10 228 208 176 180  67 250  43  50
 31 170  65  45 159 255 173  92 210  96
  9 195 171  29 119  58 195 249 194  26
 12 162  25  15  20  85 207 154  76 123
 34 182  82  35 186 153  78 221  79  24
  0   0   0   0   0   0   0   0   0  61
```

And encodes into the following octet string for ease of storage:

```
d5 22 97 4f 48 6b 61 3b a4 01 4f 49 8a e6 44 56 ad 73 84 47 7b b8 24 be 9d ab
78 a9 c1 db 00 0f 4b 3b 85 a6 ca 90 8f 30 37 0a e4 d0 b0 b4 43 fa 2b 32 1f aa
41 2d 9f ff ad 5c d2 60 09 c3 ab 1d 77 3a c3 f9 c2 1a 0c a2 19 0f 14 55 cf 9a
4c 7b 22 b6 52 23 ba 99 4e dd 4f 18 3d
```

It was derived from the Keyset Seed Matrix M_* using the following choices for α_i:

$$\alpha_0 = 163, \alpha_1 = 68, \alpha_2 = 46, \alpha_3 = 204, \alpha_4 = 30, \alpha_5 = 34, \alpha_6 = 153, \alpha_7 = 213, \alpha_8 = 135, \alpha_9 = 207$$

A.1.2 Tag Conjugacy Set

The Tag Conjugacy Set is created by randomly choosing conjugates and their inverses. This example key was created using the following choices (numbered 0-31) from the Tag Conjugates in Annex C.1.4:

$$c_0 = 12(inv), c_1 = 8, c_2 = 27, c_3 = 12(inv), c_4 = 15(inv), c_5 = 25(inv), c_6 = 28, c_7 = 7(inv), c_8 = 16,$$

$$c_9 = 4, c_{10} = 31(inv), c_{11} = 5(inv), c_{12} = 2, c_{13} = 5, c_{14} = 5(inv), c_{15} = 2, c_{16} = 4(inv)$$

A.1.3 Tag Public Key

The Tag Public Key is a Matrix and Permutation which can be computed via E-Multiplication of the Private Key with the Conjugacy Set, starting with the identity permutation. The resulting Public Key Matrix looks like:

```
194 228 126  60  34 188 184 184  47 222
133  80 198 251 203 209  21  46  49  48
137 245 194 214  62 239 210 207 120   8
 13  12  42 117  22 199  44  59 153 119
  7 125 179 128  64 182  31  90  80 169
 66  45 144 178 138  99  23 217  94 128
168 110  86 198 141 205 254 108 224 144
247 150 173  28  80  92 109  86 233 245
 54 183  32 224  46 178  21 120  69  40
  0   0   0   0   0   0   0   0   0  61
```

And the permutation is:

```
0 1 2 3 6 7 9 5 8 4
```

This encodes into the following octet string which gets sent over the air:

```
c2 e4 7e 3c 22 bc b8 b8 2f de 85 50 c6 fb cb d1 15 2e 31 30 89 f5 c2
d6 3e ef d2 cf 78 08 0d 0c 2a 75 16 c7 2c 3b 99 77 07 7d b3 80 40 b6
1f 5a 50 a9 42 2d 90 b2 8a 63 17 d9 5e 80 a8 6e 56 c6 8d cd fe 6c e0
90 f7 96 ad 1c 50 5c 6d 56 e9 f5 36 b7 20 e0 2e b2 15 78 45 28 3d

01 23 67 95 84
```

A.1.4 Interrogator Private Key

The Interrogator Private Key is a Matrix that looks like:

```
 53 208  52 191 244 116 127 180  54  69
159  96 203 189 236 252 164 199  10 104
156 149 253 236 131  47  70 158  73 139
122 207  76  15  88  71 118 101  25  49
236 135  51 192 155   9 155 218 209 154
 48 188 174  90  15 231 181 139 132 247
217  28 221 167 118  85 201  79 130 210
  2 193   4 108  65 231  17  26 242 167
208 200 106 107 132 116 115  34 113 105
  0   0   0   0   0   0   0   0   0  17
```

And encodes into the following octet string for ease of storage:

```
35 d0 34 bf f4 74 7f b4 36 45 9f 60 cb bd ec fc a4 c7 0a 68 9c 95 fd
ec 83 2f 46 9e 49 8b 7a cf 4c 0f 58 47 76 65 19 31 ec 87 33 c0 9b 09
9b da d1 9a 30 bc ae 5a 0f e7 b5 8b 84 f7 d9 1c dd a7 76 55 c9 4f 82
d2 02 c1 04 6c 41 e7 11 1a f2 a7 d0 c8 6a 6b 84 74 73 22 71 69 11
```

It was derived from the Keyset Seed Matrix M_* using the following choices for α_i:

$$\alpha_0 = 222, \alpha_1 = 199, \alpha_2 = 186, \alpha_3 = 164, \alpha_4 = 213, \alpha_5 = 210, \alpha_6 = 208, \alpha_7 = 223, \alpha_8 = 2, \alpha_9 = 28$$

A.1.5 Interrogator Conjugacy Set

The Interrogator Conjugacy Set is created by randomly choosing conjugates and their inverses. This example key was created using the following choices (numbered 0-31) from the Interrogator Conjugates in Annex C.1.5:

$$d_0 = 22, d_1 = 0, d_2 = 3(inv), d_3 = 11(inv), d_4 = 3, d_5 = 10, d_6 = 20, d_7 = 24, d_8 = 8(inv), d_9 = 25(inv), d_{10} = 0(inv), d_{11} = 21, d_{12} = 9(inv), d_{13} = 26, d_{14} = 13(inv), d_{15} = 21(inv), d_{16} = 9(inv)$$

A.1.6 Interrogator Public Key (computed from Private Data)

Using E-multiplication one can compute the Interrogator Public Key from the Private Data in the previous two sections. This computation results in a Matrix that looks like:

```
 76  59  67  60  26  52  57  44 124 218
 55 125 138 214 227  11 186 208 175 179
193 239  37 103 221  56  78 165 199 132
 18  69  48 100 126 222 181 133  98 246
 21 165  14 186 198 143 147 237  61  34
203 196 122 135  41 232  15  90 134 252
239 229 176 229   4 176 144 194 103 116
170 188  23 189 254  55 175  88 178 124
 36  44 100 109 128 255 245 139 228 196
  0   0   0   0   0   0   0   0   0  17
```

And a permutation:

```
2 3 1 0 4 5 6 7 8 9
```

This encodes into the following octet string which gets sent over the air:

```
4c 3b 43 3c 1a 34 39 2c 7c da 37 7d 8a d6 e3 0b ba d0 af b3 c1 ef 25
67 dd 38 4e a5 c7 84 12 45 30 64 7e de b5 85 62 f6 15 a5 0e ba c6 8f
93 ed 3d 22 cb c4 7a 87 29 e8 0f 5a 86 fc ef e5 b0 e5 04 b0 90 c2 67
74 aa bc 17 bd fe 37 af 58 b2 7c 24 2c 64 6d 80 ff f5 8b e4 c4 11

23 10 45 67 89
```

A.1.7 Computed Shared Secret

When you combine the Tag Public Key with the Interrogator Private Data you compute a shared secret that has a matrix that looks like:

```
 56 161 201 181  21  56 179  27 122 168
 10 132 136 145 193  61 177  74   3 163
  0  50 139 226 116  61 203  88 156 144
  1  85 206  43  27   4 106  11 127 231
246  20  19 171 118 135 167 110 238   7
  6 153 116 150 143  88   3  95 242 232
139 127 130 110 244 124 107 210  62 150
119 154  77 154 167 255 216  73  85 235
 60 190 220  26 150  81 242  95 183  19
  0   0   0   0   0   0   0   0   0 192
```

And a permutation that looks like:

```
2 3 1 0 6 7 9 5 8 4
```

Which encodes into the following octet string:

```
38 a1 c9 b5 15 38 b3 1b 7a a8 0a 84 88 91 c1 3d b1 4a 03 a3 00 32 8b
e2 74 3d cb 58 9c 90 01 55 ce 2b 1b 04 6a 0b 7f e7 f6 14 13 ab 76 87
a7 6e ee 07 06 99 74 96 8f 58 03 5f f2 e8 8b 7f 82 6e f4 7c 6b d2 3e
96 77 9a 4d 9a a7 ff d8 49 55 eb 3c be dc 1a 96 51 f2 5f b7 13 c0

23 10 67 95 84
```

Using AEHash, computing the hash of this string results in the following 256-bit hash:

```
d3 0b de b6 1c a8 6c 53 0e 9d 01 ae 7a 08 cb 18 57 22 2f ab 78 41 b9
3a 70 05 54 40 95 c9 10 ca
```

If Size = 27, then the tag would respond with 27 bits of the hashed shared secret, padding the result:

```
d3 0b de a0
```

A.2 Ironwood KAP Test Vectors

The following sections detail the Ironwood KAP protocol vectors with a B10F256 keyset. The keyset in question uses the following set of Tvalues (in decimal):

```
74 127 12 152 5 15 83 92 186 191
```

A.2.1 Tag Keys

Each Tag has two private matrices:

```
4b 28 45 49 3e bb ad 6b 8e be
6f 30 ac e9 f4 b2 0b bd 46 d4
02 45 74 b8 a4 d9 be 78 e8 67
e2 1a cf 26 ba cd ed 51 d6 9a
f4 f7 45 a4 7e 6c 20 05 a9 f8
16 86 be 61 f1 2a 42 38 19 c6
b4 cf 1f bb d6 80 1c 11 83 48
7b 7e 37 93 4b 59 77 24 1d de
d7 e6 f4 18 d3 fb 01 88 5c 36
7a 36 75 c3 e2 c1 aa 22 6a e5
```

and

```
31 64 21 7d 80 bc 18 c3 3f 3d
e7 e3 15 36 a9 f9 6f a5 8a b5
b8 fe f3 6b 04 c6 7d 37 a7 29
97 a0 e7 8e 2d a4 67 7a 33 02
7b 51 4c 75 c9 32 9e 8a 71 81
c9 72 5b 23 08 fb 48 cf b4 34
```

```
25 0f e2 de da 3a e8 31 3c a3
3e a8 d7 f4 d4 7f d7 9c 15 6b
5b 16 54 52 2d c5 4a a7 af 45
fa fe e3 05 4c a5 e1 49 1b c3
```

and two private braids:

```
08 8a 00 64 32 16 c5 b5 f1 32 56 c7 04 64 3a 56 c2 9d 0b 63 86 53 25
6c 7c 0c 85 31 e8 5b 1f 11 94 e9 5b 5f 03 a5 27 4a c2 32 99 09 5a da
f8 a5 6c 7c 60 64 29 8f 8b 5a f6 8c a7 4a da f8 00 44 32 14 c7 c0 02
21 0c 85 31 f0 11 0c 85 31 f1 19 4e 85 31 f0 53 1f 18 35 f1 19 4c 85
31 f0 4a d8 f8 8c 86 42 98 f8 9d 2b 6b df 11 10 c8 53 1f 07 a1 6d 00
ca 64 2d 8b 63 e3 15 35 ef 7b df 03 21 4d 7b de f8 3e 26 4a d8 f8 8c
83 21 90 a6 be 0e 5b 08 64 2d a9 5b 04 43 21 6c 7c 4e 74 29 af 7c 16
d6 99 0b 6b 48 64 2d 8f 83 5f 07 a5 6c 7c 1a e4 2d a2 21 92 b5 b1 6d
7c 56 d7 c1 8c 63 54 c7 c1 4c 63 18 e5 b1 ea 63 9c e7 3e 0d 7c 14 c7
ad 8f 83 5f 18 29 8f 8b 5f 15 b5 f0 53 18 e7 3d 8f 8b e0 c7 2d 8f 8b
e0 c6 31 ce 7b 1e a6 39 f0 6b e0 f6 39 ce 73 9c c7 c5 f0 53 18 c6 31
8c 7b 1f 06 3e 2b 5b 5f 06 39 ce 73 d6 c7 c1 8e 5b 1f 18 a9 8c 63 18
c6 be 0a 63 9c f8 3e 2b 6b e0 c6 3d 8f 8b e0 c7 c1 6c 7c 56 d7 c1 4c
73 d8 f5 31 cf 63 e0 a6 39 4c 52 9a a6 39 ce 7b 1f 07 c6 0c 73 e0 a6
3d ad 63 98 f8 be 0a 63 d6 c7 c5 4c 7c 1f 05 31 f0 7c 5a f7 c6 0f 8c
18 f8 c6 2c 7c 1f 15 31 f1 82 98 f6 b5 6c 7c 18 e5 b1 f0 63 e3 18 c6
2c 7a d4 c7 c1 ed 63 e0 e7 3e 31 7c 14 a5 31 8c 73 94 c5 31 ce 7a d8
f8 b9 aa 6b e2 d7 c1 4c 62 98 c7 39 ca 62 98 f6 3d 6c 7c 5f 05 29 4a
6a 9a f8 b5 ca 6a 98 c6 be 0a 63 98 c7 39 cf 63 e2 f5 b5 f0 52 98 f5
b1 f0 62 98 c7 c5 6d 7b e3 18 be 31 7c 18 e5 b1 f1 53 5c a6 a9 af 6b
e0 a6 3d 4c 7c 5a f8 29 8f 63 e2 f8 31 ec 7a 98 f8 29 8f 83 e3 06 3d
8f 8c 1f 18 bd f1 8c 5f 17 be 0c 72 98 f8 a9 8e 7c 18 f8 c1 8e 73 e2
f8 29 8f 63 e0 d7 c1 4c 7a d8 f8 a9 8f 83 e0 a6 3e 0f 8b 5e f8 c1 f1
83 1f 18 c5 8f 8c 5e a6 b9 af 7b 5c a6 b9 af 8a da f7 c1 8f 8a d6 b5
ad 6b 6b dc d5 a9 af 8b e2 d7 c5 af 8b 9a f8 3e 0f 63 e0 d7 bd ef 7b
e0 f8 2d ac 73 1e b6 b5 ac 5b 1f 18 31 f0 72 98 f8 31 f1 8c 63 15 31
f0 7c 1a e5 b5 ef 8c 18 f5 b1 f1 5a d6 b5 35 f1 82 98 f8 b5 ac 7c 60
c7 39 f0 53 1f 16 3e 2a 63 e2 d7 b5 ef 7b d6 b6 b1 6d 6a d6 d6 ad ab
6b de a6 b9 ae 6b 94 d7 35 f1 5b 1f 06 3e 0f 8c 58 b6 3d 4c 7c 63 05
31 eb 6a d8 b6 3e 0c 73 1f 16 bd f1 53 5f 18 c6 0b 6b 5e f7 be 2b 5a
d6 d7 c5 ef 5b 5a f7 ad 6d 5a da f5 ad 6b 6b df 16 bd eb 6b 5f 15 ad
ad 6b 5a d7 be 31 5b 5e b5 ad 6b 5b 56 d6 bd f1 8a da f6 ad 6d 7c 5a
f5 b5 af 5a da f6 b5 eb 5b 5f 18 b5 ed 7b df 15 b5 af 8b de d6 b5 af
8a d6 d6 bd f1 8b 56 b5 b5 ed 7b de f7 be 31 8a da d7 b5 ef 7b e2 b5
b5 af 8c 62 f7 c5 6b 6a d6 d5 b5 f1 5a d6 d7 b5 ad 5a da d7 be 2b 6b
16 d7 ad ad 72 da d6 b5 af 7c 56 b6 b5 ed 7c 56 b6 b5 ab 5b 5e f8 ad
af 7b de f7 c5 f1 7c 5a d6 bd f1 8a da f8 b5 f1 5a d6 d6 b5 eb 6a da
b5 b5 ef 8a d6 d6 be 2b 6b 5a f7 c6 2f 5b 5a f8 c6 31 8b e2 b5 b5 af
```

```
6b d6 b5 ad ad 7c 62 d7 ad ad 7c 5a f5 ad ad 7c 5f 16 b5 ef 6b 5e b6
ad 6d 5a da f8 c6 2b 5b 5e f7 c5 af 7b e3 16 3e 0f 8a 9a f8 3e 31 8c
60 f8 29 8f 8c 56 c7 c1 af 82 d8 f8 c1 8f 8a d8 f8 a9 ae 5b 5e d6 b9
ae 6b e0 c7 ad 8f 82 94 d7 be 2f 7b e3 07 3e 0a 63 d6 c7 c5 4d 72 9a
f8 3d 8e 63 e2 a6 3e 0f 82 98 d7 c6 0b 63 e0 d7 c5 ef 83 e0 f6 3e 0d
7c 5e f7 c6 31 8b de f8 3d 8f 53 1f 06 3e 0a 63 e2 b6 3e 2a 6b e0 e7
c1 4d 53 5f 05 b5 f1 8c 58 f8 c6 0d 7b df 16 3e 0d 7b e3 07 c1 ec 7c
18 e5 b5 6c 7c 18 f8 3e 0a 63 d6 c7 c1 8e 5b 1f 06 be 30 7a d8 f8 35
f1 82 d8 f5 b1 f0 6b e2 c7 c6 0d 7c 60 f8 29 8e 7a d8 f8 39 8c 73 e0
d7 c1 4b 6b e0 f5 b1 f0 63 5f 18 29 4c 63 5f 07 b1 ea 63 9c f8 31 cf
63 9c f8 29 4c 6b e0 b6 be 0c 63 18 c6 31 eb 63 9f 05 29 8d 7c 58 e7
c5 4c 63 1a f8 b1 f0 73 e2 a6 31 af 82 da f8 3e 0c 7a d8 f8 a9 af 82
da f8 c5 8f 83 18 f5 b1 f1 53 5e f7 c6 31 83 e0 b6 3d 6c 7c 62 a6 b9
6d 7b 5a f7 c6 31 6b 58 f8 31 f1 8c 63 07 c6 31 8c 56 c5 b1 6c 7c 54
c7 c1 4c 7a d8 f8 a9 af 8c 62 c7 a5 4c 63 9f 07 3e 0b 32 14 a6 31 af
82 16 53 a1 48 5b 5f 03 25 6c 7c 04 43 21 4c 72 98 c7 b1 c5 3a 56 c7
c1 8d 7c 48 63 a1 4b 6b e2 64 21 2b 6b e0 74 14 e9 53 1c e7 39 cf 89
4e 95 31 af 88 ca 74 2d af 81 0c 95 31 e2 21 d0 a6 3d 6c 7a d8 f3 a5
6c 7c 4a 74 a9 8c 71 0c 85 b1 c9 5b 1c 22 88 84 3a 16 c7 9d 2b 63 d8
e7 c5 2a 63 5f 12 9d 0a 5b 5f 02 19 0a 00 88 61 10 c8 42 14 a3 20 44
32 10 b6 b9 2b 62 80 22 14 62 21 d0 b6 be 05 3a 56 a3 20 03 29 92 a6
be 23 29 d2 a6 a8 87 49 84 50 8c 00
```

and

```
12 14 00 64 32 16 c5 b5 f1 32 56 c7 04 64 3a 56 c2 9d 0b 63 86 53 25
6c 7c 46 53 a5 6d 7c 16 d6 ad 84 32 16 11 94 e8 52 da d7 c5 6c 7c 60
85 31 f1 19 4e 95 b5 f0 00 88 64 29 8f 80 88 11 10 c8 53 1f 01 10 c8
53 1f 18 94 e5 38 ca 74 29 af 78 ca 64 29 af 8a d8 f8 8c 86 4a 98 f8
c1 4c 78 88 64 29 8f 83 1e 85 b4 a5 00 ca 64 2d ab 63 e2 a6 bd f1 83
e3 18 19 0b 6b 5a c7 c1 8f 89 92 b6 3e 23 20 c8 64 29 4d 7c 08 64 2d
8f 82 56 d7 c1 4c 7a 56 c7 c0 44 32 14 d7 c4 e7 42 da c7 c5 a6 42 da
d2 19 0b 63 e0 d7 c1 e9 5b 1f 04 a9 af 11 0e 85 b1 2b 5b 5c d7 c5 af
82 98 c6 35 4c 7c 14 c6 31 8e 5b 1e a6 39 ce 73 e0 d7 c1 4c 7a d8 f8
35 f1 82 98 f8 b5 f1 5b 5f 05 31 8e 73 d8 f8 be 0c 72 d8 f8 be 0c 63
1c e7 b1 ea 63 9f 06 be 0e 73 18 c6 31 ed 63 9c e7 3d 8f 6b 5a c7 3d
8f 63 d8 f8 31 8c 6b e0 a6 31 ce 73 e2 c7 c1 8e 73 9c e7 3e 31 5b 5f
06 3d 6b 63 9f 18 a9 af 7b e0 e7 39 8e 7c 1f 05 31 ed 63 e2 a6 3e 0a
63 e3 07 3e 0a 52 da f5 b5 f0 53 1f 07 31 cc 73 e0 f8 b5 f0 63 9f 05
b1 cf 83 1f 18 b1 f0 7c 18 f6 b5 8f 8a 98 f6 3d 8e 73 e3 05 31 f1 8c
5a c7 39 ce 52 96 c7 c1 8e 73 1a b5 31 8c 63 9e a6 3e 0d 7b 5f 05 31
cf 8c 18 c6 31 8c 6b e0 a6 39 cf 83 e0 f8 ad af 83 1c f8 a9 8f 8b 5f
05 31 f0 7c 1f 06 39 ec 7c 56 d7 c1 8f 5b 1f 18 31 ce 7c 1c e7 c6 0b
63 e2 f7 c1 8f 63 9c e7 c5 6d 7c 14 c7 c6 31 82 94 a5 29 4c 62 94 a6
31 4c 73 9f 07 c1 6c 73 e3 18 c5 4c 63 1a f7 31 af 7b 9a f7 bd af 82
```

