SPAE & CSPAE algorithms

v1.01, November 6th 2019, Sebastien Riou, Tiempo-secure

Introduction

The main motivation for the development of SPAE has been the protection of firmware and data residing in external flash in the context of embedded systems. This use case requires both high bandwidth and protection against physical attacks. The main constraints is to use AES, so most recent lightweight proposal are out of scope. This constraint comes from several considerations:

- Regulation: only "NIST approved" primitives are accepted by some institutional bodies (not limited to USA).
- Customer acceptance: an SOC is a huge investment, silicon manufacturers are therefore reluctant to implement non standard primitives (and nobody gets fired for selecting an AES based solution).
- Development effort: developing side channel resistant implementation is a huge investment, silicon manufacturers naturally prefer to reuse existing secure AES implementation.

As of 2019, it seems that none of the published AEAD schemes using AES are entirely satisfactory. We reviewed the schemes listed in table Comparison of selected AEAD schemes.

Table 1. Comparison of selected AEAD schemes

Name	Non trivial operations count	Consequence of Nonce reuse
OCB	(2+m+a)Ek + (1+m+a)Inc	ForgeabilityEquality of blocks revealed
GCM	(1+m)Ek + (1+m+a)MultH	ForgeabilityXor of plaintexts revealed
CCM	(2m+a+2)Ek	Xor of plaintexts revealed
EAX	(2m+a+1)Ek	Xor of plaintexts revealed
SIV	(2m+a)Ek	Equality of message revealed

Notation

- m: length of message, in blocks.
- a: length of associated data, in blocks.
- Ek: the encryption with the key k. The slowest of all operations.
- MultH: GF128 multiplication. It is typically faster than Ek.
- Inc: The "inc" operation defined in OCB. It is typically faster than MultH.

OCB is patented so it is unpalatable to silicon manufacturers. GCM footprint and (physical) attack surface is bigger due to the MultH operation. SIV, CCM and EAX are slow and energy hungry as they do two pass over the data. Finally the risks of nonce reuse in GCM and OCB are high for applications where the nonce is generated in the field (IoT, smart cards...).

NOTE

XCBC and XECB have been excluded from the review as they are patented and not well documented. OCB is also patented but the author license it for free to open source projects and the author gives clear diagrams.

We propose a new alternative which leaks slightly more than SIV but has much better performances, we call it SPAE for "Single Pass Authenticated Encryption". A conservative variant dubbed CSPAE is also described in this document.

Table 2. SPAE & CSPAE properties

Name	Non trivial operations count	Consequence of Nonce reuse
SPAE	(1+m+a)Ek	Equality of first blocks revealed
CSPAE	(2+m+a)Ek	Equality of first blocks revealed

NOTE

In SPAE there is a Ek operation which can be precomputed. If this operation is counted like the others then the operation count is (2+m+a)Ek.

The abstract box model

Typically AEAD algorithms are evaluated in a security model where the attacker can submit any combination of nonce, message and associated data as long as the nonce is not reuse for two encryptions. We feel that the general security model for the study of AEAD is putting a lot of constraints on the algorithm which in practice can be avoided. The abstract box model intent to define a security model which takes into account practical aspects to relax the constraints on the algorithm. The abstract box is an object which contains a secret key, an implementation of the AEAD algorithm, and a mechanism to generate nonce internally. Its purpose is to encrypt or decrypt data submitted by the user without revealing the key. As it is abstract, the user cannot attempt any physical measurement or modification on it. The only thing possible is to invoke either the encryption or the decryption processes described below.

AEAD encryption

In encryption, the abstract box takes as input the message and the associated data. It outputs the cipher text, the authentication tag and the nonce. As a result, the attacker cannot choose the nonce. At best it may be able to predict it if, for example, the abstract box use a counter to generate the nonce. If the predictability of the nonce is a problem, an AEAD algorithm may simply state that the nonce has to be unpredictable. If the abstract box is unable to generate a fresh nonce, it outputs nothing (this may happen if, for example, the abstract box use a counter and it has reach its maximum value). The nonce may be output before any input has been fed in, so the attacker can adapt the message and the associated data after observing the nonce chosen by the abstract box.