```
98 e7 c5 6d 7b de f7 bd f0 63 9e c7 c1 cf 8a 98 f8 c5 ed 7c 14 c7 39
8f 8c 63 07 2d 8f 83 1f 16 bd eb 6b e0 a6 39 8a 53 18 e7 29 8a 63 18
c7 ad 8f 83 e3 15 31 cf 82 98 f6 b1 f0 6b e0 a6 3d 6c 7c 54 c7 c6 2e
53 5c d7 be 0f 83 e3 06 3e 31 8b 1f 07 c5 4c 7c 60 a6 3d ad 5b 1f 06
39 6c 7c 18 f8 c6 31 82 da c7 c5 4c 7b 58 f8 c1 4c 53 1c f6 3e 0f 8b
df 06 39 f1 8c 63 07 c5 6b 6b 1c f8 c1 8e 53 1c b6 b1 ca 52 96 c7 ad
8b 63 d4 c7 b1 ce 7c 14 c7 39 f0 73 18 f8 3e 0e 73 98 c7 3e 30 53 14
d5 35 6a 63 d8 e7 3d 8e 73 e3 07 c1 f0 52 94 a5 2d af 7c 54 c6 be 2d
7c 14 a6 b9 af 53 18 c6 31 af 82 98 e7 31 8f 63 e0 c7 31 cf 83 e0 a5
b5 f0 63 e3 18 ad 8e 73 e2 e6 a9 8c 63 5f 17 29 aa 63 5f 05 29 6c 5b
5e a6 be 0c 73 1c c7 31 cc 63 1c b6 3d 6a 63 e2 d6 b9 4a 52 9a a6 31
af 8b 5c a6 a9 8c 6b e2 d7 c1 4c 63 18 c6 39 f0 52 96 d5 b5 f0 63 1f
07 c5 6b 5a d6 b5 ad ae 6a 9a f7 bd ef 7b 9a f8 b5 ed 7c 5c a5 29 4d
53 5f 05 35 cd 7b de a6 35 ca 63 18 d7 bd 4c 6b de d6 b9 4d 73 54 d7
29 6d 7c 1f 07 c1 4a 52 94 a5 31 8e 7c 62 d7 c1 8c 63 1c e6 31 ce 63
1e c7 39 ce 73 9f 07 c5 6d 7c 1a f8 c1 f1 7b e2 f8 29 8f 63 e2 a6 b9
4d 53 5f 16 be 0a 63 94 d5 31 f1 6b e0 a6 3d 8f 8b e0 c7 b1 ea 63 e0
a6 3e 0f 8c 18 f8 b5 ef 7b e3 18 bd f1 8c 14 c7 29 8f 53 18 c6 31 f0
6b da f8 29 8e 73 e0 c6 be 30 53 18 f8 39 ce 7c 62 f7 bd f0 63 9c e7
39 f1 8c 1c e7 ad 6b 5b 1f 17 c1 8f 83 e3 17 c1 8e 73 9c e7 3e 0f 8c
62 f7 bd f1 83 e0 a6 b9 4d 7a da f8 29 8e 7c 63 18 c6 30 73 e3 18 be
0c 7b 1f 17 c1 8e 73 18 e7 39 ea 63 e3 06 be 0a 63 e3 07 c1 f1 6b de
f7 bd eb 6b e0 a6 3d 6c 7c 5e f8 31 ec 7c 60 e7 c1 4c 7b 58 f8 35 f0
53 1e b6 3e 2a 63 e3 17 29 ae 6b df 07 c1 f1 83 1f 18 c5 8f 83 e2 a6
3e 30 53 1e d6 ad 8f 83 1c b6 3e 0c 7c 63 18 c1 6d 63 e2 a6 3d ac 7c
14 c7 39 4c 7c 54 d5 a9 af 6b d8 b6 b9 4d 73 5f 06 b9 6d 6b 5a d6 b5
cc 6b 9a f6 29 4a 52 da f8 c6 0a 53 18 a5 29 4a 53 54 c7 c1 f1 72 96
d6 bd ed 6b df 18 b5 ac 7b 5a d6 b1 ec 73 9f 18 ad 6b 53 1a e5 29 ae
6b e3 18 c5 ad 6b 5a b5 b5 cd 73 5e f8 39 ca 52 94 a5 29 6c 7c 18 f8
3d 8f 83 5e f7 bd ef 83 e0 b6 3e 2b 6b 96 d7 bd ea 6b 94 d7 35 cd 7c
16 d6 3e 31 5a d6 b5 a9 af 7c 63 18 ad 6d 63 94 c7 c1 8f 8c 5a f6 bd
ef 6b 5a e6 35 cc 53 5e f7 bd ef 83 e0 b6 3d 6c 73 9f 17 29 8c 63 54
c6 31 ae 5b 5e a6 31 ae 6b 9a f7 b9 ae 63 5f 16 b9 ab 5a d6 a6 be 0f
5a da c7 b1 f1 5b 1f 17 29 8a 63 54 d7 be 31 6b 1c f8 29 6d 63 e0 e7
c1 4a 6b e2 f7 bd f0 7c 1c f6 3e 2e 6b 9a f7 b9 af 72 94 a5 29 ae 5b
5a d6 b5 ee 63 18 d7 bd cd 7b 5a f7 a9 af 82 da f8 ad af 82 98 f8 c5
6c 7c 54 d7 c5 ef 7c 60 f6 3e 0d 7b e3 07 c1 ec 7c 18 f8 b5 ef 8b e0
a6 3d 6c 7c 18 f8 3e 31 62 96 c7 c6 30 63 da b6 2d 8f 83 1c c7 b1 f1
53 1f 05 31 cf 8c 60 e7 31 cf 83 e0 f8 bd ef 7b de f8 3d 6c 7c 54 d7
c6 0b 63 9f 07 c1 cf 83 5e f8 3e 31 5b 1c f8 c1 f0 73 9f 15 ad 6b 5a
98 d7 c1 cf 83 e2 d5 b5 8a 5b 16 c7 39 cf 5b 5a b5 ad 6d 63 9c f6 39
ce 7c 18 e7 39 ce 73 e2 c7 b1 f1 8c 62 f5 b5 ef 82 98 e7 3e 2d 7b de
f7 c1 8e 7b 1f 18 c1 8e 63 e3 05 b5 ad 5a d6 b6 b5 ad 73 5e b5 ad 6d
6a d6 d7 be 2b 63 e0 c7 c5 af 7b de f5 35 ca 6b d6 b5 ad ab 6b 5a d7
```

```
c6 2b 6b df 15 b5 cb 6a d6 d7 c5 af 5a da f6 b5 6b 5b 5f 16 b5 ad 7a
d6 d7 b5 f1 5b 5e b6 b5 eb 6b df 15 35 ef 7a 98 d7 b9 8d 7b 98 d7 b9
aa 63 18 c6 31 8d 72 9a f7 bd ef 5b 5f 18 b1 cf 8c 18 f6 39 cf 63 e3
18 c1 8c 7c 5e f7 c1 f1 8c 56 a6 35 ef 8c 62 d6 2d af 8a 9a f7 b5 ad
6b e2 b5 b5 ae 53 5c a6 bd ef 7b de d6 b5 ad 6b da d7 c5 6d 7b e2 a6
3e 0a 63 e0 c7 3e 31 8b e0 c7 c6 0a 6a 98 f8 b9 4d 73 5e a6 be 0f 63
98 c7 c5 ed 7b de f6 be 2d 6b 98 d7 31 af 8a d8 e7 c6 0a 63 e0 f6 39
cf 82 98 e7 39 ca 52 d8 e7 c5 4d 7c 1f 16 bd ae 63 5e a6 35 ee 6b e0
a6 be 2f 8c 63 18 b1 ce 7a d8 f8 31 ec 73 e0 f8 c6 0f 83 18 d7 c5 af
7a da e5 29 4c 6b de f7 b9 4a 6b 94 d7 bd ef 7c 63 15 ad 6b 5a d8 f8
be 0c 63 18 f8 b1 f1 8c 1f 15 31 f1 6b 16 d6 bd ef 8c 5f 15 b5 cb 6b
9a f7 bd ca 6b 9a f7 b5 6b 6b 16 d6 ad 6b 6b e2 c7 ad 8f 83 1f 05 31
eb 63 e3 15 35 ef 82 98 e7 c5 6d 72 da d6 b5 ad 7b d6 d7 29 af 7a da
f8 b5 f0 63 1e c7 39 ed 6b 58 f6 39 cf 6b 5a c7 c1 8c 73 e0 e7 3e 2b
6b e0 c6 3e 30 73 98 c7 3d ac 73 e3 15 ad 6d 73 54 d7 be 0d 72 9a f5
31 ae 53 5e b6 b9 4a 6b df 18 a9 8c 73 e0 f8 31 f0 53 1c f8 39 ce 73
e0 f8 c6 31 5a d6 b5 ad ac 52 96 c5 b1 6d 6b 14 b6 b5 ad 7b e2 b5 ad
4c 6a d4 c6 31 8c 62 94 c6 3e 0a 63 96 c7 c5 4c 7c 5a f6 ad ad 6a da
d6 bd 6d 7b da f8 c6 2f 7b e0 b6 bd ef 8c 58 f8 c5 6d 7b de f7 b9 ae
53 5e f7 b5 f1 8a da f7 a9 af 73 5f 16 bd ef 8c 14 c7 39 f0 53 1e b6
3d 4c 73 1f 06 bd ef 8b 1f 06 bd ad 6b 5a d6 be 30 5b 56 b5 b1 cf 8c
56 d6 39 ce 52 d8 f5 b1 ca 53 18 c6 31 f0 53 1c e7 c1 ca 63 1f 07 c1
cf 6b 1c e6 39 8f 8c 54 c5 29 4d 7b d4 c6 35 4c 63 18 d7 c5 ae 52 94
b6 b1 6c 5b 5a f7 29 4d 7c 1e c7 c5 6c 73 9c e7 3e 0a 53 1c e5 31 8e
7c 56 c7 3e 0a 52 94 c7 3e 31 8b 1f 17 ad 4c 6b 96 d7 b1 6d 7b de d6
bd f1 5b 1f 15 35 ca 6b e0 e7 c1 aa 63 e0 f8 29 8d 7c 60 b6 3e 0c 7c
5e f7 c6 2d 7b 5e f6 bd ef 7b 5a d6 bd cc 6b 9a f8 ad ab 6b e3 17 bd
f0 53 1f 15 b5 f0 63 e0 a5 b1 f0 63 9c f8 b5 f0 63 e2 b6 3e 2a 6b e3
18 29 8f 8b df 18 ad af 82 98 f8 c6 31 8a d6 c7 c1 8e 5b 1f 17 c5 6d
72 9a f7 c5 4c 73 d8 f8 3e 0e 7c 63 18 ad 6b 5a d4 c7 c6 30 7b 1c f8
35 ca 63 5e f8 b5 8f 8b de f5 35 f0 6b e3 17 35 f1 8c 62 d7 b5 ef 7b
9a f5 ad ad 7b de f5 a9 8d 7c 1f 16 39 f0 63 e0 b6 be 2b 6b 94 a5 29
6d 7b da e5 31 aa 6b df 05 b5 ae 5b 5a f8 35 f1 7c 56 b5 ad ad 6b de
f6 b5 ef 6b d6 b5 b5 8b 62 da f7 35 f1 5b 1f 06 3d 8f 8b e0 c7 c6 0b
6b df 15 35 ef 72 9a b5 35 ca 5b 5e d6 b9 af 8c 63 07 c5 4c 6b df 18
c6 30 63 18 c7 c6 0c 73 9c e7 39 6d 63 da c7 39 ce 63 1f 15 b1 cf 8c
18 f8 29 8f 83 9c e7 c5 4d 72 da f7 a9 af 83 5f 18 c6 31 8c 62 c7 3e
31 8c 14 a5 29 4a 63 e0 e7 39 4c 7c 18 e7 a9 8c 7c 14 d7 c6 0b 63 d6
c7 c1 af 7c 1e c7 3e 0d 7c 14 c7 ad 8e 63 e0 a6 be 0b 63 d6 c7 c1 ae
6b e2 c7 c1 8d 7c 14 a6 31 af 8b 1e a6 39 cf 83 1c b6 39 8f 5b 1c e7
c1 4c 6b e0 b6 be 0c 63 18 c6 31 eb 63 9f 05 29 8d 7c 58 f5 b1 ce 7b
1c e6 35 4c 63 9c e7 3e 0a 63 d8 e7 3e 30 52 94 a6 31 ec 7c 1a e5 b5
f1 5b 1f 07 3e 0d 73 1a f8 2d ad 7c 56 c7 c1 8f 8b 1f 06 be 2c 7c 18
f8 b5 6b 62 da b6 bd ef 7b de f5 35 ef 7b da f8 c6 31 8c 14 a5 2d ae
```

```
6b e0 c7 ad 8f 8a 98 f8 3e 31 8b 5f 05 31 eb 63 e2 f8 31 8f 83 94 c5
31 f1 63 e0 c7 c6 31 82 96 d6 b1 f1 7c 18 c6 39 ec 7c 63 18 c1 8f 83
1f 17 be 0a 6b dc b6 be 2d 7c 5f 06 3d 8f 8c 54 d7 c5 f1 8c 16 c7 c5
f0 63 e0 f8 ad af 53 5c a6 35 ef 6b 94 d7 bd eb 62 da d6 b5 ad 5a d6
b5 ad 6d 7a da f6 be 2b 63 e2 a6 3d 8f 83 1c f8 c5 f1 6b e0 a6 3e 31
8c 56 c7 c5 4c 7c 62 d7 c1 4c 73 98 a6 3d 6c 7c 5f 15 31 f1 8c 1c c6
31 ce 7b 1f 05 31 ce 5b 1f 15 35 ef 8c 62 f6 be 0a 63 98 a5 29 aa 63
e0 a6 3e 0c 63 9c e7 3e 2d 7c 18 e5 29 4a 52 d8 e7 39 f0 63 9c e7 3e
2c 7c 18 e7 b1 cf 83 e2 d7 c1 8e 7b 1f 18 c6 31 83 9f 18 bd f1 8c 18
c6 31 f0 63 d6 c7 39 ce 73 e0 c7 2d 8e 7b 1e c7 c5 ae 6b df 07 c1 8f
8c 56 c7 a5 4c 63 9f 07 3e 0b 32 14 a6 31 af 82 16 53 a1 4a 42 da f8
25 6c 71 d2 a6 3e 02 21 90 a6 39 0a 63 1c f8 34 a7 4a 9a f8 be 04 32
16 d7 c1 09 5b 5f 02 18 e9 5b 5f 02 10 a7 4a da f8 31 ce 73 9e 53 a5
6c 73 e0 d7 c4 65 3a 16 d7 c0 44 31 0c 95 31 cf 63 d2 b6 3e 25 3a 54
c6 39 f0 51 90 a6 35 f0 52 da f8 08 86 4a d8 f1 10 e9 53 1c e7 c4 e9
53 5e 53 a1 4b 6b e2 a6 be 28 52 da f8 2d af 80 04 43 21 42 21 90 22
19 02 21 90 a5 b5 c6 42 4c 82 19 2b 62 80 22 14 62 21 d0 b6 be 0c 61
4e 95 a8 c8 00 ca 64 a9 af 88 ca 74 a9 aa 21 d2 61 14 23 00
```

which when E-Multiplied and combined yield the following public key matrix:

```
59 84 da 78 fb 26 3d 53 cc 8f
62 5c 34 80 3b 81 e6 74 a4 73
5c 62 5e be 5c 4f 34 e4 d0 82
46 b2 f0 c7 af d2 48 91 55 9e
c2 d5 d6 94 97 b0 17 8a ff ef
e9 c9 e5 53 81 04 a1 3c 71 4d
20 e7 15 98 57 4b 26 23 71 3d
e7 92 57 48 09 de e9 4d f0 eb
9a 2e dd f7 af 5a ed 56 d5 67
95 e4 50 2c 81 b5 8e 7a 25 81
```

A.2.2 Interrogator Keys

The Interrogator has a private matrix:

```
26 6b a7 b1 e6 04 d6 99 83 01
d8 c5 28 46 5c 1d a5 5e 3a ac
c1 27 d1 82 42 26 b5 c2 a1 b2
c8 b7 3d 08 a8 0f 0c 8e 57 bd
19 0e 43 be 58 15 4d cd d2 d5
4e 98 7f 04 76 03 e6 62 ad b8
8c e5 40 d9 b5 52 cd 95 d6 5c
19 bc 13 e6 b2 ac b6 a6 7f 25
8e 59 c4 3d 7e 14 2c 9e fd 75
33 d8 35 1b 8d 14 64 83 f6 0e
```

A public matrix:

```
e1 44 17 37 f3 99 a2 0f e5 14
a3 7f 6d 74 8f 67 e8 62 27 43
b6 ae 1b 73 3c 91 44 bd 12 e5
58 b8 c8 1f 94 66 cb 17 ea 82
a4 90 bc 67 68 0e a0 9f 40 a1
1e ee f7 2d c6 c4 17 74 83 72
b8 95 ce 76 35 f5 c1 2d 17 5b
65 2b f0 8a 17 28 05 eb 41 1d
a3 cf 4e c8 0d c0 1b 7f 00 c0
f1 bb 0d b7 66 d8 8a cb ee b7
```

And a public permutation:

```
1 2 3 4 9 5 10 8 7 6
```

A.2.3 Tag Shared Secret Computation

To compute the shared secret, the Tag computes two E-Multiplications using the Interrogator’s public key, one using the first set of matrix and braid:

```
ba 74 1b b5 eb c6 53 52 a9 88
99 9e 62 02 39 17 df f8 fb 70
73 57 f2 8d 6f f1 ba 39 94 fc
d0 ea b6 10 c0 aa dd 06 0c a9
37 3f da 28 6d 70 f4 e8 a7 45
cc 97 fa 01 1b 94 01 b0 d8 b8
e3 a4 92 ca f4 74 6b 69 24 bc
09 4d e5 db 32 5b fd e9 ec 1e
8f b8 ea 54 f7 0c be 2c af 11
a1 6e 34 d4 9d 7c 1a 28 b5 57
```

and another using the second set:

```
68 1c 90 f6 13 f0 da 75 7b 7b
27 9f fc 1f c1 95 91 03 87 a5
12 6d 7c d9 31 04 ba 8d 77 c6
cc 1a 67 b3 d6 e3 86 51 bb 54
22 9c de a1 97 5d 7c 47 21 99
25 70 36 16 e9 69 9c 91 f8 49
14 e7 bb ed 2a 77 9a 76 b8 f2
8d 32 a5 26 c6 fb 18 c9 2b 34
37 dd f6 c9 01 94 3b ac b4 a5
83 cb df 6c 63 80 91 91 df e3
```

Then it sends the S column vector to the Interrogator:

```
eb 39 6f c0 6d 1b f4 32 f7 9d
```

Which results in the corresponding shared secret:

```
13 c1 31 d6 97 e9 2a c6 1 63
```

A.2.4 Interrogator Shared Secret Computation

The Interrogator uses the public key of the Tag plus its own private matrix to compute the following matrix:

```
fe 13 7c 81 17 68 8f 4c 45 bf
e3 8b 64 bc 0d 87 88 54 a8 08
d6 63 51 b1 49 c6 fb 68 a6 23
a2 24 93 5b e7 67 f0 4b 99 b3
9b e6 b8 cd 06 7b 60 6e f6 aa
ae d4 fc 25 e4 8f 7a a7 4a b3
e5 42 ec 7e 34 e7 92 a9 04 98
0d ce d2 85 36 5d 10 bc 10 0b
f9 de e7 61 72 59 ba c0 db d3
05 3e 18 30 58 d4 68 1d 0d 33
```

Then it uses the S column vector supplied by the Tag and can compute the same shared secret:

```
13 c1 31 d6 97 e9 2a c6 1 63
```

A.3 AEHash Test Vectors

The following sections detail a simplified instance of AEHash function parameters and then show an input message and the resulting hash output.

A.3.1 Simplified AEHash Parameters

We define an instance of the AEHash with the following parameters:

First we set N=4 and q=8 (B4F8), which provides a 48-bit hash. (Note that in production we recommend a 256-bit hash using B8F16; the instance detailed here is a complete toy, shown here only for demonstration purposes, and is insecure for any operation).

Working within B4F8 we then need to define the initial matrix, permutation, and T-values.

Matrix:

```
1 0 0 0
0 1 0 0
0 0 1 0
0 0 0 1
```

Permutation: 1 2 3 4
T-values: 2 3 5 6

Finally, we need to define λ and the associated hash braids. For this example we set λ=2, which means we have four (4) hash braids:

1. $b_3 b_3 b_2 b_1$
2. $b_3 b_2 b_2 b_1$
3. $b_3 b_2 b_1 b_1$
4. $b_3 b_1 b_3 b_3$

A.3.2 Simplified AEHash Input and Output

When you apply the hash in the previous section to the input string ``This is a test“ (Hex: `54 68 69 73 20 69 73 20 61 20 74 65 73 74`) it results in the 48-bit hash: `90 c7 1c 24 20 01`.

A.3.3 Full AEHash Test Vectors

The AEKAP protocol in this document uses the AEHash Parameter B8F16L5 as defined in XXX. This defines a 256-bit hash with 32 hashbraids. When you apply the AEHash with these parameters to the input string ``This is a test'' (Hex: `54 68 69 73 20 69 73 20 61 20 74 65 73 74)` it results in the 256-bit hash: `2f 5b 19 73 9d c1 74 b6 50 ab 8d 0d aa 1f 36 28 2d 20 69 44 b6 c7 88 04 45 57 c9 e2 c7 64 4b 78`.

Annex B
(informative)

Cipher description

B.1 Asymmetric cryptography with the Algebraic Eraser

The AE Key Exchange Protocol (AEKAP) enables two users, Alice and Bob, to evaluate a shared secret using their own private key and the public key of the other user. The following definitions are used in the description algorithm which provides the security for this protocol where Alice is a Tag and Bob is an Interrogator.

B.1.1 AEKAP Public (Keyset) Parameters

The AEKAP contains the following public information:

- A fixed matrix $M_* \in GL\left(N, F_q\right)$, which is chosen to ensure security (see [7]),
- A set of conjugates in B_N for each group, Tags:

$$C = \{c_1 = za_1z^{-1}, c_2 = za_2z^{-1}, \dots, c_k = za_kz^{-1}\},$$

and Interrogators:

$$D = \{d_1 = zb_1z^{-1}, d_2 = zb_2z^{-1}, \dots, d_\ell = zb_\ell z^{-1}\},$$

where it is assumed that each of the conjugates is *rewritten*, i.e., a Braid group algorithm [5,6] is applied to the conjugates making the element z intractable to derive. The Braid element $z,$ together with the Braid group elements $a_1, \dots, a_k, b_1, \dots, b_\ell$ are chosen to insure security. One important feature of these sets of braid elements is that $a_ib_j = b_ja_i$, for all $i = 1, \dots, k, j = 1, \dots, \ell$.

- A set of T-values, which is an array of N entries in F_q that get used as part of the E-multiplication.

This public information (matrix, user conjugate set, and T-values) make up the keyspace for AEKAP. For two users to communicate they must share a common keyspace. This is similar to Diffie-Hellman where you choose a common prime, or in ECC where you choose a common curve. In AEKAP you choose a common matrix and conjugate set. The main difference in that there are two sets of conjugates in the set and each user must choose theirs from the opposite set (e.g., Tags choose from set A, and Interrogators from set B).

Note that M_* must be of a special form to prevent certain classes of weak-key attacks, similar conceptually to the attacks possible if an RSA key is chosen randomly or chosen using two large random primes instead of computed as the product of two large primes chosen to prevent known attacks. The special method of choosing the matrix assures that this class of attack is not possible. Similarly, braid element z must be chosen to be large enough to prevent a different class of attacks, similar conceptually to choosing a Diffie-Hellman prime that's too small.

Note that the matrix M_* T-values, and the conjugate sets C and D are created once and shared amongst all Tags and Interrogators. All Interrogators know the Interrogator conjugates (D), all Tags know the Tag conjugates (C), and everyone knows the matrix and T-values. Also note that the Matrix and conjugates are only required to generate a keypair. Once a keypair is generated only the T-values remain necessary to compute the shared secret. So in the case of a Tag with a fixed (static) keypair, it only needs to know the T-values and its public/private keys and not the public matrix or Tag conjugates.

It is expected that Interrogators will have the full keyset parameter data available (matrix and Interrogator conjugates) in order to generate ephemeral keys. For Tags it's expected that static keys will get generated during manufacture, so the manufacturer must has access to the keyset parameter data (matrix and conjugates), but the Tags will not.

B.1.2 AEKAP Public/Private Keypairs (Tag and Interrogator Keys)

User Private Data have two components

– The Private key is a polynomial of degree N-1 in the matrix M_* with coefficients in the field F_q: in the case of Alice,

$$M_A = \sum_{i=0}^{N-1} \alpha_i M_*^i.$$

In other words, the Private Key (M_A) is an NxN Matrix where each of the N^2 entries is a member of the field F_q -- computed based on the public keyspace matrix M_*.

– The Conjugacy Set consists of a product of a sequence of the user's conjugates, again in the case of Alice,

$$c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot \; c_{i_{L_A}}$$

which is itself an element in the Braid group.

In other words the user randomly chooses L_A conjugates (and their inverses) from the user's conjugate set in the keyspace and combines them together. This combination can happen in real time, or, because the result is just another entry in the Braid group (e.g. another conjugate) it can be reduced for storage, generally ending up about twice the size of the published conjugates.

To compute the inverse of a braid you reverse the order of all the Artin generators and then you take the inverse of each. For example, if you had the braid b_1 b_2 b_3^{-1} b_2^{-1}, to compute the inverse you reverse and inverse the generators resulting in b_2 b_3 b_2^{-1} b_1^{-1}.

– Alice's public key is obtained via E-Multiplication:

$$(M_A, 1) \star \left(c_{i_1} \cdot c_{i_2} \cdots \; c_{i_{L_A}}, \quad \sigma_{c_{i_1}} \cdot \sigma_{c_{i_2}} \cdots \; \sigma_{c_{i_{L_A}}} \right),$$

where 1 is the identity permutation in S_N.

In other words, the result of the E-Multiplication is a pair: an NxN matrix where each entry is a member of the field F_q, and a permutation of N entries (S_N). This is the composition of the Public Key.

B.1.3 Computing the Shared Secret

Both Alice and Bob can simultaneously compute the shared secret/exchanged key by using their own private data and the public key of the other:

– Alice receives Bob's public key,

$$(M_B, 1) \star \left(d_{j_1} \cdot d_{j_2} \cdot \cdots \cdot \; d_{j_{L_B}}, \sigma_{d_{j_1}} \cdot \sigma_{d_{j_2}} \cdot \cdots \cdot \sigma_{d_{j_{L_B}}} \right)$$

and computes

$$(M_A, 1) \cdot (M_B, 1) \star \left(d_{j_1} \cdot d_{j_2} \cdot \cdots \cdot\ d_{j_{L_B}},\ \sigma_{d_{j_1}} \cdot \sigma_{d_{j_2}} \cdot \cdots \cdot \sigma_{d_{j_{L_B}}}\right) \star \left(c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot\ c_{i_{L_A}},\ \sigma_{c_{i_1}} \cdot \sigma_{c_{i_2}} \cdot \cdots \cdot \sigma_{c_{i_{L_A}}}\right).$$

Likewise, Bob receives Alice's public key and computes

$$(M_B, 1) \cdot (M_A, 1) \star \left(c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot\ c_{i_{L_A}}, \sigma_{d_{i_1}} \cdot \sigma_{d_{i_2}} \cdot \cdots \cdot \sigma_{d_{i_{L_B}}}\right) \star \left(d_{j_1} \cdot d_{j_2} \cdot \cdots \cdot\ d_{j_{L_B}},\ \sigma_{d_{j_1}} \cdot \sigma_{d_{j_2}} \cdot \cdots \cdot \sigma_{d_{j_{L_B}}}\right).$$

Both of these computations result in the shared secret/exchanged key:

$$(M_A, 1) \cdot (M_B, 1) \star \left(d_{j_1} \cdot d_{j_2} \cdot \cdots \cdot\ d_{j_{L_B}},\ \sigma_{d_{j_1}} \cdot \sigma_{d_{j_2}} \cdot \cdots \cdot \sigma_{d_{j_{L_B}}}\right) \star \left(c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot\ c_{i_{L_A}}, \sigma_{c_{i_1}} \cdot \sigma_{c_{i_2}} \cdot \cdots \cdot \sigma_{c_{i_{L_A}}}\right) = (M_B, 1) \cdot (M_A, 1) \star \left(c_{i_1} \cdot c_{i_2} \cdot \cdots \cdot\ c_{i_{L_A}},\ \sigma_{d_{i_1}} \cdot \sigma_{d_{i_2}} \cdot \cdots \cdot \sigma_{d_{i_{L_B}}}\right) \star \left(d_{j_1} \cdot d_{j_2} \cdot \cdots \cdot\ d_{j_{L_B}},\ \sigma_{d_{j_1}} \cdot \sigma_{d_{j_2}} \cdot \cdots \cdot \sigma_{d_{j_{L_B}}}\right).$$

As before, the result of this computation is an NxN Matrix and a Permutation.

B.2 Ironwood Key Agreement Protocol

This section details the Ironwood Key Agreement Protocol, a variant of AEDH used for Profile [ii] of this specification.

B.2.1 Ironwood Public Key Parameters

The Ironwood KAP contains the following public information:

- The Braid group B_N where $N \geq 10$ is an even integer.
- A finite field F_q of q elements.
- A non-singular matrix $m_0 \in GL(N, F_q)$ which is chosen to ensure security.
- A set of conjugates in B_N for each group, Tags:

$$\{\, za_1z^{-1},\ za_2z^{-1}, \dots ,\ za_kz^{-1}\},$$

and Interrogators:

$$\{\, zb_1z^{-1},\ \ zb_2z^{-1}, \dots ,\ zb_\ell z^{-1}\},$$

where it is assumed that each of the conjugates is *rewritten*, i.e., a Braid group algorithm [5,6] is applied to the conjugates making the element z intractable to derive. The Braid element z, together with the Braid group elements $a_1, \dots, a_k, b_1, \dots, b_\ell$ are chosen to insure security. One important feature of these sets of braid elements is that $a_ib_j = b_ja_i$, for all $i = 1, \dots, k,\ j = 1, \dots, \ell$.

B.2.2 Ironwood Interrogator Private/Public Keypairs

- A fixed random private braid word β_{A} (i.e., an expression in the Interrogator conjugates), which is chosen by a TTP for each Interrogator. This value is never supplied to the Interrogator but is instead used to generate the following:
- A random private matrix $C_A = \sum_{i=0}^{N-1} \alpha_i m_0^i$
- The TTP computed public key

$$\mathrm{Pub}_{\mathrm{A}} = \ (C_A, id) \star \beta_A \ = (C_A \cdot M_A\,, \sigma_A)$$

B.2.3 Ironwood Tag Private/Public Keypairs

- Two fixed random private braid words, $\beta_{\mathrm{B}}\,, \beta_B',$ in the Tag conjugates (i.e., expressions in the Interrogator conjugates), which were chosen by a TTP for each Tag.
- Two random private matrices: $C_B = \sum_{i=0}^{N-1} f_i\, m_0^i\,, C_B' = \sum_{i=0}^{N-1} f_i'\, m_0^i$ which were chosen by a TTP for each Tag.
- The Tag is provisioned with T – values, $\{\tau_1, \tau_2, \dots, \tau_N\} \subseteq F_q,\ \ \tau_2\ \neq 0{,}1,$ and is enabled to execute E-multiplication using the T – values.
- The first part of the public key of the Tag, which will be signed by a certificate authority, is obtained by evaluating the E-multiplications

$$(id, id) \star \beta_{\mathrm{B}} = \ (M_B,\ \sigma_B), \qquad (id, id) \star \beta_B' \ = (M_B',\ \sigma_B')$$

and then forming the product $C_B \cdot M_B \cdot (C_B' \cdot M_B')^{-1}$ and computing its inverse: $(C_B \cdot M_B \cdot (C_B' \cdot M_B')^{-1})^{-1}$

B.2.4 Computing the Shared Secret

The Ironwood KAP proceeds with the Interrogator sending its public key to the Tag, the Tag using the received public key to generate the second component of its public key, and the Tag sending its public key to the Interrogator. Both the Tag and the Interrogator can then evaluate the shared secret.

- The Interrogator sends its public key, $(C_A \cdot M_A\,, \sigma_A)$, to the Tag.
- The Tag receives $(C_A \cdot M_A\,, \sigma_A)$, and uses the T – values to evaluate two E-multiplications. Let Y_B, Y_B' be defined by the identities whose follow from the user conjugates commuting:

$$(C_B, id) \cdot (C_A \cdot M_A\,, \sigma_A) \star \beta_{\mathrm{B}} \ = \ (C_A, id) \cdot (C_B \cdot M_B, \sigma_B) \star \beta_A = (Y_B, \sigma_A \sigma_B),$$

$$\left(C_B', id\right) \cdot (C_A \cdot M_A\,, \sigma_A) \star \beta_B' \ \ = \ (C_A, id) \cdot \left(C_B' \cdot M_B'\,, \sigma_B'\right) \star \beta_A = \left(Y_B', \sigma_B \sigma_A\right).$$

The Tag defined the vectors

$$s = \frac{N}{2} \text{ column of the matrix } Y_B,$$

$$s' = \frac{N}{2} \text{ column of the matrix } Y_B'.$$

and sends the ordered pair $((C_B \cdot M_B \cdot (C_B' \cdot M_B')^{-1})^{-1},\ s)$. The vector s', which the Tag has evaluated is the shared secret. Note that the pair can be sent separately; the fixed part, $(C_B \cdot M_B \cdot (C_B' \cdot M_B')^{-1})^{-1}$, can be part of a signed certificate and the second part, s, can be sent as part of the protocol.

– The Interrogator obtains the shared secret as follows:

$$s' = C_A \cdot C_B' \cdot M_B' \cdot M_B^{-1} \cdot C_B^{-1} \cdot C_A^{-1} \cdot s.$$

B.3 Hashing with the Algebraic Eraser

The AEHash algorithm is another cryptographic primitive that can be built on E-multiplication. However for the AEHash algorithm we require a slight modification to the definition of E-multiplication. In the definition of $\star$ the T-values remain the same at every step of the iterative process. Now we wish to define a new operation, denoted $\star'$, in which the T-values themselves are permuted along the way. Assuming that $\beta = b_{i_1}^{\epsilon_1} b_2^{\epsilon_2} \cdots b_{i_k}^{\epsilon_k}$, we define

$$T_1 = t-\text{values} = \{\tau_1, \dots, \tau_N\},$$

and let

$$T_2 = {}^{\sigma_0 \cdot \sigma_{b_{i_1}}} T_1.$$

We modify the original definition of E-multiplication by defining a new operation $\star'$ in the following way. Modify the second step of the E-multiplication in by using the set T_2 for T-values to obtain,

$$\left(M \cdot {}^{\sigma_0}\left(CB\left(b_{i_1}^{\epsilon_1}\right)\right) \downarrow_{T_1} \cdot {}^{\sigma_0 \sigma_{b_{i_1}}}\left(CB\left(b_{i_2}^{\epsilon_2}\right)\right) \downarrow_{T_2}, \sigma_0 \cdot \sigma_{b_{i_1}} \cdot \sigma_{b_{i_2}}\right).$$

Iterating this process we obtain the $\star'$ operation . It is this variation of E-multiplication that we will use to define our hash function.

Let S denote a string of bits and let λ denote a fixed non-zero positive integer. By padding S we can assume that the length of S, denoted Card(S), is divisible by λ. Thus, letting D_S = Card(S), we see that S can be viewed as a union of blocks, each of which has length λ:

$$S = \bigcup_{i=1}^{D_S} Block(i)$$

Let v(i) denote the integer that the binary string Block(i) represents. By construction, we have 0 ≤ v(i) ≤ $2^{\lambda-1}$.

The AEHash function, H_{AE} is specified by the following data:

$$\{B_N, q, \lambda, t - values = \{\tau_1, \dots, \tau_N\}, \{c_0, c_1, \dots, c_{2^\lambda - 1}\} \subset B_N, (n_0, \sigma_0) \in N_q \times S_N\}$$

where

- B_N is the braid group on N strands;
- q is a power of a 2, the T-values are invertible elements in F_q , the collection of braid group elements;
- $\{c_0, c_1, \dots, c_{2^\lambda - 1}\}$ is fixed and assumed to generate a free subgroup of B_N on said set of fixed elements;
- $(n_0, \sigma_0) \in N_q \times S_N$ is an ordered pair.

The output of the AEHash is defined to be the sequence of bits that specify the matrix, which is evaluated through a sequence of E-multiplications. The length of the AEHash is given by

$$N^2 \cdot \text{ceil}(\log_2(q)),$$

where for x > 0, the function ceil(x) (denotes the ceiling of x) which is the smallest integer n such that x ≤ n.

The lengths of the elements c_i, will impact the efficiency of the hash function. In our initial testing we chose the length to be in the range of $2N$ which proved to be sufficient security.Each element c_i is associated with a sequence of colored Burau matrices and permutations whose product we denote (though we do not explicitly evaluate) by $(CB(c_i), \sigma_{c_i})$. The string S, having been broken in to blocks of length λ, is associated with a sequence of braid words:

$$c_{S,v(1)}, c_{S,v(2)}, \dots, c_{S,v(D_S)}.$$

Thus S is associated with a sequence colored Burau/permutation pairs:

$$\left(CB\left(c_{S,v(1)}\right), \sigma_{c_{S,v(1)}}\right), \left(CB\left(c_{S,v(2)}\right), \sigma_{c_{S,v(2)}}\right), \dots, \left(CB\left(c_{S,v(D_S)}\right), \sigma_{c_{S,v(D_S)}}\right).$$

The hash of the string S, denoted $H_{AE}(S)$, is the matrix part of the output of the iterative modified E-multiplication

B.4 E-Multiplication

The core of each of these protocols is the concept of E-multiplication and the associated AE key agreement protocol, which is reviewed in this Annex for completeness.

E-multiplication definitions:

- B_N, the Braid group, $\{b_1, b_2, \dots, b_{N-1}\}$ the Artin generators,
- $CB\left(b_i^{\pm 1}\right) = N$-variable colored Burau matrix associated with $b_i^{\pm 1}$,
- $F_q =$ finite field of q elements (where q $= p^k, for\ p\ (prime)\ and\ k \geq 1, e.g\ 2^r$),
- $S_N =$ permutation group on N symbols; $\sigma \in S_N$, can act on $CB\left(b_i^{\pm 1}\right)$, the result is denoted ${}^{\sigma}\left(CB\left(b_i^{\pm 1}\right)\right)$,
- $T -$ values, $\{\tau_1, \tau_2, \dots, \tau_N\} \subseteq F_q$, a collection of invertible elements, the notation $\downarrow_{T-values}$ indicates replacing variables with the $T -$ values.

E-multiplication: an operation that inputs two ordered pairs,

$$(M, \sigma_0), \quad (\beta, \sigma_\beta),$$

where $M \in GL(N, F_q)$, $\sigma_0 \in S_N, \beta \in B_N$, and σ_β is the permutation associated to β, and produces a new ordered pair (M', σ'), where $M' \in GL(N, F_q)$, $\sigma' \in S_N$. The definition of E-multiplication when the braid $\beta = b_i^{\pm 1}$ is given by

$$(M, \sigma_0) \star \left(b_i^{\pm 1}, \sigma_{b_i^{\pm 1}}\right) = \left(M \cdot {}^{\sigma_0}\left(CB\left(b_i^{\pm 1}\right)\right) \downarrow_{T-values},\ \ \sigma_0 \cdot \sigma_{b_i^{\pm 1}}\right).$$

In the general case, when $\beta = b_{i_1}^{\epsilon_1} b_{i_2}^{\epsilon_2} \cdots b_{i_k}^{\epsilon_k}$, (where $\epsilon_i = \pm 1$) the E-multiplication is executed iteratively:

$$(M, \sigma_0) \star (\beta, \sigma_\beta) = \left(\left((M, \sigma_0) \star \left(b_{i_1}^{\epsilon_1}, \sigma_{b_{i_1}}\right)\right) \star \left(b_{i_2}^{\epsilon_2}, \sigma_{b_{i_2}}\right)\right) \star \cdots \star \left(b_{i_k}^{\epsilon_k}, \sigma_{b_{i_k}}\right).$$

As a concrete example, assume we are working in B4F7 with T-values 2 4 6 3. We start have a current matrix and permutation:

$$\begin{pmatrix} 1 & 4 & 3 & 5 \\ 2 & 5 & 2 & 6 \\ 3 & 6 & 2 & 1 \\ 2 & 4 & 2 & 5 \end{pmatrix}, (2,4,3,1)$$

Next we want to apply b_2 so we need to use the current permutation and T-values to plug into the appropriate CB matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ t2 & -t2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 4 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

When we matrix-multiply within the finite field (F7) and apply the braid twist we wind up with the following matrix and permutation:

$$\begin{pmatrix} 6 & 2 & 0 & 5 \\ 3 & 6 & 0 & 6 \\ 0 & 3 & 1 & 1 \\ 0 & 2 & 6 & 5 \end{pmatrix}, (2,3,4,1)$$

B.5 AE Implementation Considerations

- There are several parameters in the system that determine the security level: N, q, the number of user conjugates, and the length of the conjugacy set. The lengths of the user conjugates are dependent on the requisite security level. The method used to produce the sets of conjugates has the security level built in as a parameter.
- The size of the search space for Alice's private key is 2^{Nr} where r = $log_2(q)$. The storage space for the Private key is $N^2r + N log_2(N)$ bits.
- The size of the search space for Alice's conjugacy set is $(2k)^{L_A}$, which means that if Alice has a larger set of conjugates she can use a shorter conjugacy set. Conversely, if having a smaller set of conjugates is mandated, the private conjugacy set, can be increased in length to maintain security. The storage size for the conjugacy set is approximately twice the size of the individual published conjugates.
- Due to the iterative definition of the E-multiplication, increasing the length of Alice's conjugacy set increases the processing time to compute either Alice's public key, or the shared secret *linearly.* This is a unique feature of the AEKAP.
- There is the option for users to choose new private/public keys at any time. If Alice changes key pairs, while the second user's key pair remains fixed, the resulting shared secret will be different every time. This is another key feature of the AEKAP. Alternately Alice and Bob could use an encrypted nonce to provide replay protection.

Annex C
(normative)

AEDH Keyset Parameters

C.1 B10F256 Keyset Parameters

C.1.1 Overview

This keyset provides a security level of 2^{80} using a braid with 10 strands and a field of 256 (2^8). The field F256 is defined using the polynomial $x^8 + x^4 + x^3 + x + 1$. The keyset OID is 1.3.6.1.4.1.44196.1.2.1 which can be used e.g. in a certificate to notify an Interrogator of the keyset in use. When using this keyset the AEDHP parameter is 96 bytes (91 bytes for the matrix and 5 bytes for the permutation).

C.1.2 T-values

This keyset uses the following set of 10 ordered T-values (in decimal):

```
238,126,59,218,9,12,132,122,46,86
```

C.1.3 Seed Matrix

This keyset uses the following 10x10 matrix in F256 as the seed matrix (M_*) packed as per Section 2.2.1:

```
50 47 50 7d ae 60 64 6d 03 e5 22 7e a8 b3 60 2a 65 76 18 5e e7 e2 a5
02 aa 49 0f 64 94 8c 0e 28 14 31 07 47 6a d1 3e 36 fd 9b 91 cc dd a3
7f 55 bc 5a a5 d0 11 00 2e 20 6f a7 60 a4 73 5e 3e 82 20 14 e9 74 a4
c0 c3 81 04 13 d9 a9 e3 bd ac 9f 39 13 08 ca 9c d3 25 e9 6a 1c 01
```

C.1.4 Tag Conjugates

This keyset uses the following 32 conjugates to generate keypairs for Tags. To reach the required security level the key generator shall choose at least sixteen (16) of these conjugates and their inverses when building the key. Each conjugate below is packed as per Section 2.2.3 with the first two bytes specifying the number of Artin generators in the braid:

```
0. 02 3b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
   63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
   b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86 42
   9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b3 a5 6d 7c 4e 95 b5
   f0 00 88 64 29 af 7b de f7 bd ef 7b df 07 3e 20 19 4a 74 a9 8f 8c 62
   31 04 63 08 42 32 9d 0a 6b de 32 99 0a 6b c2 32 19 0a 6b de e5 35 ed
   6b 5a d7 c5 8f 8c 60 c7 c5 ef 8a d4 d7 be 2b 5b 5a d7 bd ef 8c 58 b6
   bd 4d 7c 14 c7 c1 8f 63 d6 c7 c1 4c 6a 98 c7 39 f1 6b da b6 b9 08 31
   92 64 21 08 42 10 84 21 2b 6b e0 43 21 4c 70 88 64 29 80 11 0c 85 9d
   25 39 ce 85 00 43 29 90 85 84 65 3a 14 c6 30 86 4a 98 c1 10 45 3a 54
```

```
    c7 21 44 32 16 c7 a9 8e 21 d0 b3 a1 4c 63 e2 b6 ad af 89 0e 22 10 c9
    5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98 d2
    9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22 21
    d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
 1. 02 55 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
    4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
    05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
    63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
    b1 f0 6b c6 53 a1 6d 72 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44 31
    90 a6 bd ee 32 56 d3 a1 6d 29 4c 95 ad a1 19 0e 94 9d 2b 6b e2 74 ad
    af 80 04 43 21 4d 7b de f7 bd ef 7b de f8 39 f1 28 06 41 94 80 19 4a
    11 8c 65 3a 54 c7 c6 25 3a 14 c7 c6 30 7c 42 32 99 0a 63 e3 10 8c 86
    42 98 e5 b1 f0 63 96 c7 c1 8f 83 e3 16 bd 6d 5b 5a d7 35 ca 6b d6 d5
    ad 6b 5a d8 b6 b5 6d 7b df 15 ad 8f 8a 98 f8 c6 0a 6a 98 d7 c1 6d 7b
    5f 18 b5 f0 63 9c e6 31 eb 63 9f 17 b5 f1 5b 10 83 19 26 42 10 84 21
    08 42 12 b6 be 04 32 14 c7 08 86 42 98 01 10 c8 59 4e 73 a1 40 10 ca
    64 21 61 19 4e 85 31 8c 21 92 a6 35 02 20 8a 74 a9 8e 42 d8 e3 20 86
    4a 9a 85 34 e8 52 98 f8 19 0a 63 9f 14 ad af 81 04 22 1d 2b 6b 94 d1
    90 e9 53 5f 16 be 05 3a 14 c7 c4 c8 53 1a 53 a0 e9 53 1f 17 c5 ae 21
    90 a5 29 82 29 90 a6 be 2d 6b c8 64 25 4d 08 88 74 a9 ae 42 ce 85 b5
    cc 63 04 43 24 e5 18 00
 2. 02 3f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
    4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
    05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
    63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
    b1 f1 19 4e 95 35 cb 62 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44 31
    90 a6 bd ee 32 56 d3 94 a7 42 da 64 ad 6d 08 c8 74 ad 67 4a da f8 00
    44 32 14 c7 c6 31 8c 63 18 c6 27 4a d8 e7 c5 ef 7c 40 32 0c a4 00 ca
    51 88 23 08 46 11 94 e9 53 1f 10 8c a7 42 98 f8 8c a6 42 98 f8 bc 23
    21 90 a6 bd f0 63 e3 18 29 8f 8b 1f 05 35 f1 8c 63 18 c1 f0 7c 58 f8
    a9 ae 5b 5a f7 b9 af 8c 63 07 c6 2f 7b 5e b6 ad 8b 6a da f3 21 06 32
    4c 84 21 08 42 10 84 25 6d 7c 08 64 29 8e 11 0c 85 30 02 21 90 a2 9d
    07 21 d0 42 10 c7 49 4e 82 9c e8 50 04 32 99 08 58 46 53 a1 4c 63 08
    64 a9 8c 11 04 53 a5 4c 79 cc 85 90 c8 5b 1e 95 b1 e8 53 1a 64 8c 86
    32 44 43 21 4c 63 e2 f8 25 6d 70 88 64 29 4a 6b e2 32 18 87 4a 98 f8
    c1 a9 42 9a 74 a9 ae 32 14 c6 30 44 3a 14 d7 c5 ad 78 ca 64 94 c9 53
    42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
 3. 02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
    4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
    05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
    63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
    b1 f0 6b c6 53 a1 6d 72 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44 31
    90 a6 bd ee 32 56 c2 9c a5 3a 16 d2 99 2b 5b 42 32 1d 2b 59 d2 b6 be
    00 11 0c 85 31 f1 8c 63 18 c6 31 89 d2 b6 39 f1 7b df 10 0c 83 29 00
    32 94 a7 4a 98 f8 94 e8 53 1f 10 8c a6 42 da f0 8c 86 42 9a f8 b5 8f
    8b de d6 bd f1 6b 5a f8 b5 f1 5b 5e b6 bd ef 7a 9a e5 35 ef 7b 96 d7
    c6 2c 7c 56 d7 b9 4d 73 5f 05 b5 8f 53 1f 18 35 ee 53 5e b5 b5 eb 32
    10 63 24 c8 42 10 84 21 08 42 56 d7 c0 86 42 98 e1 10 c8 53 00 22 19
    0a 49 90 92 99 01 19 4c 92 19 0a 32 10 b0 8c a7 42 98 c6 00 44 32 54
    c7 31 c0 11 04 53 a1 6c 7a d8 43 21 6c 71 92 a6 38 87 42 ce 85 31 8f
    8a da b6 be 24 38 88 43 25 6d 70 88 64 29 4a 68 c8 74 a9 af 8b 5f 02
```

```
   9d 0a 63 e3 13 99 0a 63 4a 74 1d 2a 6b da e2 19 0a 52 98 22 99 0a 6b
   e2 d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
4. 02 3f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a f8 08 86 42 4c 85 31 0a
   53 1a f8 19 0a 63 e3 12 9d 2b 6b e2 74 ad af 82 98 f3 a5 6c 7c 0c 85
   31 e5 3a 56 c7 c4 65 3a 54 d7 a1 6d 7c 44 43 21 4c 7c 0e 93 a5 6d 72
   9a f7 10 c6 42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 56 95 88
   86 4a 8c 95 a8 44 32 56 b1 94 e9 5b 5f 11 94 e9 5b 5f 00 08 86 42 9a
   f7 bd ef 7b de f7 bd f0 73 e2 53 a5 4c 7c 63 11 94 e8 53 1f 11 94 c8
   53 1f 07 c5 ef 8c 62 11 90 c9 5b 5a c7 c6 0d 7b e0 f6 3e 0d 7c 5e f8
   3e 0a 63 da b5 b5 ad 6a d6 b6 3e 31 8a 98 e7 c6 0d 7b da e5 35 f0 63
   54 d7 c5 ab 5b 5f 18 35 ed 5b 5f 17 b9 08 31 92 64 21 08 42 10 84 21
   2b 6b e0 43 21 4c 70 88 64 29 80 11 0c 85 a1 40 10 ca 64 21 61 19 4e
   85 31 8c 21 92 a6 35 02 11 4e 95 31 e6 42 86 43 21 6c 7a 56 c7 c5 0a
   69 92 32 18 c9 53 5c 43 21 4c 63 5f 07 08 86 41 92 b1 90 c4 3a 54 c7
   c6 29 42 9a 74 a9 ae 32 14 c6 30 44 3a 14 d7 c5 ad 78 ca 64 94 c9 53
   42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
5. 02 3d b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8 8c
   a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63 e2
   32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 95 b5 e7
   4a da f8 a1 4c 79 d2 b6 3e 06 42 98 f2 9d 2b 63 e2 32 9d 2a 6b d0 b6
   be 03 21 90 a6 3e 29 5b 5c a6 bd e2 21 c8 64 29 af 7b 8c 95 b4 e8 5b
   4a 53 25 6b 68 46 43 a5 2b 11 0c 95 25 6a 11 0c 83 20 c9 5a 8c 95 9d
   29 4a d2 74 9c e9 4a ce 74 ac 65 3a 56 d7 c4 65 3a 56 d7 c0 02 21 90
   a6 bd ef 7b de f7 bd ef 7c 1c f8 84 65 3a 54 c7 c6 25 3a 14 c7 c4 21
   19 4c 85 b5 e1 19 0c 95 35 f1 7c 5f 05 31 f1 6b df 15 b5 ee 53 5e f7
   c6 31 7b e3 17 bd ef 8c 63 18 c5 ef 4a 98 d3 a1 4a 6a 98 c6 31 8c 63
   18 c6 be 04 32 14 c7 08 86 42 98 01 10 c8 50 88 64 19 08 00 ca 64 24
   a6 49 90 a0 8c 86 32 10 b0 8c a7 42 98 c6 00 44 32 54 c6 a0 02 20 8a
   74 a9 8e 42 d8 e3 20 86 4a 9a 85 34 e8 52 98 f8 19 0a 63 9f 11 10 e9
   3a 56 d7 c0 42 21 d2 b6 b9 4c 3a 54 d7 c4 e8 5b 5e b6 be 25 32 14 c7
   c6 24 32 14 c6 b8 86 42 98 c6 10 44 3a 14 d7 c5 ad 79 92 53 25 4d 08
   88 74 a9 ae 42 ce 85 b5 cc 63 04 43 24 e5 18 00
6. 02 4d b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
   63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
   b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86 42
   9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b3 a5 6d 7c 00 22 19
   0a 63 e3 18 c6 31 8c 63 12 9d 2b 63 9f 17 bd f1 00 c8 32 90 03 28 06
   52 88 23 29 d2 a6 3e 23 29 d0 a6 3e 23 29 90 a6 3d 8f 83 5e f7 c5 ae
   6b de f0 8c 86 42 da f8 b1 f1 8b da d6 b9 af 7c 60 a6 3e 2b 5b 1f 06
   be 2f 7c 60 f6 3e 2a 6b e0 b6 bd ed 6b e3 18 ad ae 5b 5e b6 b9 4a 53
   1a f8 b5 6d 7c 1a e4 18 c6 49 cc 84 21 08 42 10 84 25 6d 7c 08 64 29
   8e 11 0c 85 30 02 21 90 b3 a1 40 10 ca 64 21 61 19 4e 85 31 8c 21 92
   a6 30 44 11 4e 95 31 c4 32 16 c7 19 2a 63 8e 85 14 c8 59 4e 85 31 8f
   81 0c 85 31 cf 8a 56 95 b5 f0 10 88 74 ad ae 53 46 43 a5 4d 7c 5a f8
   14 e8 53 1f 13 21 4c 69 4e 83 a5 4c 7c 5f 16 b8 86 42 94 a6 08 a6 42
   9a f8 b5 af 08 c8 71 10 c8 4a 98 74 a9 ae 42 ce 85 b5 cc 63 04 43 24
   e5 18 00
```

```
7. 02 29 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8 8c
   a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63 e2
   32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5 6d
   7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c4 65 3a 54 d7 2d 89 5b 5f 12
   19 0a 63 e2 74 ad ae 53 5e f1 10 c6 42 9a f7 bc 86 21 92 b6 9c a7 29
   d0 b6 99 2b 5b 42 32 1d 2b 59 d2 b6 be 00 11 0c 85 31 f1 8c 63 18 c6
   31 89 d2 b6 39 f1 7b df 10 0c 83 29 00 32 8c 65 29 4a 52 94 21 08 c6
   32 94 a7 4a 98 f8 8c 63 08 46 32 9d 0a 63 e2 f1 94 c8 53 5c d7 be 31
   8c 42 32 19 0a 6b df 07 3e 31 8c 62 f8 ad 4c 7c 58 f8 31 f0 53 1f 05
   b5 cb 6b da f5 35 f1 62 0c 63 24 e6 42 10 84 21 08 42 12 b6 be 04 32
   14 c7 08 86 42 98 01 10 c8 51 c8 60 8c 87 11 0e 85 14 c8 42 c2 32 9d
   0a 63 18 43 25 4c 6a 00 22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e
   85 29 8f 81 90 a6 39 f1 11 0e 93 a5 6d 7c 04 22 1d 2b 6b 94 c3 a5 4d
   7c 4e 85 b5 eb 6b e2 53 21 4c 7c 62 43 21 4c 6b 88 64 29 8c 61 04 43
   a1 4d 7c 5a d7 99 25 32 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32
   4e 51 80
8. 02 3b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
   63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
   b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86 42
   9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 80 04 43 21
   4c 7c 63 18 c6 31 8c 62 53 a5 6c 73 e2 f7 be 25 00 c8 32 90 03 28 06
   52 8c 63 18 80 11 94 21 18 c2 30 8c a7 4a 98 f8 c4 23 29 d0 a6 bd e1
   19 4c 85 b5 af 08 c8 64 ad 4d 7b de f7 ad 6d 7c 58 f8 c1 8e 5b 1f 05
   35 f1 8b 1f 15 35 f1 6b de e5 b5 ea 63 5f 16 b5 c8 31 8c 93 99 08 42
   10 84 21 08 4a da f8 10 c8 53 1c 22 19 0a 60 04 43 21 44 31 82 32 1c
   44 3a 14 53 21 0b 08 ca 74 29 8c 61 0c 95 31 a8 00 88 22 9d 2a 63 96
   c7 25 4c 71 d0 a6 14 c8 53 1a 53 a1 4a 63 e0 43 21 4c 73 e2 95 b5 f0
   10 88 74 ad ae 53 46 43 a5 4d 7c 5a f8 14 e8 53 1f 13 21 4c 69 4e 83
   a5 4c 7c 5f 16 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22 21
   d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
9. 02 41 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8 8c
   a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63 e2
   32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5 6d
   7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c1 af 19 4e 85 b5 c9 5b 5f 12
   19 0a 63 e2 74 ad ae 53 5e f1 10 c6 42 9a f7 b8 c9 5b 4e 85 b4 a5 32
   56 b6 84 64 3a 56 95 9d 2b 6b e2 95 b5 f0 00 88 64 29 af 7b de f7 bd
   ef 7b df 07 3e 20 19 4a 74 a9 8f 88 c6 32 9d 0a 63 e2 10 84 21 19 4c
   85 31 cf 88 46 43 21 4c 72 d8 f8 31 f1 8c 1c f8 ad af 5b 56 b5 b5 af
   72 9a e5 35 ca 62 98 d7 bd ca 6b de a6 b9 4d 7a da d5 ad 6c 5b 5e b6
   bd 6d 7c 62 b6 bd ea 6b dc b6 bd af 7a da f8 3e 0e 63 1c e7 c5 ed 7a
   da e4 20 c6 49 90 84 21 08 42 10 84 ad af 81 0c 85 31 c2 21 90 a6 00
   44 32 16 74 94 e7 3a 14 01 0c a6 42 16 11 94 e8 53 18 c2 19 2a 63 04
   41 14 e9 53 1c 85 10 c8 5b 1e a6 38 87 42 ce 85 31 8f 8a da b6 be 24
   38 88 43 25 6d 70 88 64 29 4a 68 c8 74 a9 af 8b 5f 02 9d 0a 63 e3 13
   99 0a 63 4a 74 1d 2a 6b da e2 19 0a 52 98 22 99 0a 6b e2 d6 bc 86 42
   54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
10.     02 35 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
```

```
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 89 d2 b6
    be 00 11 0c 85 35 ef 7b de f7 bd ef 7b e0 e7 c4 a0 19 06 52 00 65 29
    4a 52 94 e9 53 1f 18 84 65 3a 14 d7 bd ee 08 ca 64 29 af 78 46 43 25
    6d 6b 56 d5 b5 f1 8a da e6 bd ef 7b df 15 b5 8b 6b 5a c7 c6 0c 6b dc
    a6 bd f1 5b 5e f7 c5 ef 8a 98 f8 29 8c 63 5f 05 b5 ea 63 5c 84 18 c9
    32 10 84 21 08 42 10 95 b5 f0 21 90 a6 38 44 32 14 c0 08 86 42 8a 73
    a1 40 10 ca 64 21 61 19 4e 85 31 8c 21 92 a6 35 02 20 8a 74 a9 8e 42
    d8 e3 20 86 4a 9a 85 34 e8 52 98 f8 19 0a 63 9f 14 ad af 81 04 22 1d
    2b 6b 94 d1 90 e9 53 5f 16 be 05 3a 14 c7 c4 c8 53 1a 53 a0 e9 53 1f
    17 c5 ae 21 90 a5 29 82 29 90 a6 be 2d 6b c8 64 25 4d 08 88 74 a9 ae
    42 ce 85 b5 cc 63 04 43 24 e5 18 00
11.     02 37 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 c3 29 d2 b6 3e 0d 78 ca 74 2d 89 5b 5f
    12 19 0a 63 e2 74 ad ae 6b de 22 19 0a 42 9a f7 bd 6c 29 ca 53 a1 6d
    29 92 b5 b4 23 21 d2 b5 88 86 4a 8c 95 a8 44 32 56 94 a5 2b 4a 56 74
    9c e9 5a ce 94 ad 63 29 d2 b6 be 23 29 d2 b6 be 00 11 0c 85 35 ef 7b
    de f7 bd ef 7b e0 e7 c4 23 29 d2 a6 3e 21 19 4e 85 31 f1 7c 42 32 99
    0a 63 e2 d0 8c 86 42 d8 f8 31 f1 82 98 f8 c6 2d 5a d6 c7 c5 ad 63 e3
    06 be 0a 63 e2 d7 bd 6d 7b 5f 14 29 66 42 16 85 29 4a 52 94 a5 29 6d
    7c 08 64 29 8e 11 0c 85 30 02 21 90 b3 a0 02 21 c8 72 1c 87 42 82 22
    14 c8 42 c2 32 9d 0a 63 18 43 25 4c 60 04 41 14 e9 53 1c 85 b1 c9 53
    0e 85 31 85 32 14 c7 3c a6 4a 98 c7 c0 86 42 98 e7 c4 e9 5a 56 d7 c0
    42 21 d2 b6 b9 4d 19 0e 95 35 f1 3a 16 d7 ad af 89 4c 85 31 f1 89 0c
    85 31 ae 21 90 a6 31 84 11 0e 85 35 f1 6b 5e 64 94 c9 53 42 22 1d 2a
    6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
12.     02 21 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c4 65 3a 54 d7 2d 89 5b 5f
    12 19 0a 63 e2 74 ad ae 53 5e f1 10 c6 42 9a f7 b8 c9 5b 4e 85 b4 a5
    32 56 b6 84 64 3a 56 95 9d 2b 6b e2 95 b5 f0 00 88 64 29 af 7b de f7
    bd ef 7b df 07 3e 20 19 4a 74 a9 8f 88 c6 32 9d 0a 6b e2 10 84 21 08
    42 10 84 23 29 90 a6 3e 2d 7b 9a f0 8c 86 42 9a f8 c6 31 8a d8 b6 2d
    8f 8a d8 b6 3e 2f 7b e2 b5 31 f0 5b 5e f8 ad 8f 8a 9a f8 b5 eb 6b e0
    a5 29 8d 7c 5a b6 be 08 41 8c 93 21 08 42 10 84 21 09 5b 5f 02 19 0a
    63 84 43 21 4c 00 88 64 28 a7 3a 14 01 0c a6 42 16 11 94 e8 53 18 c2
    19 2a 63 50 22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 81
    90 a6 39 f1 4a da f8 10 42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0 53 a1
    4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22 99 0a 6b e2
    d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
13.     02 1b b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 cf 80 ca 74 a9 af 88 ca 74 2d 89 5b 5f
    12 19 0a 63 e2 74 ad ae 6b de 22 19 08 53 5e f7 25 6d 3a 16 d2 94 c9
    5a da 11 90 e9 49 d2 b6 be 27 4a da f8 00 44 32 14 d7 bd ef 7b de f7
    bd ef 83 9f 12 80 64 19 48 01 94 a3 18 ca 52 9d 2a 63 e3 12 9d 0a 63
    e0 f0 8c a6 42 98 f8 bc 23 21 92 b6 b5 cd 7b de f7 bd ca 53 5e d6 b5
    ad 6b e2 c7 ad 8b 63 e0 a6 bd f0 72 d8 f5 b5 8e 7c 56 d7 c6 2f 6a da
    f8 be 2d 6b e0 84 18 c9 32 10 84 21 08 42 10 95 b5 f0 21 90 a6 38 44
    32 14 c0 08 86 42 8a 73 a1 40 10 ca 64 21 61 19 4e 85 31 8c 21 92 a6
    35 02 20 8a 74 a9 8e 42 d8 e3 20 86 4a 9a 85 34 e8 52 98 f8 ad af 89
    0e 22 10 c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4
    e6 42 98 d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90
    95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
14.       02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b3 a5 6d 7c 00 22
    19 0a 63 e3 18 c6 31 8c 63 12 9d 2b 63 9f 17 bd f1 00 c8 32 90 02 19
    4a 51 8c 81 19 4e 95 31 f1 08 ca 74 29 af 8b e2 11 94 c8 53 5e 11 90
    c8 53 5f 18 b5 af 7b df 18 ad ae 5b 5c d7 bd ee 53 5e f6 ad af 8a d8
    f8 c5 4c 7c 14 c7 c5 6c 7c 60 d7 c1 4d 53 1f 16 b1 f0 6b 96 d7 a9 af
    82 da e6 a9 8d 72 96 d7 ac c8 41 8c 93 21 08 42 10 84 21 09 5b 5f 02
    19 0a 63 84 43 21 4c 00 88 64 2c e8 50 04 32 99 08 58 46 53 a1 4c 63
    08 64 a9 8d 40 88 22 9d 2a 63 96 c7 25 4c 71 0e 85 30 a6 42 9a 53 a1
    4a 63 e2 b6 be 22 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be 2d 7c 0a
    74 29 8f 8c 4e 64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a 64 29 af
    8b 5a f0 8c 87 11 0c 84 a9 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51
    80
15.       02 51 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 89 d2 b6
    be 00 11 0c 85 35 ef 7b de f7 bd ef 7b e0 e7 c4 a0 19 06 52 00 65 08
    c6 40 8c 65 28 ca 74 a9 8f 88 46 53 a1 4c 7c 63 11 94 c8 53 1e 11 90
    c8 5b 1e b6 3e 0a 63 96 c7 c1 8e 7a 98 e6 3e 0c 7c 14 c7 b1 f0 63 d8
    f8 31 f1 6b d6 d5 ad 6c 52 da f5 35 cb 6b da f6 ad af 8c 58 f8 39 cf
    8b d6 d7 b9 6d 7a da f8 39 f1 7b 5f 15 b1 08 31 92 64 21 08 42 10 84
    21 2b 6b e0 43 21 4c 70 88 64 29 80 11 0c 85 94 e7 3a 14 01 0c a6 42
    16 11 94 e8 53 18 c2 19 2a 63 04 41 14 e9 53 1c 85 10 c8 5b 1e a6 38
    87 42 ce 85 31 8f 8a da b6 be 24 38 88 43 25 6d 70 88 64 29 4a 68 c8
    74 a9 af 8b 5f 02 9d 0a 63 e3 13 99 0a 63 4a 74 1d 2a 6b da e2 19 0a
    52 98 22 99 0a 6b e2 d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6
    30 44 32 4e 51 80
16.       02 39 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a7 19 4c 95 b1 f0 3a 54 d7 08 86 42 98 85 30
    c8 42 54 d7 c1 4c 7c 62 53 a5 2b 6b e0 c7 9d 2b 63 e0 85 31 e5 3a 56
    c7 c4 65 3a 54 d7 a1 6d 7c 48 64 29 8f 8a 56 d7 29 af 78 88 72 19 0a
    6b de e3 25 6d 3a 16 d2 94 c9 5a da 11 90 e9 4a ce 95 b5 f1 3a 56 d7
    c0 02 21 90 a6 bd ef 7b de f7 bd ef 7c 1c f8 80 64 19 48 01 94 83 28
    c6 51 94 e9 53 1f 12 9d 0a 63 e3 11 94 c8 5b 1c f8 31 f1 88 46 43 21
    4c 7c 56 b5 ad 6b 6b da f6 b5 ad 73 5f 18 ad ad 7b dc a6 a9 ae 5b 5e
    d7 b5 f1 63 e3 06 39 cf 82 9a a6 31 ae 5b 5f 15 b1 08 31 92 64 21 08
    42 10 84 21 2b 6b e0 43 21 4c 70 88 64 29 80 11 0c 85 94 e8 29 ce 85
    00 43 29 90 85 84 65 3a 14 c6 30 86 4a 98 c1 10 45 3a 54 c7 21 6c 72
    54 c3 a1 4c 61 4c 85 31 cf 29 92 a6 31 f1 4a da b1 10 86 4a da f8 ad
    ae 11 0c 85 29 4d 19 0e 95 35 f1 6b e0 53 a1 4c 7c 62 73 21 4c 69 4e
    83 1d 2a 6b da e2 19 0a 52 98 22 99 0a 6b e2 d6 bc 86 42 54 d0 88 87
    4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
17.      02 3b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 80 04 43
    21 4c 7c 63 18 c6 31 8c 62 53 a5 6c 73 e2 f7 be 25 00 c8 32 90 03 29
    4a 52 94 a7 4a 98 f8 84 65 3a 14 c7 c4 65 32 14 c7 c1 f1 08 c8 64 29
    ae 6b e0 b6 39 f0 63 e3 18 3e 0b 63 e0 d7 c1 f0 7c 63 18 b5 ed 73 5e
    f7 bd ef 7b de e6 bd ed 6b 5c b6 be 2b 6a d6 a4 18 c6 49 cc 84 21 08
    42 10 84 25 6d 7c 08 64 29 8e 11 0c 85 30 02 21 90 a3 1d 25 39 d0 53
    94 a7 49 ce 85 00 43 29 90 85 84 65 3a 14 c6 30 86 4a 98 d4 08 82 29
    d2 a6 39 6c 72 54 c7 1d 0a 61 4c 85 31 a5 3a 14 a6 3e 2b 6b e2 22 10
    c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98
    d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22
    21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
18.      02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 cb 62 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44
    31 90 a6 bd ee 32 56 c2 9c a5 3a 16 d2 99 2b 5b 42 32 1d 2b 59 d2 b6
    be 00 11 0c 85 31 f1 8c 63 18 c6 31 89 d2 b6 39 f1 7b df 10 0c 83 29
    00 32 94 63 18 c2 10 8c a5 29 d2 a6 3e 31 08 46 31 84 61 18 46 53 a1
    4c 7c 42 32 99 0b 6b 5a 11 90 c8 5b 1f 18 a9 8f 83 e0 a6 3e 2d 7b de
    f7 c6 2b 5b 16 c7 c5 4c 7c 14 c7 b1 f0 7c 18 e7 b1 f1 6b e2 b6 bd ca
    5b 5e b3 21 06 32 4c 84 21 08 42 10 84 25 6d 7c 08 64 29 8e 11 0c 85
    30 02 21 90 b3 a4 a5 3a 0a 73 a1 40 10 ca 64 21 61 19 4e 85 31 8c 21
    92 a6 35 02 20 8a 74 a9 8e 42 d8 e3 25 4c 3a 14 53 21 4c 69 4e 85 29
    8f 81 0c 85 31 cf 8a 56 d7 c0 42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0
    53 a1 4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22 99 0a
    6b e2 d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51
    80
19.      02 2f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 89 d2 b6
    be 00 11 0c 85 35 ef 7b de f7 bd ef 7b e0 e7 c4 a0 19 4a 31 04 63 19
    4a 52 9d 2a 63 e0 11 8c 21 18 46 11 94 e8 53 1f 17 bc 23 29 90 b6 b5
    af 78 46 43 21 4d 7c 1a f7 ad ad 6b 5a f8 3d 6b 5a d8 e7 c6 0d 7c 5f
    05 31 8f 63 e0 c7 c1 aa 63 1a e5 b5 f1 5b 10 83 19 26 42 10 84 21 08
    42 12 b6 be 04 32 14 c7 08 86 42 98 01 10 c8 59 4e 82 9c e8 50 04 32
```

```
   99 08 58 46 53 a1 4c 63 08 64 a9 8d 40 88 22 9d 2a 63 96 c7 25 4c 71
   d0 a6 14 c8 53 1a 53 a1 4a 63 e2 b6 be 22 21 0c 95 b5 c2 21 90 a5 29
   a3 21 d2 a6 be 2d 7c 0a 74 29 8f 8c 4e 64 29 8d 29 d0 74 a9 af 6b 88
   64 29 4a 60 8a 64 29 af 8b 5a f2 19 09 53 42 22 1d 2a 6b 90 b3 a1 6d
   73 18 c1 10 c9 39 46 00
20.     02 2f b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
   8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
   e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 95 b5
   e7 4a da f8 a1 4c 79 d2 b6 3e 06 42 98 f2 9d 2b 63 e0 d7 8c a7 42 da
   e4 ad af 80 c8 64 29 8f 89 d2 b6 b9 4d 7b c4 43 19 0a 6b de e3 25 6c
   29 ca 53 a1 6d 29 92 b5 b4 23 21 d2 b5 9d 2b 6b e2 95 b5 f0 00 88 64
   29 af 7b de f7 bd ef 7b df 07 3e 20 19 06 52 00 64 19 00 32 84 23 19
   42 10 8c 61 08 42 11 8c 21 08 42 32 84 65 3a 54 c7 c6 21 19 4e 85 35
   ef 7c 42 32 99 0b 68 46 43 21 6c 5b 1f 06 3e 30 5b 1f 17 31 af 7b 5a
   d7 be 2d 7a 9a f8 2d af 8a d8 f8 a9 8c 6b 94 b6 bd 48 41 8c 93 21 08
   42 10 84 21 09 5b 5f 02 19 0a 63 84 43 21 4c 00 88 64 2c e8 50 04 32
   99 08 58 46 53 a1 4c 63 08 64 a9 8d 40 8a 74 a9 83 29 d0 a6 39 0b 63
   8c 95 31 c4 3a 14 d3 21 4c 69 4e 85 29 8f 8a da f8 88 84 32 56 d7 08
   86 42 94 a6 8c 87 4a 9a f8 b5 f0 29 d0 a6 3e 31 39 90 a6 35 c6 42 98
   c6 18 44 3a 14 d7 c5 ad 78 ca 64 94 c9 53 42 22 1d 2a 6b 90 b3 a1 6d
   73 18 c1 10 c9 39 46 00
21.     02 43 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
   42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 89 d2 b6
   be 00 11 0c 85 35 ef 7b de f7 bd ef 7b e0 e7 c4 a0 19 06 52 8c 65 3a
   54 c7 c0 01 18 42 10 84 23 08 ca 74 29 8f 8c 46 53 21 4c 7c 1f 18 c4
   23 21 90 b6 3e 0c 7c 56 d7 ad af 5a 9a f7 b9 6c 5b 5e d7 35 4d 72 da
   f7 c1 8e 63 9f 15 ad 4c 7c 62 d7 b5 6d 7b d6 d7 c6 0a 6b e3 06 35 f0
   52 da b6 b9 08 31 92 64 21 08 42 10 84 21 2b 6b e0 43 21 4c 70 88 64
   29 80 11 0c 85 10 a6 29 ce 85 00 43 29 90 85 84 65 3a 14 c6 30 86 4a
   98 d4 08 82 29 d2 a6 39 0b 63 8c 82 19 2a 6a 14 d3 a1 4a 63 e0 64 29
   8e 7c 52 b6 be 04 10 88 74 ad ae 53 46 43 a5 4d 7c 5a f8 14 e8 53 1f
   13 21 4c 69 4e 83 a5 4c 7c 5f 16 b8 86 42 94 a6 08 a6 42 9a f8 b5 af
   21 90 95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
22.     02 4b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f0 6b c6 53 a1 6d 72 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44
   31 90 a6 bd ee 32 56 c2 9c a5 3a 16 d2 99 2b 5b 42 32 1d 2b 59 d2 b6
   be 29 5b 5f 00 08 86 42 9a f7 bd ef 7b de f7 bd f0 73 e2 01 90 65 20
   04 01 90 23 08 42 32 94 a3 29 42 32 9d 2a 63 e3 10 8c a7 42 9a f7 84
   65 32 14 d7 bd f1 63 e2 11 90 c9 5a 98 f8 29 8c 7b 1f 06 be 2f 7c 1c
   f8 b5 ef 7b d4 d7 c1 6d 6b e3 18 c6 0f 5b 1f 18 c5 4d 7b df 18 be 0a
   63 9c c6 3d 6c 73 e2 e5 b5 f1 5b 5a e4 20 c6 49 90 84 21 08 42 10 84
   ad af 81 0c 85 31 c2 21 90 a6 00 44 32 16 73 a1 40 10 ca 64 21 61 19
   4e 85 31 8c 21 92 a6 35 02 20 8a 74 a9 8e 42 d8 e3 20 86 4a 9a 85 34
   e8 52 98 f8 ad af 89 0e 22 10 c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2
```

```
    d7 c0 a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6
    42 9a f8 b5 af 21 90 95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93
    94 60
23.      02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 bc e9 5b 5f 04 ad af 81 0c 85 2d 8f 8c 04 53 a1 4d 7c
    10 a6 38 23 29 92 b6 3e 23 21 d2 a6 b8 44 32 12 64 29 88 52 98 d7 c0
    c8 53 1f 18 94 e9 5b 5e 74 ad af 8a 14 c7 9d 2b 63 e0 64 29 8f 29 d2
    b6 3e 23 29 d2 a6 bd 0b 6b e0 32 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
    42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b1 10 c9 52 56 a1
    10 c9 52 12 b5 19 2b 5a ce 93 9d 2b 19 4e 95 b5 f1 19 4e 95 b5 f0 00
    88 64 29 af 7b de f7 bd ef 7b df 07 3e 21 19 4e 95 31 f1 29 d0 a6 3e
    31 08 ca 64 2d 8f 88 46 43 25 4c 7c 1f 18 b5 ed 6b 5e e6 bd ee 53 1a
    e5 b5 ad 6b 9a f6 bd ad 7b 56 d7 b5 6d 7c 58 f8 ad ae 53 14 c5 35 ed
    72 94 a6 35 f1 6a da f8 35 c6 41 8c 64 9c c8 42 10 84 21 08 42 56 d7
    c0 86 42 98 e1 10 c8 53 00 22 19 0b 3a 14 01 0c a6 42 16 11 94 e8 53
    18 c2 19 2a 63 04 41 14 e9 53 1c 85 10 c8 5b 1e a6 38 87 42 ce 85 31
    8f 81 90 a6 39 f1 4a d2 b6 be 04 10 88 74 ad ae 53 46 43 a5 4d 7c 4e
    85 b5 eb 6b e2 53 21 4c 7c 62 43 21 4c 6b 88 64 29 8c 61 04 43 a1 4d
    7c 5a d7 99 25 32 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51
    80
24.      02 27 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c4 65 3a 54 d7 a1 6d 7c 48
    64 29 8f 8a 56 d7 29 af 78 88 72 19 0a 6b de e3 25 6d 3a 16 d2 94 c9
    5a da 11 90 e9 49 d2 b6 be 27 4a da f8 00 44 32 14 d7 bd ef 7b de f7
    bd ef 83 9f 12 80 64 19 48 01 94 a4 19 46 31 84 23 29 d2 a6 3e 25 3a
    14 c7 c4 65 32 14 d0 8c 86 4a 9a f7 c1 f1 6b da d7 31 af 7b da e5 35
    4d 72 9a f7 bd ef 7b de a6 be 0b 63 e2 b6 be 0a 63 e0 b6 be 31 7c 60
    d7 c5 6b 6b e3 05 31 8d 7b 56 d6 b9 08 31 92 64 21 08 42 10 84 21 2b
    6b e0 43 21 4c 70 88 64 29 80 11 0c 85 9c e8 50 04 32 99 08 58 46 53
    a1 4c 63 08 64 a9 8d 40 88 22 9d 2a 63 96 c7 25 4c 71 0e 85 30 a6 42
    9a 53 a1 4a 63 e2 b6 be 22 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be
    2d 7c 0a 74 29 8f 8c 4e 64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a
    64 29 af 8b 5a f2 19 09 53 42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9
    39 46 00
25.      02 53 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
    4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
    95 b1 f0 6b c6 53 a1 6d 72 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44
    31 90 a6 bd ef 21 88 64 ad a7 29 ca 74 2d a6 4a d6 d0 8c 87 4a d6 74
    ad af 80 04 43 21 4c 7c 63 18 c6 31 8c 62 74 ad 8e 7c 5e f7 c4 03 20
    ca 40 0c a3 19 4e 95 31 f1 88 46 53 a1 4d 7b df 10 8c a6 42 da d0 8c
    86 42 da f5 35 ca 6a 9a e5 31 aa 6b de d5 b5 8a 5b 56 b5 b5 ed 7a da
    f5 b5 eb 6b e2 b6 3e 30 63 96 c7 c1 f0 63 9e d6 b5 8f 82 98 f8 2d 8f
    83 1f 15 b5 eb 6b d4 c6 bd eb 53 1a f8 31 ae 41 8c 64 9c c8 42 10 84
    21 08 42 56 d7 c0 86 42 98 e1 10 c8 53 00 22 19 0a 29 ce 85 00 43 29
    90 85 84 65 3a 14 c6 30 86 4a 98 c1 10 45 3a 54 c7 21 44 32 16 c7 a9
    8e 21 d0 b3 a1 4c 63 e2 b6 ad af 89 0e 22 10 c9 5b 5c 22 19 0a 52 9a
    32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86
```

```
   42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22 21 d2 a6 b9 0b 3a 16 d7
   31 8c 11 0c 93 94 60
26.     02 41 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f1 19 4e 95 35 cb 62 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44
   32 14 64 29 af 7b d6 d3 a1 6d 29 4c 95 ad a1 19 0e 94 9c e9 5b 5f 13
   a5 6d 70 04 43 21 4d 7b de f7 bd ef 7b de f8 39 f1 28 06 41 94 80 19
   06 53 a5 4c 7c 4a 74 29 8e 78 ca 64 2c 23 21 90 a6 3d 6d 63 e2 a6 bd
   f0 53 5e f7 c1 f1 5b 5e b5 b5 8b 6b de b6 2d 8b 6b df 18 ad ae 53 5e
   f7 29 af 7b d6 d6 be 0a 63 e3 18 35 ef 7c 62 d7 b5 f0 7a d8 e7 c5 ed
   7a da e4 20 c6 49 90 84 21 08 42 10 84 ad af 81 0c 85 31 c2 21 90 a6
   00 44 32 16 74 94 e7 3a 14 01 0c a6 42 16 11 94 e8 53 18 c2 19 2a 63
   50 22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 8a da f8 90
   e2 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be 2d 7c 0a 74 29 8f 8c 4e
   64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a 64 29 af 8b 5a f0 8c 87
   11 0c 84 a9 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
27.     02 4d b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
   42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 74 ad af 89 d2 b6
   be 00 11 0c 85 35 ef 7b de f7 bd ef 7b e0 e7 c4 a0 19 06 52 00 65 29
   d2 a6 3e 31 08 ca 74 29 af 78 42 10 8c a6 42 9a f0 8c 86 42 da f8 b1
   ea 63 e0 c7 c1 4c 72 d8 f8 31 eb 63 e3 06 3e 2d 72 96 d7 ad ad 6b 5c
   a6 bd eb 6b 5a d7 b5 ed 7c 62 b5 b5 8b 6a da b5 b5 ef 8b 56 d6 3e 0c
   7c 5c a5 2d af 8a 98 d7 21 06 32 4c 84 21 08 42 10 84 25 6d 7c 08 64
   29 8e 11 0c 85 30 02 21 90 a2 9c e8 50 04 32 99 08 58 46 53 a1 4c 63
   08 64 a9 8c 11 04 53 a5 4c 72 14 43 21 6c 7a 98 e2 1d 0b 3a 14 c6 3e
   2b 6a da 43 88 84 32 56 d7 c5 ae 11 0c 85 29 4d 19 0e 95 35 f1 3a 16
   d7 ad af 89 4c 85 31 f1 89 48 64 29 8c 31 d2 a6 bd ae 21 90 a5 29 82
   29 90 a6 be 2d 6b c8 64 25 4d 08 88 74 a9 ae 42 ce 85 b5 cc 63 04 43
   24 e5 18 00
28.     02 2f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
   42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b3 a5 6d 7c 4e 95
   b5 f0 00 88 64 29 af 7b de f7 bd ef 7b df 07 3e 20 19 06 52 00 65 29
   4e 95 31 f1 19 4e 85 31 f1 88 ca 64 29 8f 8c 42 32 19 0b 6b 1f 16 b1
   f1 53 1f 16 bd af 7b 5e f6 bd ad 7b da f7 b5 ca 6b e2 b6 b5 ef 8c 56
   b6 b5 ad 5b 56 d7 c1 8c 73 e0 a6 35 f1 6a da e4 20 c6 49 90 84 21 08
   42 10 84 ad af 81 0c 85 31 c2 21 90 a6 00 44 32 16 74 28 02 19 4c 84
   2c 23 29 d0 a6 31 a2 21 92 a6 35 02 20 8a 74 a9 8e 5b 1c 95 31 c7 42
   98 53 21 4c 69 4e 85 29 8f 8a da f8 88 84 32 56 d7 08 86 42 94 a6 8c
   87 4a 9a f8 b5 f0 29 d0 a6 3e 31 39 90 a6 34 a7 41 d2 a6 bd ae 21 90
   a5 29 82 29 90 a6 be 2d 6b c2 32 1c 44 32 12 a6 1d 2a 6b 90 b3 a1 6d
   73 18 c1 10 c9 39 46 00
```

```
29.      02 41 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 bc e9 5b 5f 04 ad af 81 0c 85 2d 8f 8c 04 53 a1 4d 7c
   10 a6 38 23 29 92 b6 3e 23 21 d2 a6 b8 44 32 12 64 29 88 52 98 d7 c0
   c8 53 1f 18 94 e9 5b 5e 74 ad af 8a 14 c7 9d 2b 63 e0 64 29 8f 29 d2
   b6 3e 23 29 d2 a6 bd 0b 6b e0 32 19 0a 63 e2 95 b5 ca 6b de 22 1c 86
   42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 84 64 3a 52 b1 10 c9 52 56 a1
   10 c9 59 d2 95 ad 67 4a 56 b5 ac 65 3a 56 d7 c0 02 21 90 a6 3e 31 8c
   63 18 c6 31 08 ca 74 ad 8e 7c 5e f7 c4 23 29 d2 a6 3e 31 08 ca 74 29
   8f 83 e2 11 94 c8 53 1f 10 8c 86 42 9a f8 ad ae 5b 5e d7 c6 2d 7b e3
   18 c6 0d 7b e3 18 c6 31 8c 62 f8 c5 af 6b 94 c5 29 aa 63 5f 16 bc e8
   52 cc 84 2d 0a 52 94 a5 29 4a 52 da f8 10 c8 53 1c 22 19 0a 60 04 43
   21 40 11 0c 72 1c 87 42 82 22 14 c8 42 c2 32 9d 0a 63 18 43 25 4c 60
   04 41 14 e9 53 1c 85 10 c8 5b 1e a6 38 87 42 ce 85 31 8f 8a da b6 be
   24 38 88 43 25 6d 70 88 64 29 4a 68 c8 74 a9 af 8b 5f 02 9d 0a 63 e3
   13 99 0a 63 4a 74 1d 2a 6b da e2 19 0a 52 98 22 99 0a 6b e2 d6 bc 86
   42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
30.      02 3b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21
   4a 63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e
   95 b1 f1 19 4e 95 35 cb 62 56 d7 c4 86 42 98 f8 9d 2b 6b 94 d7 bc 44
   31 90 a6 bd ee 32 56 d3 94 a7 42 da 64 ad 6d 08 c8 74 ad 67 4a da f8
   00 44 32 14 c7 c6 31 8c 63 18 c6 27 4a d8 e7 c5 ef 7c 40 32 0c a4 00
   ca 52 84 63 20 46 32 9d 2a 63 e2 53 a1 4c 7c 5e f0 84 65 32 14 d7 84
   64 32 16 d7 c5 8f 8b e2 b6 bd af 7b de d7 2d ae 5b 5f 18 b1 f0 7c 63
   18 31 f1 6b 58 f8 c6 2b 5a 9a f7 29 af 53 5f 05 2d af 8b 5e a6 35 ca
   5b 5e a4 18 c6 49 cc 84 21 08 42 10 84 25 6d 7c 08 64 29 8e 11 0c 85
   30 02 21 90 b3 a1 40 10 ca 64 21 61 19 4e 85 31 8c 21 92 a6 35 02 20
   8a 74 a9 8e 42 d8 e3 20 86 4a 9a 85 34 e8 52 98 f8 ad af 89 0e 22 10
   c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98
   d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22
   21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
31.      02 3b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 bc e9 5b 5f 04 ad af 81 0c 85 2d 8f 8c 04 53 a1 4d 7c
   10 a6 38 23 29 92 b6 3e 23 21 d2 a6 b8 44 32 12 64 29 88 52 98 d7 c0
   c8 53 1f 18 94 e9 3a 56 d7 c5 4c 79 d2 b6 3e 08 53 1e 53 a5 6c 7c 46
   53 a5 4d 72 d8 95 b5 f1 21 90 a6 3e 27 4a da e5 35 ef 11 0c 64 29 af
   7b c8 62 19 2b 69 ca 72 9d 0b 69 92 b5 b4 23 21 d2 b5 9d 2b 6b e0 01
   10 c8 53 1f 18 c6 31 8c 63 18 9d 2b 63 9f 17 bd f1 00 ca 51 88 23 20
   46 52 84 21 18 ca 51 94 a3 29 d2 a6 3e 31 19 4e 85 31 f1 19 4c 85 31
   f1 7b 5a f0 8c 86 4a 9a f7 29 af 83 1f 06 b9 af 7b df 18 b5 ef 7b 5a
   f7 b5 ed 7a d6 b5 a9 06 31 92 73 21 08 42 10 84 21 09 5b 5f 02 19 0a
   63 84 43 21 4c 00 88 64 28 87 29 0c 74 9d 04 21 0c 74 1d 25 3a 4e 85
   00 43 29 90 a4 2c 23 29 d0 a6 31 84 32 54 c6 08 85 3a 54 c7 21 6c 72
   54 c3 a1 4c 61 4c 85 31 cf 29 92 a6 31 f0 21 90 a6 39 f0 11 4c 95 94
   e9 59 d2 b6 be 02 21 d2 b6 b9 4c 3a 54 d7 c5 af 81 4e 85 31 f1 89 90
   a6 35 c6 42 98 c6 18 44 3a 14 d7 c5 ad 78 ca 01 94 c9 21 92 32 99 2a
   61 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
```

C.1.5 Interrogator Conjugates

This keyset uses the following 32 conjugates to generate keypairs for Interrogators. To reach the required security level the key generator shall choose at least sixteen (16) of these conjugates and their inverses when building the key. Each conjugate below is packed as per Section 2.2.3 with the first two bytes specifying the number of Artin generators in the braid:

```
0. 02 3f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 04 65 3a 14 d7 c4 65 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d 2b
   6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98 e7
   c0 c8 53 1e 53 a5 6c 7c 46 53 a5 69 53 5f 03 21 4d 11 0c 85 31 f0 21
   d2 74 ad af 29 d0 a6 bd c6 42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 11 90
   c9 5a d2 b6 bc e9 5b 5f 00 08 86 42 98 f8 c6 31 8c 63 18 c6 25 3a 56
   d7 be 0f 8b e2 95 31 f1 82 98 e7 3e 31 53 1f 18 c6 31 8c 63 16 b5 af
   7c 62 f6 be 08 53 1f 18 c6 31 8a d8 f8 31 f1 82 9a b5 35 ef 7b dc a6
   bd f0 7c 62 b6 ad 6b 5a d6 b5 ad 6d 62 d8 f8 bd ee 53 5f 05 31 f1 6b
   d4 c6 b9 4c 53 18 d5 ad 4d 7c 5e d7 ad 6d 7a da f8 21 0a 52 10 a5 29
   4a 52 94 a5 29 6d 7c 0c 85 10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a 00
   22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 8a da f8 0c 87
   11 08 64 ad ae 11 0c 85 29 4d 18 c8 74 a9 af 8b 5f 02 9d 0a 63 e3 05
   9c c8 53 1a e3 21 4c 63 04 43 a1 4d 7c 5a d7 8c a0 19 4c 92 19 23 29
   92 a6 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
1. 02 23 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8 8c
   a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63 e2
   32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5 6d
   7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c4 65 3a 54 d7 2d 89 5b 5f 12
   19 0a 63 e2 74 ad ae 53 5e f1 10 c6 42 9a f7 be 06 4a d8 53 94 e8 5b
   4a 64 ad 6d 7c 42 32 1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7 bd
   ef 7b de f7 bd f0 73 e2 f8 be 2a 6b de e5 b5 f0 4a d6 c5 b5 af 73 1a
   f7 bd ab 6b d6 d7 ad af 8c 62 b6 be 2a 63 e3 05 31 f0 7c 5f 15 b5 ae
   53 5f 15 31 f0 7c 56 a6 3e 2d 7b 5a d6 b5 cd 73 5f 18 3e 31 8b de f7
   c6 30 53 18 f8 39 cf 82 98 c6 29 ae 53 54 d7 2d af 8a da f6 bd 6d 7b
   e0 84 29 48 42 94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85 31
   8c 11 0c 95 31 a8 00 88 22 9d 2a 63 90 b6 38 c8 21 92 a6 a1 4d 3a 14
   a6 3e 06 42 98 e7 c5 2b 6b e0 22 08 44 3a 56 d7 29 a3 19 0e 95 35 f1
   6b e0 c2 9d 0a 63 e3 13 21 4c 6b 8c 85 31 8c 11 0e 85 35 f1 6b da e6
   8c a6 49 4c 95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
2. 02 4f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 98 85 35 e7 4a da f8 ad af 81 0c 85 2d 8f 8c 04 53 a1 4d 7c 10
   a6 38 23 29 92 b6 3e 23 21 d2 a6 bc e9 5b 5f 01 10 c6 42 da f8 19 0a
   6a 98 e2 18 e9 5b 1f 04 29 8f 63 e2 74 a9 ae 5b 4c 95 b5 ef 19 0e 22
   18 e9 5b 5f 13 a5 6d 79 4e 95 35 ed 7c 04 43 21 44 32 14 c7 08 87 11
   0c 85 31 f1 5b 5e a6 bd ca 6b de e4 ad a5 3a 16 d2 94 c9 5a da f0 8c
   87 4a d2 b3 a5 6d 7c 00 22 19 0a 63 e3 18 c6 31 8c 63 18 9d 2b 6b df
   07 c5 f1 4a 98 f8 c1 4c 73 9f 18 a9 8f 83 e2 f7 bd f1 6b 5f 04 29 8f
   8a d8 f8 c5 6c 5b 5a f5 b5 ab 5a da f8 c6 2f 8b e2 b6 b5 ad 7b de f8
   29 ae 53 5e f6 b5 af 7c 56 d5 b1 f0 53 1f 16 bd ee 6b de e5 35 f0 5b
   1f 18 c1 8f 5b 1f 17 35 ea 6b 9a f8 b5 f0 53 18 f6 39 cf 8a da f5 b5
   ca 6a 9a f8 29 8a 63 5e b6 21 4a 52 10 b4 29 4a 52 94 a5 29 4b 6b e0
   63 19 0a 21 90 85 9d 0a 63 18 22 19 2a 63 50 01 10 42 29 d2 a6 39 0b
   63 8c 82 19 2a 6a 14 d3 a1 4a 63 e2 b6 be 03 21 c4 42 19 2b 6b 84 43
   21 4a 53 5f 03 a5 4c 7c 60 d4 a1 4d 18 8a 74 a9 ae 32 14 c6 30 44 3a
   14 d7 c5 ad 78 ca 64 94 c9 53 42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10
   c9 39 46 00
3. 02 2b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42 98
   e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 63 a1 6d
   79 92 b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14 c7 3e 03 29 d2 a6
   be 23 29 d2 85 b5 f0 32 14 d1 10 c8 53 1f 13 a5 6d 73 5e e4 29 af 7b
   92 b6 9c a7 42 da 53 25 6b 6b c2 32 1d 29 3a 56 d7 c0 02 21 90 a6 3e
   31 8c 63 18 c6 31 89 4e 95 b5 ef 83 e2 f8 a5 4c 7c 60 a6 39 f1 7b df
   15 b5 ed 7b 98 d7 bd ed 6b da d7 b5 ed 7c 63 18 b5 cc 42 9a e6 be 31
   5b 5c d7 ad 8b 6b 5a f8 ad ae 6a 9a f7 2d ad 6b d6 b6 bd ed 7c 58 f8
   c6 2b 63 9f 05 35 ee 63 1a f8 29 4a 53 56 a6 be 2d 7a d6 d7 ad af 82
   10 a5 21 0a 52 94 a5 29 4a 52 96 d7 c0 c8 51 08 43 21 0b 3a 14 c6 30
   44 32 54 c6 a0 02 20 8a 74 a9 8e 5b 1c 95 31 c7 42 98 53 21 4c 69 4e
   85 29 8f 81 0c 85 31 cf 8a 56 d7 c0 42 21 d2 b6 b9 4d 19 0e 95 35 f1
   6b e0 53 a1 4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22
   99 0a 6b e2 d6 bc 23 21 c4 43 21 2a 61 d2 a6 b9 0b 3a 16 d7 31 8c 11
   0c 93 94 60
4. 02 43 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a e1 10 c8 49 90 a6 21 4a
   63 5f 03 21 4c 7c 62 53 a4 e9 5b 5f 15 31 e7 4a d8 f8 21 4c 79 4e 95
   b1 f1 19 4e 95 35 e8 5b 5f 12 19 0a 63 e0 74 9d 2b 6b 94 d7 bc 44 31
   90 a6 bd ee 32 56 c2 9c a7 42 da 53 25 6b 6b d2 b6 be 21 19 4e 73 a5
   6d 7c 00 22 19 0a 6b de f7 bd ef 7b de f7 c1 cf 8b e2 f8 a5 4d 7b 94
   c6 bd ad 6b da f8 c5 8f 8b df 06 3e 2d 7b 9a f7 c5 8f 83 1f 16 be 2d
   72 14 d7 ad ad 7c 58 f8 31 f0 7c 58 f8 c5 f1 7c 14 d7 bd ef 8a d8 f8
   31 ec 7c 1a f8 29 8f 5b 1f 15 31 f0 7c 1f 18 c6 31 6b de d6 be 0a 63
   e3 15 b5 ef 7c 5f 06 35 4c 63 d8 f8 31 89 53 50 a6 31 4a 6a 98 c6 31
   8c 63 18 c6 be 08 53 0c 85 10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a 00
   22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 81 90 a6 39 f1
   4a da f8 10 42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0 53 a1 4c 7c 4c 85
   31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22 99 0a 6b e2 d6 bc 23 21
   c4 43 21 2a 61 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
5. 02 3d b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 90 23 29 d0 a6 be 25 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d 2b
   6b e0 22 19 0a 32 14 43 1d 0b 6b e2 64 ad 86 42 da d3 a5 6d 7c 10 a6
   39 f0 32 14 c7 94 e9 5b 1f 11 94 e9 53 5c b6 25 6d 7c 0c 85 88 86 42
   98 f8 94 e9 5b 5c a6 bd c6 42 9a f7 be 06 4a da 74 2d a5 29 92 b5 b5
   f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22 19 0a 6b de f7 bd ef 7b de
   f7 c1 cf 8b e2 a6 3e 30 53 10 a6 39 f0 63 e2 d7 b5 ee 6b d2 b6 ad ad
   6b 56 b5 b5 8b 6b 16 d7 bd eb 5b 5a d7 be 2b 6b d6 d5 b5 cd 7b 5f 18
   2d 8f 83 1e b6 ad ac 52 d8 b6 3e 2b 6b dc d7 bd ae 53 5e f5 35 cd 7c
   5a f6 b1 6d 6b e0 a6 35 6a 6b e0 a5 2d 88 52 94 84 2d 0a 52 94 a5 29
   4a 52 da f8 30 c8 51 08 43 21 0b 3a 14 c6 30 44 32 54 c6 a0 02 11 4e
   95 31 cb 63 92 a6 38 e8 53 04 53 21 4c 69 4e 85 29 8f 8a da f8 88 84
   32 56 d7 08 86 42 94 a6 8c 87 4a 9a f8 b5 f0 29 d0 a6 3e 31 39 90 a6
   34 a7 41 d2 a6 bd ae 21 90 a5 29 82 29 90 a6 be 2d 6b c8 64 25 4d 08
   88 74 a9 ae 42 ce 85 b5 cc 63 04 43 24 e5 18 00
6. 02 27 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42 98
   e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 63 a1 6d
   79 92 b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14 c7 3e 03 29 d2 a6
   be 23 29 d2 85 b5 f0 32 14 d1 10 c8 53 1f 13 a5 6d 73 5e e4 29 af 7b
   92 b6 9c a7 42 da 53 25 6b 6b c2 32 1d 29 3a 56 d7 c0 02 21 90 a6 3e
   31 8c 63 18 c6 31 89 4e 95 b5 ef 83 e2 f8 be 29 53 5e e5 31 af 6b 5a
   f6 be 31 63 e2 e6 bd ee 6b df 16 b9 0b 6b 5e e6 bd f1 8c 5e f8 3e 2b
   53 5e f7 c1 f1 5a d6 b5 a9 af 7c 5a e5 35 eb 5b 5a d6 be 0b 6b 58 f8
   a9 8f 8c 14 c7 a9 8e 7c 18 c6 be 0a 52 94 d5 a9 af 8b 5e b6 bd 6d 7b
   e0 84 29 48 42 94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85 31
   8c 11 0c 95 31 a8 00 88 22 9d 2a 63 96 c7 25 4c 71 d0 a6 14 c8 53 1a
   53 a1 4a 63 e2 b6 be 22 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be 2d
   7c 0a 74 29 8f 8c 4e 64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a 64
   29 af 8b 5a f2 19 09 53 42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39
   46 00
7. 02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63 e3
   05 04 65 3a 14 d7 c4 65 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d 2b
   6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98 e7
   c0 c8 53 1e 53 a5 6c 7c 46 53 a5 69 53 5f 03 21 4d 11 0c 85 31 f0 3a
   54 53 94 e9 5b 5c a6 bd c6 42 9a f7 be 06 4a da 74 2d a5 29 92 b5 b5
   f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22 19 0a 6b de f7 bd ef 7b de
   f7 c1 cf 8b e2 f8 a9 af 7b 94 85 b5 ae 6b df 18 c6 2d 62 da d7 bd f0
   63 e0 c7 c6 2f 6b 5e e6 b9 af 7c 62 d7 b9 af 7b dc b6 be 2f 6b e3 07
   b1 f1 7c 18 f6 3d 6c 7c 14 c7 2d ad 6b 5a d6 b1 cf 83 1f 18 bd ee 53
   54 d7 c5 8e 7c 14 c6 31 4a 63 5c a5 b5 f1 7c 5a f8 ad af 8b e0 84 29
   48 42 94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85 31 8c 11 0c
   95 31 a8 00 84 53 a5 4c 72 d8 e4 a9 8e 3a 14 c1 14 c8 53 1a 53 a1 4a
   63 e2 b6 be 22 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be 2d 7c 0a 74
   29 8f 8c 4e 64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a 64 29 af 8b
   5a f0 8c 87 11 0c 84 a9 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
8. 02 31 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3 21
   4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42 98
   e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 da f8 29 aa
   63 88 63 a5 6c 7c 10 a6 39 f1 39 cc 32 9d 2a 6b e2 32 9d 28 5b 5f 03
   21 4c 63 c4 43 21 4c 7c 4e 95 b5 ea 6b dc a6 bd ef 82 56 d3 94 e8 5b
   4a 64 ad 6d 7c 42 32 1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7 bd
   ef 7b de f7 bd f0 73 e2 f8 be 2a 6b de e5 21 6d 6b 9a f7 c6 30 7c 62
   f7 be 0b 63 e0 d7 c6 0f 83 9f 17 b9 4d 7c 58 f8 3e 2a 63 e0 a6 be 31
   8c 62 b6 bd 6d 7a da d7 b9 af 6b 5a d6 b5 ee 6b 9a f7 29 af 7b e3 16
   3e 0d 53 5f 05 b5 ea 63 5f 16 3d 6b 6b 1c c6 31 cc 7c 1a f8 2d af 8a
   da f8 be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21 0c 84 2c
   e8 53 18 c1 10 c9 53 1a 80 08 45 3a 54 c7 2d 8e 4a 98 e3 a1 4c 11 4c
   85 31 a5 3a 14 a6 3e 04 32 14 c7 3e 29 5b 5f 01 10 44 3a 56 d7 29 a3
   19 0e 95 35 f1 6b e0 53 a1 4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2
   19 0a 52 98 22 99 0a 6b e2 d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b
   5c c6 30 44 32 4e 51 80
```

```
9. 02 1f b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8 8c
   a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63 e2
   32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5 6d
   7c 54 c7 9d 2b 63 e0 85 31 cf 80 ca 74 a9 af 88 ca 74 2d 89 5b 5f 12
   19 0a 63 e2 74 ad ae 6b de 22 19 08 53 5e f7 c1 2b 61 4e 53 a1 6d 29
   92 b5 b5 f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22 19 0a 6b de f7 bd
   ef 7b de f7 c1 cf 8b e2 f8 a9 af 7b 94 85 b5 ae 6b df 18 c5 ad 7c 56
   b6 b5 ef 7c 1f 18 be 0b 6b 96 d6 bd ef 8c 56 d7 bd ea 6b df 16 bd ef
   8c 63 05 b5 8f 8a 9a f7 29 af 53 5f 18 29 8e 63 e3 18 31 f1 63 9c e7
   3e 0a 6b 98 c5 35 ee 53 54 d7 c1 6d 7c 56 d7 bd 6d 7b e0 84 29 48 42
   94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85 31 8c 11 0c 95 31
   a8 00 88 22 9d 2a 63 90 b6 38 c8 21 92 a6 a1 4d 3a 14 a6 3e 2b 6b e2
   43 88 84 32 56 d7 08 86 42 94 a6 8c 87 4a 9a f8 b5 f0 29 d0 a6 3e 31
   39 90 a6 34 a7 41 d2 a6 bd ae 21 90 a5 29 82 29 90 a6 be 2d 6b c2 32
   1c 44 32 12 a6 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
10.     02 25 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
   8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
   e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
   6d 7c 54 c7 9d 2b 63 e0 85 31 c3 29 d2 b6 3e 23 29 d2 a6 b9 6c 4a da
   f8 90 c8 53 1f 13 a5 6d 73 5e f1 10 c6 42 9a f7 be 06 4a d8 53 94 e8
   5b 4a 64 ad 6d 7c 42 32 1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7
   bd ef 7b de f7 bd f0 73 e2 f8 a9 8f 8c 60 a6 21 4d 7b e0 f8 a5 6d 7b
   de f7 b5 eb 6a d8 b6 b5 ad 5b 5e a6 b9 4d 73 5e f8 b5 ad 6b 5e f5 b5
   af 7b de f5 ad 6d 6b 5c d7 c1 f1 8b 16 d7 be 2b 63 e0 f8 c5 6a 63 d8
   f8 35 f1 8b 1c e7 3e 0a 63 9e c7 3d 4c 63 9f 06 be 2d 7b d6 d7 be 08
   42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21 0c 84 2c e8 53 18 c1
   10 c9 53 1a 80 08 82 29 d2 a6 39 0b 63 8c 95 30 e8 51 4c 85 31 a5 3a
   14 a6 3e 2b 6b e2 22 10 c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0
   a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a
   f8 b5 af 08 c8 71 10 c8 4a 98 74 a9 ae 42 ce 85 b5 cc 63 04 43 24 e5
   18 00
11.     02 49 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 04 65 3a 14 d7 c4 65 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d
   2b 6b e0 22 19 0a 32 14 43 1d 0b 6b e2 64 ad 86 42 da d3 a5 6d 7c 10
   a6 39 f0 32 14 c7 94 e9 5b 1f 11 94 e9 5a 54 d7 c0 c8 53 44 43 21 4c
   7c 0e 95 14 e5 3a 56 d7 29 af 71 90 a6 bd ee 32 56 c2 9c a7 42 da 53
   25 6b 6b c2 32 1d 29 3a 56 d7 c0 02 21 90 a6 3e 31 8c 63 18 c6 31 89
   4e 95 b5 ef 83 e2 f8 a5 4c 7c 60 a6 39 f1 7b df 18 ad 8f 83 5f 18 c1
   0a 6b df 18 c6 0e 73 1f 15 b5 ed 7a da f5 ad ac 52 da b5 ad ad 7a 9a
   e5 b5 ee 63 5c d7 29 af 7a da b6 b5 af 8a d8 f8 c6 2f 5b 5a d7 35 ca
   6b de f7 c1 cf 63 d4 c6 31 8e 7c 1a f8 c1 6d 5b 5e f5 b5 ef 82 10 a5
   21 0a 52 94 a5 29 4a 52 96 d7 c0 c8 51 08 43 21 0b 3a 14 c6 30 44 32
   54 c6 a0 02 20 8a 74 a9 8e 5b 1c 95 31 c6 21 d0 a6 99 0a 69 4e 85 29
   8f 81 0c 85 31 cf 8a 56 d7 c0 42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0
   53 a1 4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22 99 0a
   6b e2 d6 bc 86 42 54 d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51
   80
12.     02 55 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21
```

```
    46 42 88 63 1d 0b 6b 90 a6 bd e9 5b 5f 14 29 8f 3a 56 c7 94 e9 5b 1f
    11 94 e9 53 5c b6 ad af 80 88 64 29 8e 73 1f 05 21 4d 7b 5e b6 be 06
    42 c4 43 21 4c 79 4e 95 b1 f0 63 e3 03 21 4c 7c 63 03 21 6d 71 0e 82
    9d 2a 6b ce 85 b5 af 89 4e 95 b5 e1 19 0e 94 9d 2b 6b e0 01 10 c8 53
    1f 18 c6 31 8c 63 18 c4 a7 4a da f7 c1 f1 7c 52 a6 3e 31 42 98 e7 c5
    ef 53 5e f7 c1 0a 63 e3 16 3e 31 8c 56 d7 c5 af 8c 14 c7 3e 2a 63 e0
    f8 29 8f 5b 1f 18 c6 30 53 1e b5 ad 6b 5a d6 b5 ad 6d 6b 5a d6 3e 2b
    5a d4 d7 c5 ef 7c 60 f8 c5 8f 8a 9a f7 bd ca 6b 94 a5 35 4d 7c 16 d7
    c5 6d 7b d6 d7 be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21
    0c 84 2c e8 53 18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 6c 72 54 c7 1d
    0a 61 4c 85 31 a5 3a 14 a6 3e 2b 6b e2 22 10 c9 5b 5c 22 19 0a 52 9a
    32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86
    42 94 a6 08 a6 42 9a f8 b5 af 08 c8 71 10 c8 4a 98 74 a9 ae 42 ce 85
    b5 cc 63 04 43 24 e5 18 00
13.       02 19 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42
    98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 da f8 29
    aa 63 88 63 a5 6c 7c 10 a6 39 f1 39 cc 32 9d 2a 6b e2 32 9d 28 5b 5f
    03 21 4c 63 c4 43 21 4c 7c 4e 95 b5 ea 6b dc a6 bd ee 4a da 72 9d 0b
    69 4c 95 ad af 08 c8 74 a4 e9 5b 5f 00 08 86 42 98 f8 c6 31 8c 63 18
    c6 25 3a 56 d7 be 0f 8b e2 95 31 f1 82 98 e7 3e 31 8a 9a f8 be 31 83
    9f 16 bd cd 7b de f7 be 2d 72 14 d5 35 ef 82 9a f5 a9 ae 53 5e f5 b5
    6d 6b 5f 05 b1 f1 7a da d6 b5 ae 63 5e f8 b5 ca 6b de f7 c6 31 83 e2
    d6 bd f1 53 1a a6 29 4c 6b e2 d7 ad 6d 7a da f8 21 0a 52 10 a5 29 4a
    52 94 a5 29 6d 7c 0c 85 10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a 00 22
    08 a7 4a 98 e5 b1 c9 53 1c 74 29 85 32 14 c6 94 e8 52 98 f8 ad af 88
    88 43 25 6d 70 88 64 29 4a 68 c8 74 a9 af 8b 5f 02 9d 0a 63 e3 13 99
    0a 63 4a 74 1d 2a 6b da e2 19 0a 52 98 22 99 0a 6b e2 d6 bc 86 42 54
    d0 88 87 4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
14.       02 3b b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 c3 29 d2 b6 3e 23 29 d2 a6 b9 6c 4a da
    f8 90 c8 53 1f 13 a5 6d 73 5e f1 10 c6 42 9a f7 be 06 4a d8 53 94 e8
    5b 4a 64 ad 6d 7c 52 b6 be 21 19 4e 73 a5 6d 7c 00 22 19 0a 6b de f7
    bd ef 7b de f7 c1 cf 8b e2 a6 3e 31 82 98 85 35 ef 83 d2 b6 3e 31 82
    98 e7 c1 4c 7c 56 d7 ad ab 6a d6 d6 b9 4d 7b de d7 bd af 5a 9a f8 b5
    cb 6b d4 d7 35 ef 7b dc a6 bd 6d 7c 56 b6 3e 2b 63 e3 18 be 0a 63 d8
    f8 ad af 8b 5e d7 c1 6d 63 9f 17 bd cd 7c 18 a6 3e 31 63 e0 e5 29 4a
    5b 1f 15 31 8c 63 1e d6 3d 6c 7c 5e b6 be 2e 42 94 a4 21 68 52 94 a5
    29 4a 52 96 d7 c0 c8 51 08 43 21 0b 3a 14 c6 30 44 32 54 c6 a0 02 20
    8a 74 a9 8e 42 d8 e3 20 86 4a 9a 85 34 e8 52 98 f8 ad af 89 0e 22 10
    c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2 d7 c0 a7 42 98 f8 c4 e6 42 98
    d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 21 90 95 34 22
    21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93 94 60
15.       02 2f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42
    98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 74 2c
    c8 5b 5e b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14 c7 3e 03 29 d2
    a6 be 23 29 d2 85 b5 f0 32 14 d1 10 c8 53 1f 13 a5 6d 73 5e e4 29 af
    7b 92 b6 9c a7 42 da 53 25 6b 6b c2 32 1d 29 3a 56 d7 c4 e9 5b 5f 00
    08 86 42 9a f7 bd ef 7b de f7 bd f0 73 e2 f8 be 29 53 5e e5 35 ed 6b
    de f8 c6 2f 7c 5a f7 bd ef 8b 5e f7 be 09 5b 58 f8 c6 0a 6b df 07 c5
    6b 6b de f7 be 2b 5a da d7 2d ad 6b 5a d6 b5 f1 5a 98 f8 29 8e 63 94
    c7 c1 4c 73 e0 e5 31 f0 6b 98 c6 bd f1 6b 5f 06 3d 8f 5b 1f 17 c5 6d
    7c 10 a5 29 08 5a 14 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85
    31 8c 11 0c 95 31 a8 00 84 53 a5 4c 72 d8 e4 a9 8e 3a 14 c2 99 03 21
    90 a6 34 65 3a 14 a6 3e 02 21 90 a6 39 f1 4a da f8 08 87 4a da e5 34
    64 3a 54 d7 c5 af 81 4e 85 31 f1 32 14 c6 94 e8 3a 54 c7 c5 f1 6b 88
    64 29 4a 60 8a 64 29 af 8b 5a f2 19 09 53 42 22 1d 2a 6b 90 b3 a1 6d
    73 18 c1 10 c9 39 46 00
16.      02 59 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21
    46 42 88 63 a1 6d 79 92 b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14
    c7 94 e9 5b 1f 06 bc 65 3a 16 d7 25 6d 7c 0c 85 88 86 42 98 f8 94 e9
    5b 5c a6 bd c6 42 9a f7 be 06 4a d8 53 94 e8 5b 4a 64 ad 6d 7c 42 32
    1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7 bd ef 7b de f7 bd f0 73
    e2 f8 be 2a 6b de e5 21 6d 6b 9a f7 c6 30 7c 62 f7 be 30 5b 5f 16 be
    31 63 e0 c7 c1 8f 8b de f8 c5 ef 7c 62 b6 3e 0a 53 5f 18 2d af 83 1e
    c7 c5 6c 7c 1a f8 3e 0f 82 98 f6 3e 2f 8b 9a f8 3e 2a 63 e0 a6 ad 4d
    7c 1f 18 c1 6d 6b 1e b6 3e 0d 7c 5c a6 a9 8c 6b e2 c7 3d 4c 63 9f 06
    be 2d 7b d6 d7 be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21
    0c 84 2c e8 53 18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 6c 72 54 c7 18
    87 42 9a 64 29 a5 3a 14 a6 3e 04 32 14 c7 3e 29 5b 5f 01 08 87 4a da
    e5 34 64 3a 54 d7 c5 af 81 4e 85 31 f1 32 14 c6 94 e8 3a 54 c7 c5 f1
    6b 88 64 29 4a 60 8a 64 29 af 8b 5a f0 8c 87 11 0c 84 a9 87 4a 9a e4
    2c e8 5b 5c c6 30 44 32 4e 51 80
17.      02 4b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 35 f0 42 98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21
    46 42 88 63 1d 0b 6b 90 a6 bd e9 5b 5f 14 29 8f 3a 56 c7 94 e9 5b 1f
    11 94 e9 53 5c b6 ad af 80 88 64 29 8e 73 1f 05 21 4d 7b 5e b6 be 06
    42 c4 43 21 4c 79 4e 95 b1 f0 63 e3 03 21 4c 7c 63 03 21 6d 71 0e 82
    9d 2a 6b ce 85 b5 af 89 4e 95 b5 e1 19 0e 94 9d 2b 6b e2 74 ad af 80
    04 43 21 4d 7b de f7 bd ef 7b de f8 39 f1 7c 52 a6 3e 31 42 98 f8 bd
    f1 82 14 c7 c5 2b 6b 5a d6 b5 ad 6b dc a6 bd 6b 5a d6 b5 35 f1 83 e2
    d5 ad 6d 7a 9a f8 b5 ad 62 d8 f5 a9 8c 7c 14 c7 c5 cb 6b 5a e6 bd f1
    8a da f7 b9 8d 72 da f7 bd ea 63 5f 16 39 eb 53 18 f6 3e 2b 6b d6 d7
    c1 0a 52 90 85 a1 4a 52 94 a5 29 4a 5b 5f 03 21 44 21 0c 84 2c e8 53
    18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 6c 72 54 c7 1d 0a 61 4c 85 31
    a5 3a 14 a6 3e 2b 6b e2 22 10 c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2
    d7 c0 a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6
    42 9a f8 b5 af 21 90 95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93
    94 60
18.      02 37 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42
    98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 63 a1
    6d 79 92 b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14 c7 3e 03 29 d2
    a6 be 23 29 d2 85 b5 f0 32 14 d1 10 c8 53 1f 13 a5 6d 73 5e e4 29 af
    7b e0 95 b4 e5 3a 16 d2 99 2b 5b 5f 14 ad af 88 46 53 9c e9 5b 5f 00
    08 86 42 9a f7 bd ef 7b de f7 bd f0 73 e2 f8 a9 8f 8c 14 c4 29 8e 7c
```

```
   52 b6 bd ad 6b 5e f7 bd ef 53 5c b6 b1 6d 73 1a a6 be 2f 82 98 d7 2d
   af 8b da f7 b5 af 82 da f8 be 30 7c 58 f8 35 ef 8a da f5 b5 ef 53 5c
   a6 a9 ae 5b 5e f5 b5 af 8c 58 e7 c5 4c 7b 1c e7 c1 4c 7b 1c f5 31 8f
   63 d6 c7 c5 f1 5b 5f 04 29 4a 42 16 85 29 4a 52 94 a5 29 6d 7c 0c 85
   10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a 00 21 14 e9 53 1c b6 39 2a 63
   8e 85 30 45 32 14 c6 94 e8 52 98 f8 10 c8 53 1c f8 a5 6d 7c 04 22 1d
   2b 6b 94 d1 90 e9 53 5f 16 be 05 3a 14 c7 c4 c8 53 1a 53 a0 e9 53 1f
   17 c5 ae 21 90 a5 29 82 29 90 a6 35 ed 7c 5a f2 19 09 53 42 22 1d 2a
   6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
19.      02 4f b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 a5 6d 7c 46 53
   a1 6d 7c 08 64 28 87 42 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
   e2 32 1d 2a 6b ce 95 b5 f0 11 0c 85 19 0a 21 d0 b6 bc c9 5b 0c 85 b5
   ef 3a 56 d7 c4 c8 53 1e c7 a9 a8 53 1f 03 21 4c 73 e0 d7 c0 65 3a 16
   d7 c4 65 29 92 b6 be 02 21 90 a6 29 8e 41 4c 85 31 e5 3a 56 c7 c5 4c
   7c 60 a6 3e 31 82 16 d7 1d 22 29 d2 a6 bc e8 5b 5a f8 94 e9 5b 5e 11
   90 e9 49 d2 b6 be 27 4a da f8 00 44 32 14 d7 bd ef 7b de f7 bd ef 83
   9f 17 c5 f1 4a 9a f7 a1 4d 7b 5a f7 be 31 8b df 18 21 4c 7c 1a f7 bd
   cb 6b df 16 be 31 5b 5e d7 a9 ae 53 5e d7 c6 0f 5a d6 c7 c1 8d 7c 63
   05 31 f0 7c 56 c7 c5 4d 7b e0 b6 3e 30 63 e3 15 b5 ef 7b d4 d7 2d af
   73 5f 16 b1 f0 73 e0 c7 39 6c 7a d8 f5 ad ac 73 18 c7 c1 af 6b d6 d7
   be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21 0c 84 2c e8 53
   18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 6c 72 54 c7 1d 0a 61 4c 85 31
   a5 3a 14 a6 3e 2b 6b e2 22 18 86 4a da e1 10 c8 52 94 d1 8c 87 4a 9a
   f8 b5 f0 29 d0 a6 3e 31 39 90 a6 34 a7 41 d2 a6 bd ae 21 90 a5 29 82
   29 90 a6 be 2d 6b c2 32 1c 44 32 12 a6 1d 2a 6b 90 b3 a1 6d 73 18 c1
   10 c9 39 46 00
20.      02 55 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
   e3 05 90 23 29 d0 a6 be 25 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d
   2b 6b e0 22 19 0a 32 14 43 1d 0b 6b e2 64 ad 86 42 da d3 a5 6d 7c 10
   a6 39 f0 32 14 c7 94 e9 5b 1f 11 94 e9 53 5c b6 25 6d 7c 0c 85 88 86
   42 98 f8 94 e9 5b 5c a6 bd c6 42 9a f7 be 06 4a d8 53 94 e8 5b 4a 64
   ad 6d 7c 42 32 1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7 bd ef 7b
   de f7 bd f0 73 e2 f8 be 2a 6b de e5 21 6d 6b 9a f7 c6 30 7c 63 05 b1
   6d 6b 1f 15 b5 8f 82 98 f8 b5 eb 6b 5e e5 35 ca 62 9a f8 b5 f0 63 d8
   f8 c5 6a 63 96 c7 c5 ad 73 5e f8 c1 f1 83 5e e5 35 ef 8c 62 b6 3e 2a
   6b e3 05 b1 f1 83 1f 16 b5 ae 6a 98 c6 be 2c 73 d4 c6 39 f0 6b e2 d7
   bd 6d 7b e0 84 29 48 42 94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42
   ce 85 31 8c 11 0c 95 31 a8 00 88 22 9d 2a 63 96 c7 25 4c 71 88 74 29
   a6 42 9a 53 a1 4a 63 e0 43 21 4c 73 e2 95 b5 f0 10 88 74 ad ae 53 46
   43 a5 4d 7c 5a f8 14 e8 53 1f 13 21 4c 69 4e 83 a5 4c 7c 5f 16 b8 86
   42 94 a6 08 a6 42 9a f8 b5 af 08 c8 71 10 c8 4a 98 74 a9 ae 42 ce 85
   b5 cc 63 04 43 24 e5 18 00
21.      02 3f b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42
   98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 63 a1
   6d 79 92 b6 19 0b 6b 4e 95 b5 f1 32 14 c7 b1 f0 32 14 c7 94 e9 5b 1f
   06 b9 6d 78 ca 64 ad af 7c 0c 85 88 86 42 98 f8 94 e9 5b 5c a6 bd c6
   42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 b6 bc 23 21 d2 93 a5 6d 7c 00 22
   19 0a 63 e3 18 c6 31 8c 63 18 94 e9 5b 5e f8 3e 2f 8b e2 95 35 ee 53
   1a f6 b5 af 6b e3 18 b1 f0 63 98 f8 31 0a 63 d8 f8 c1 8f 8b 5e d5 ad
```

```
    ae 6b df 16 ad 8b 6b e2 f7 c6 2a 63 e3 18 3e 31 7a da f7 bd ee 53 5c
    d7 be 31 6a d6 b5 b5 ad 73 5f 05 29 4b 6b e2 a6 a9 8a 53 18 d7 c1 6d
    7c 5a f8 21 4a 63 14 a6 31 8c 63 18 c6 31 8c 63 e2 95 b5 f1 6b e0 64
    28 84 21 90 85 30 44 32 54 d7 b0 02 21 0e 95 b5 e3 29 d2 b6 be 06 31
    90 a5 29 8c 72 16 c7 19 2a 61 d0 a1 14 c8 53 1a 53 a1 4a 63 e2 b6 be
    22 21 0c 95 b5 c2 21 90 a5 29 a3 21 d2 a6 be 2d 7c 0a 74 29 8f 8c 4e
    64 29 8d 29 d0 74 a9 af 6b 88 64 29 4a 60 8a 64 29 af 8b 5a f2 19 09
    53 42 22 1d 2a 6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
22.      02 39 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 04 65 3a 14 d7 c4 65 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d
    2b 6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98
    e7 c0 c8 53 1e 53 a5 6c 7c 46 53 a5 69 53 5f 03 21 4d 11 0c 85 31 f0
    21 d2 74 ad af 29 d0 a6 bd c6 42 9a f7 be 06 4a d8 53 94 e8 5b 4a 64
    ad 6d 7c 42 32 1d 29 3a 56 d7 c4 e9 5b 5f 00 08 86 42 9a f7 bd ef 7b
    de f7 bd f0 73 e2 f8 a9 8f 8c 60 a6 21 4d 7b e0 f8 a5 6d 7b de f7 b9
    4d 7b e3 18 b5 8b 6b 5f 15 ad 4c 73 e0 d7 c1 ce 7c 62 d7 b5 ed 73 5c
    d7 be 2d 6b e2 f8 bd ef 7c 63 18 29 8f 6b 1c c6 39 4c 73 e0 d7 be 2c
    7c 1f 15 ad 4d 7c 58 e7 3e 0f 5a da c7 31 8c 7c 1a f6 bd 6d 7b e0 84
    29 48 42 94 a5 29 4a 52 94 a5 b5 f0 32 14 42 10 c8 42 ce 85 31 8c 11
    0c 95 31 a8 00 88 22 9d 2a 63 90 b6 38 c8 21 92 a6 a1 4d 3a 14 a6 3e
    06 42 98 e7 c5 2b 6b e0 41 08 87 4a da e5 35 f0 3a 54 c7 c6 28 53 44
    53 a5 4d 71 90 a6 31 86 11 0e 85 35 f1 6b 5e 32 99 25 32 54 d0 88 87
    4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
23.      02 4b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 90 23 29 d0 a6 be 25 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d
    2b 6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98
    e7 c0 c8 53 1e 53 a5 6c 7c 46 53 a5 4d 7a 16 d7 c0 c8 58 88 64 29 8f
    81 4e 53 a5 6d 72 9a f7 19 0a 6b de e3 25 6c 29 ca 74 2d a5 32 56 b6
    bc 23 21 d2 93 a5 6d 7c 00 22 19 0a 63 e3 18 c6 31 8c 63 18 94 e9 5b
    5e f8 3e 2f 8a 54 c7 c6 0a 63 9c f8 c5 f1 7c 56 d6 b5 c8 53 54 d7 bd
    ef 7b de f7 29 af 8b 1f 15 b1 f1 82 98 f8 c6 2c 7c 1a e5 b5 ad 7b 9a
    a6 be 0b 63 e2 b6 b9 ae 6b 94 d7 bd ef 53 5c a6 be 2b 6b de f8 ad 6d
    6b 5a e6 bd f1 5a d8 e7 3e 0c 72 d8 f5 31 8c 7b 58 f8 bd 6d 7a da f8
    21 0a 52 10 a5 29 4a 52 94 a5 29 6d 7c 0c 85 10 84 32 10 b3 a1 4c 63
    04 43 25 4c 6a 00 22 08 a7 4a 98 e4 2d 8e 32 54 c3 a1 45 32 14 c6 94
    e8 52 98 f8 ad af 88 88 43 25 6d 70 88 64 29 4a 68 c8 74 a9 af 8b 5f
    02 9d 0a 63 e3 13 99 0a 63 4a 74 1d 2a 6b da e2 19 0a 52 98 22 99 0a
    6b e2 d6 bc 23 21 c4 43 21 2a 61 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93
    94 60
24.      02 37 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 a5 6d 7c 46 53
    a1 6d 7c 08 64 28 87 42 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b ce 95 b5 f0 11 0c 85 19 0a 21 d0 b3 21 6d 7a d8 64 2d
    ad 3a 56 d7 c4 c8 53 1e c7 c0 c8 53 1c f8 0c a7 4a 9a f8 8c a7 42 da
    e4 ad af 81 90 a6 88 86 42 98 f8 94 e9 5b 5c d7 b8 c8 53 5e f7 c1 2b
    61 4e 53 a1 6d 29 92 b5 b5 f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22
    19 0a 6b de f7 bd ef 7b de f7 c1 cf 8b e2 f8 a9 af 7b 96 d7 c1 2b 5b
    16 d6 bd ef 6b 5c d7 b5 ad 73 5e f7 b5 eb 6a da f8 ad 8f 8b de f7 c5
    f1 53 1e c7 c1 8f 82 98 f8 3e 30 63 9f 18 c5 ef 7b df 05 31 cb 6b 58
    f8 bd ef 83 5e f8 31 f1 6b 9a f7 c1 ec 73 9f 05 29 8c 62 9a e5 35 4d
```

```
   72 da f8 ad af 6b d6 d7 be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03
   21 44 21 0c 84 2c e8 53 18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 0b 63
   8c 82 19 2a 6a 14 d3 a1 4a 63 e0 64 29 8e 7c 52 b6 be 02 20 84 43 a5
   6d 72 9a 31 90 e9 53 5f 16 be 05 3a 14 c7 c4 c8 53 1a 53 a0 e9 53 1f
   17 c5 ae 21 90 a5 29 82 29 90 a6 be 2d 6b c2 32 1c 44 32 12 a6 1d 2a
   6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
25.     02 4b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b ce 95 b5 f0 5b 5f 02 19 0a 21 d0 b6 3e 30 11 4e 85 35 f0 42
   98 e0 8c a6 4a d8 f8 8c 87 4a 9a f3 a5 6d 7c 04 43 21 46 42 88 63 1d
   0b 6b 90 a6 bd e9 5b 5f 14 29 8f 3a 56 c7 c0 c8 53 1c f8 0c a7 4a 9a
   f8 8c a7 4a 16 d7 c0 c8 53 44 43 21 4c 79 d2 b6 3e 0c 7c 60 85 31 f1
   8c 10 b6 b8 e8 29 d2 a6 bc e8 5b 5a f8 94 e9 5b 5e 11 90 e9 49 d2 b6
   be 00 11 0c 85 31 f1 8c 63 18 c6 31 8c 4a 74 ad af 7c 1f 17 c5 f1 4a
   9a f7 a1 4d 7b 5a f7 be 31 83 90 a6 3e 2e 6b df 16 bd ed 6b e0 b6 bd
   cd 7c 1c f8 3e 0c 7c 1c a6 3e 0f 83 e2 a6 3e 0a 6a 9a f8 be 0f 8b 5e
   b6 ad ad 7b dc d7 29 af 7c 56 c7 c1 8f 8b 5e b5 ad 6b 6b 5e e5 35 ef
   6b e2 b6 3e 0e 73 e0 c7 2d 8f 53 18 c7 b5 8f 8a da f5 b5 f0 42 94 a4
   21 68 52 94 a5 29 4a 52 96 d7 c0 c8 51 08 43 21 0b 3a 14 c6 30 44 32
   54 c6 a0 02 20 8a 74 a9 8e 5b 1c 95 31 c7 42 98 53 21 4c 69 4e 85 29
   8f 81 0c 85 31 cf 8a 56 d7 c0 42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0
   53 a1 4c 7c 4c 85 31 a5 3a 0e 95 31 f1 7c 5a e2 19 0a 52 98 22 99 0a
   6b e2 d6 bc 23 21 c4 43 21 2a 61 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93
   94 60
26.     02 37 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 62
   c8 11 94 e8 5b 1f 12 99 2a 6b 96 d6 25 6d 7c 08 64 29 8e 7c 1a f8 9d
   2b 6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98
   e7 c0 c8 53 1e 53 a5 6c 7c 46 53 a5 4d 7a 16 d7 c0 c8 58 88 64 29 8f
   81 4e 53 a5 6d 72 9a f7 19 0a 6b de f8 19 2b 61 4e 53 a1 6d 29 92 b5
   b5 f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22 19 0a 6b de f7 bd ef 7b
   de f7 c1 cf 8b e2 f8 a9 af 7b 96 d7 c1 2b 5b 16 d6 bd ee 6b 9a f7 b5
   8b 6b de b5 ad ad 6b 56 b6 be 0f 83 1f 17 c1 6d 6b da f8 c1 6d 7b 9a
   f7 c6 2d 7b e0 a6 39 4b 6b 58 f5 31 f0 7c 14 d7 be 0d 7b de e6 be 0e
   5b 1e b6 3d 8e 63 1c f8 bd 6d 7a da f8 21 0a 52 10 a5 29 4a 52 94 a5
   29 6d 7c 0c 85 10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a 00 22 08 a7 4a
   98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 8a da f8 0c 87 11 08 64 ad
   ae 11 0c 85 29 4d 18 c8 74 a9 af 8b 5f 02 9d 0a 63 e3 05 9c c8 53 1a
   e3 21 4c 63 04 43 a1 4d 7c 5a d7 8c a0 19 4c 92 19 23 29 92 a6 1d 2a
   6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
27.     02 37 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 90 a6 bc e9 5b 5f 04 ad af 81 0c 85 2d 8f 8c 04 53 a1 4d 7c
   10 a6 38 23 29 92 b6 3e 23 21 d2 a6 bc e9 5b 5f 01 10 c6 42 da f8 19
   0a 6a 98 e2 18 e9 5b 1f 04 29 8e 7c 4e 73 0c a7 4a 9a f8 8c a7 4a 16
   d7 c0 c8 53 18 f1 10 c8 53 1f 13 a5 6d 7a 9a f7 29 af 7b e0 95 b4 e5
   3a 16 d2 99 2b 5b 5f 10 8c 87 4a 4e 95 b5 f1 3a 56 d7 c0 02 21 90 a6
   bd ef 7b de f7 bd ef 7c 1c f8 be 2a 63 e3 18 29 88 53 5e f8 3e 0f 8c
   52 b6 bd af 7b de f7 35 ee 53 5e b6 2d 8b 6b 56 d7 c5 6c 7c 5f 17 c1
   af 7c 5f 15 35 ea 6b e0 e7 c1 4d 73 5f 07 c6 30 53 1f 15 b1 f0 7c 63
   18 c6 31 8c 56 b5 a9 ae 6b e0 a6 bd f1 5b 1c f8 3d 6b 6b 1c c6 31 cc
   7c 1a f8 2d af 8a da f8 be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03
   21 44 21 0c 84 2c e8 53 18 c1 10 c9 53 1a 80 08 45 3a 54 c7 2d 8e 4a
```

```
    98 e3 a1 4c 11 4c 85 31 a5 3a 14 a6 3e 2b 6b e2 22 18 86 4a da e1 10
    c8 52 94 d1 8c 87 4a 9a f8 b5 f0 29 d0 a6 3e 31 39 90 a6 34 a7 41 d2
    a6 bd ae 21 90 a5 29 82 29 90 a6 be 2d 6b c2 32 1c 44 32 12 a6 1d 2a
    6b 90 b3 a1 6d 73 18 c1 10 c9 39 46 00
28.     02 35 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 c3 29 d2 b6 3e 0d 78 ca 74 2d ae 4a da
    f8 90 c8 53 1f 14 2d af 3a 56 d7 29 af 78 88 43 21 4d 7b dc 43 25 6d
    29 d0 b6 94 c9 5a da f0 8c 87 4a 4e 95 b5 f1 3a 56 d7 c0 02 21 90 a6
    bd ef 7b de f7 bd ef 7c 1c f8 be 29 53 1f 18 29 8e 7c 5e f7 ad ad 6b
    5a d6 b5 ad 6b 5a f8 b5 f0 42 da d7 b9 af 83 1f 06 3e 31 53 5c b6 bd
    ef 7b 9a f8 39 f1 8c 60 c7 b1 f0 6b df 05 35 f1 7c 60 e7 3e 0d 7c 60
    f5 b1 f1 53 5f 17 bd f1 82 d8 f8 ad 8e 7c 1a e6 31 4a 63 5f 05 b5 f1
    5b 5e f5 b5 ef 82 10 a5 21 0a 52 94 a5 29 4a 52 96 d7 c0 c8 51 08 43
    21 0b 3a 14 c6 30 44 32 54 c6 a0 02 29 d2 a6 38 65 3a 14 c7 b0 c8 5b
    1c 43 25 4c 21 d0 b3 21 4c 69 4e 85 29 8f 81 0c 85 31 cf 8a 56 d7 c0
    42 21 d2 b6 b9 4d 19 0e 95 35 f1 6b e0 53 a1 4c 7c 62 64 29 8d 71 90
    a6 31 86 11 0e 85 35 f1 6b 5e 32 80 65 32 48 64 8c a6 4a 98 74 a9 ae
    42 ce 85 b5 cc 63 04 43 24 e5 18 00
29.     02 4b b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
    21 4a 6b 90 a6 b9 62 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 63
    e3 05 90 23 29 d0 a6 be 25 32 16 d7 25 6d 7c 08 64 29 8e 7c 1a f8 9d
    2b 6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98
    e7 c0 c8 53 1e 53 a5 6c 7c 46 53 a5 69 53 5f 03 21 4d 11 0c 85 31 f0
    3a 54 53 94 e9 5b 5c a6 bd c6 42 9a f7 b8 c9 5b 0a 72 9d 0b 69 4c 95
    ad af 08 c8 74 a4 e9 5b 5f 00 08 86 42 98 f8 c6 31 8c 63 18 c6 25 3a
    56 d7 be 0f 8b e2 95 31 f1 82 98 e7 c5 ef 53 5f 17 c6 30 42 98 f6 39
    f1 8b d6 d6 b5 af 73 5e f7 bd cd 72 9a f8 c6 31 8a d8 b6 b5 eb 6b 16
    c5 b5 ab 5b 5e a6 be 0a 63 e2 b6 3e 0d 7c 60 d7 c5 f0 7b 1f 06 b9 4d
    53 5f 05 35 4d 7c 16 d7 c5 6c 73 e0 c6 a9 8a 53 1a f8 b5 eb 6b d6 d7
    be 08 42 94 84 29 4a 52 94 a5 29 4a 5b 5f 03 21 44 21 0c 84 2c e8 53
    18 c1 10 c9 53 1a 80 08 82 29 d2 a6 39 6c 72 54 c7 1d 0a 61 4c 85 31
    a5 3a 14 a6 3e 2b 6b e2 22 10 c9 5b 5c 22 19 0a 52 9a 32 1d 2a 6b e2
    d7 c0 a7 42 98 f8 c4 e6 42 98 d2 9d 07 4a 9a f6 b8 86 42 94 a6 08 a6
    42 9a f8 b5 af 21 90 95 34 22 21 d2 a6 b9 0b 3a 16 d7 31 8c 11 0c 93
    94 60
30.     02 35 b5 ac 00 88 74 ad af 3a 54 d7 29 a5 32 54 d7 29 af 4a da f8
    8c a6 4a da f8 10 c8 52 d8 f8 c0 45 3a 14 d7 c1 0a 63 82 32 99 2b 63
    e2 32 1d 2a 6b 84 43 21 26 42 98 85 29 8d 7c 0c 85 31 f1 89 4e 93 a5
    6d 7c 54 c7 9d 2b 63 e0 85 31 e5 3a 56 c7 c4 65 3a 54 d7 2d 89 5b 5f
    12 19 0a 63 e2 74 ad ae 53 5e f1 10 c6 42 9a f7 be 06 4a da 74 2d a5
    29 92 b5 b5 f1 08 c8 74 a4 e9 5b 5f 13 a5 6d 7c 00 22 19 0a 6b de f7
    bd ef 7b de f7 c1 cf 8b e2 a6 3e 31 82 98 85 35 ef 83 e0 c7 c1 8f 8a
    56 b5 ad 4c 7c 1f 18 29 8f 5b 1f 15 35 cb 6b de f7 c5 8f 8c 18 e7 c1
    f1 5b 5e b6 bd 6d 5b 56 d6 b5 ae 6b de f7 bd ca 6a 9a f8 2d ad 6b 5a
    f7 be 31 8c 56 b6 bd ef 7b e0 a6 a9 8e 73 e0 c7 b1 eb 63 98 c7 3d 6c
    7c 5f 15 b5 f0 42 94 a4 21 68 52 94 a5 29 4a 52 96 d7 c0 c8 51 08 43
    21 0b 3a 14 c6 30 44 32 54 c6 a0 02 11 4e 95 31 cb 63 92 a6 38 e8 53
    04 53 21 4c 69 4e 85 29 8f 81 0c 85 31 cf 8a 56 d7 c0 44 11 0e 95 b5
    ca 68 c6 43 a5 4d 7c 5a f8 14 e8 53 1f 13 21 4c 69 4e 83 a5 4c 7c 5f
```

```
   16 b8 86 42 94 a6 08 a6 42 9a f8 b5 af 08 c8 71 10 c8 4a 98 74 a9 ae
   42 ce 85 b5 cc 63 04 43 24 e5 18 00
31.      02 39 b5 ac 00 88 74 ad ae 29 d2 a6 b8 65 3a 16 d7 8c a6 4a da e3
   21 4a 6b 98 85 35 e2 21 90 b6 bc a7 4a da f8 a5 6d 7c 04 43 21 0b 62
   c8 11 94 e8 5b 1f 12 99 2a 6b 96 d6 25 6d 7c 08 64 29 8e 7c 1a f8 9d
   2b 6b e0 22 18 c8 59 0c 84 2d af 82 56 c2 19 0b 6b 4e 95 b5 f0 42 98
   e7 c0 c8 53 1e 53 a5 6c 7c 46 53 a5 69 53 5f 03 21 4d 11 0c 85 31 f0
   21 d2 74 ad af 29 d0 a6 bd c6 42 9a f7 b8 c9 5b 4e 85 b4 a5 32 56 11
   90 c9 5a d2 b6 bc e9 5b 5f 00 08 86 42 98 f8 c6 31 8c 63 18 c6 25 3a
   56 d7 be 0f 8b e2 95 31 f1 82 98 e7 3e 31 53 1f 18 c6 08 53 1f 18 b1
   f0 63 e0 f8 c5 ad 5a d8 f8 ad 4c 7c 60 a6 3e 2b 6b d6 d7 b9 ae 5b 5a
   d7 bd ef 62 da f5 35 cb 6b da f7 b5 f1 6b e3 07 ad 8f 83 5f 16 b9 6d
   7c 58 a5 2d ae 53 18 d5 ad 4d 7c 5e d7 ad 6d 7a da f8 21 0a 52 10 a5
   29 4a 52 94 a5 29 6d 7c 0c 85 10 84 32 10 b3 a1 4c 63 04 43 25 4c 6a
   00 22 08 a7 4a 98 e4 2d 8e 32 08 64 a9 a8 53 4e 85 29 8f 8a da f8 0c
   87 11 08 64 ad ae 11 0c 85 29 4d 7c 1e 31 90 c4 3a 54 c7 c6 29 42 9a
   74 a9 ae 32 14 c6 30 44 3a 14 d7 c5 af 6b 9a 32 99 25 32 54 d0 88 87
   4a 9a e4 2c e8 5b 5c c6 30 44 32 4e 51 80
```

Annex D
(normative)

AEHash Parameters

D.1 AEHash B8F16L5 Parameters

D.1.1 Overview

This hash parameter configuration defines a 256-bit hash with 32 braids. The following sections provide the required data for this hash configuration.

D.1.2 T-values

This hash definition uses the following set of 8 ordered T-values (in decimal): `4,15,8,4,8,4,7,12`

D.1.3 Initial Permutation

This hash definition uses the following 0-indexed initial permutation: `5,3,4,7,2,1,0,6`

D.1.4 Initial Matrix

This hash definition uses the following initial matrix:

$$\begin{pmatrix} 14 & 14 & 1 & 4 & 7 & 5 & 10 & 2 \\ 12 & 6 & 7 & 9 & 4 & 5 & 9 & 10 \\ 14 & 9 & 7 & 10 & 0 & 0 & 13 & 0 \\ 15 & 5 & 7 & 8 & 15 & 2 & 5 & 8 \\ 13 & 2 & 14 & 5 & 8 & 10 & 2 & 8 \\ 0 & 9 & 7 & 9 & 2 & 6 & 9 & 15 \\ 12 & 14 & 12 & 8 & 0 & 5 & 7 & 0 \\ 11 & 13 & 5 & 7 & 3 & 9 & 7 & 10 \end{pmatrix}$$

D.1.5 Hash Braids

This hash definition uses the following 32 hash braids:

0. $b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2 b_1 b_2 b_1 b_2$
1. $b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_2 b_3 b_2 b_3 b_1 b_2$
2. $b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_3 b_4 b_3 b_4 b_2 b_3 b_1 b_2$
3. $b_6 b_7 b_5 b_6 b_4 b_5 b_4 b_5 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2$
4. $b_6 b_7 b_5 b_6 b_5 b_6 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2$
5. $b_6 b_7 b_6 b_7 b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2$
6. $b_6 b_7 b_6 b_7 b_5 b_6 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2$
7. $b_6 b_7 b_6 b_7 b_5 b_6 b_4 b_5 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2$
8. $b_6 b_7 b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_3 b_4 b_2 b_3 b_1 b_2$
9. $b_6 b_7 b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_2 b_3 b_1 b_2$
10. $b_6 b_7 b_6 b_7 b_5 b_6 b_4 b_5 b_3 b_4 b_2 b_3 b_1 b_2 b_1 b_2$

11. $b_6b_7b_5b_6b_5b_6b_4b_5b_4b_5b_3b_4b_2b_3b_1b_2$
12. $b_6b_7b_5b_6b_5b_6b_4b_5b_3b_4b_3b_4b_2b_3b_1b_2$
13. $b_6b_7b_5b_6b_5b_6b_4b_5b_3b_4b_2b_3b_2b_3b_1b_2$
14. $b_6b_7b_5b_6b_5b_6b_4b_5b_3b_4b_2b_3b_1b_2b_1b_2$
15. $b_6b_7b_5b_6b_4b_5b_4b_5b_3b_4b_3b_4b_2b_3b_1b_2$
16. $b_6b_7b_5b_6b_4b_5b_4b_5b_3b_4b_2b_3b_2b_3b_1b_2$
17. $b_6b_7b_5b_6b_4b_5b_4b_5b_3b_4b_2b_3b_1b_2b_1b_2$
18. $b_6b_7b_5b_6b_4b_5b_3b_4b_3b_4b_2b_3b_2b_3b_1b_2$
19. $b_6b_7b_5b_6b_4b_5b_3b_4b_3b_4b_2b_3b_1b_2b_1b_2$
20. $b_6b_7b_5b_6b_4b_5b_3b_4b_2b_3b_2b_3b_1b_2b_1b_2$
21. $b_6b_7b_6b_7b_6b_7b_4b_5b_4b_5b_3b_4b_2b_3b_1b_2$
22. $b_6b_7b_6b_7b_6b_7b_4b_5b_3b_4b_3b_4b_2b_3b_1b_2$
23. $b_6b_7b_6b_7b_6b_7b_4b_5b_3b_4b_2b_3b_2b_3b_1b_2$
24. $b_6b_7b_6b_7b_6b_7b_4b_5b_3b_4b_2b_3b_1b_2b_1b_2$
25. $b_6b_7b_5b_6b_5b_6b_5b_6b_3b_4b_3b_4b_2b_3b_1b_2$
26. $b_6b_7b_5b_6b_5b_6b_5b_6b_3b_4b_2b_3b_2b_3b_1b_2$
27. $b_6b_7b_5b_6b_5b_6b_5b_6b_3b_4b_2b_3b_1b_2b_1b_2$
28. $b_6b_7b_5b_6b_4b_5b_4b_5b_4b_5b_2b_3b_2b_3b_1b_2$
29. $b_6b_7b_5b_6b_4b_5b_4b_5b_4b_5b_2b_3b_1b_2b_1b_2$
30. $b_6b_7b_5b_6b_4b_5b_2b_3b_2b_3b_2b_3b_1b_2b_1b_2$
31. $b_6b_7b_6b_7b_5b_6b_3b_4b_3b_4b_2b_3b_1b_2b_1b_2$

Bibliography

[1] A. G. Myasnikov, V. Shpilrain, and A. Ushakov, Group-based Cryptography. Advanced Courses in Mathematics – CRM Barcelona, Birkhauser Basel, 2008.

[2] I. Anshel, M. Anshel, D. Goldfeld, S. Lemieux, “Key Agreement, The Algebraic Eraser^{TM}, and Lightweight Cryptography,” Contemporary Math. 418 (2006), 1–17.

[3] M. R. Magyarik and N. R. Wagner, A Public Key Cryptosystem Based on the Word Problem. Advances in Cryptology—CRYPTO 1984, Lecture Notes in Computer Science 196, pp. 19–36. Springer, Berlin, 1985.

[4] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, New public-key cryptosystem using braid groups. Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science 1880, pp. 166–183. Springer, Berlin, 2000.

[5] Patrick Dehornoy, "A fast method for comparing braids," Advances in Math., 125 (1997) 200-235.

[6] Joan Birman, J.S. Lee, K.H. Ko, “A new approach to the word and conjugacy problems in the braid groups,” Advances in Mathematics, 139, No. 2 (1998), 322- 353.

[7] D. Goldfeld, P.E. Gunnells, “Defeating the Kalka-Teicher-Tsaban Linear Algebra Attack on the Algebraic Eraser”, 2012, http://arxiv.org/abs/1202.0598

[8] I. Anshel, D. Atkins, D. Goldfeld, P. E. Gunnells, “Defeating the Ben-Zvi, Blackburn, and Tsaban Attach on the Algebraic Eraser”, 2016, http://arxiv.org/abs/1601.04780

[9] D. Atkins, D. Goldfeld, “Addressing the Algebraic Eraser Diffie-Hellman Over-the-Air Protocol”, 2016, http://eprint.iacr.org/2016/205

[10] I. Anshel, D. Atkins, D. Goldfeld, P. E. Gunnells, “A class of hash functions based on the Algebraic Eraser^{TM}”, Groups Complexity Cryptology. ISSN 1869-6104, April, 2016.