NOTE

In practice a secure system can easily enforce that it output the nonce only after receiving all inputs. The downside is that the nonce would be considered secret during the whole computation. As a result the nonce would be an additional target for side channel attacks, so it is best to not rely on this approach in the security model.

AEAD decryption

In decryption, the secure box takes as input the nonce, the cipher text, the associated data and the expected tag. If the computed tag match the expected tag, it outputs the message otherwise it outputs nothing.

NOTE

When the mode support padding, the bit length of the plain-text and the associated data are also inputs to the decryption algorithm. Those inputs are in full control of the attacker unless the length are somehow encoded in the cipher-text or the expected tag.

Advantages

This security model allow to create optimized AEAD algorithms because it avoids the attack scenarios on the encryption which involve a chosen nonce. The nonce remains under the attacker's control for decryption but this is less critical as the decryption gives its output only if the expected tag matches the computed tag.

This security model also allows an algorithmic protection against DFA attacks: the encryption can be efficiently protected at algorithmic level by ensuring that each output cannot be repeated. If a given output can be seen only once, the attacker can get a correct output or a faulty output but not a matching pair of correct and faulty output. Similarly the AEAD decryption can be efficiently protected at algorithmic level by ensuring that the tag is correct only if all the outputs subject to DFA are correct.

NOTE

The potential protection of decryption against DFA is not specific to the abstract box model, this is a simple consequence of the definition of AEAD decryption operation. We nevertheless discuss it here as few AEAD algorithm leverage this. For example in GCM, most of Ek steps remains exposed to DFA.

SPAE mode specification

Notation

Table 3. Operators on integers

a << b	right bit shift
a ^ b	bitwise xor
a + b	addition
a - b	subtraction
a * b	multiplication
a / b	integer division, return only the integer part of the result without any rounding

Table 4. Operators used on data blocks

Ex	block encryption with key x
Dx	block decryption with key x
a ^ b	bitwise xor
xor	bitwise xor
HSWAP	swap of the left half with the right half within a block

NOTE

bitwise xor operator first perform zero extension of the smaller operand (zeroes are added as MSBs).

Instantiation parameters

SPAE rely on a block cipher to underpin its security. The block cipher choice determine the following parameter values:

- BLOCKSIZE: the size in bits of a block processed in one call to the block cipher. It is assumed to be a power of two.
- KEYSIZE: the size in bits of the secret key required by the block cipher.

In addition, SPAE has the following parameters:

• TAGSIZE: the size in bits of the tag. It is freely selectable up to BLOCKSIZE.

Requirements on the block cipher

The block cipher shall not have weak keys and shall resist related key attacks in which the related keys are derived solely by exclusive-or on the original key. As of 2019 AES-128, AES-192 and AES-256 fulfills those requirements. Related keys attacks have been published on AES-192 and AES-256 however they involve the tre ound keys rather than the original key, so the SPAE requirement is met.

SPAE encryption

Inputs

- k: the secret key.
- mlen: the message length in bits.
- alen: the associated data length in bits.
- Message: the data to encrypt and authenticate, also called plain-text. It is composed of an integer number **m** of blocks noted P_i with 0<=i<m. m = (mlen + BLOCKSIZE 1) / BLOCKSIZE .
- Associated data: the data to authenticate without encryption. It is composed of an integer number a of blocks noted A_i with 0<=j<a. a = (alen + BLOCKSIZE - 1) / BLOCKSIZE.
- Nonce: a value that is used only once for invoking SPAE encryption.

NOTE

Message and associated data are padded with zeros from **mlen**, **alen**, to the next full block boundary. This shall be enforced by the implementation.

Outputs

- Cipher-text: the encrypted data. It is composed of an integer number m of blocks noted C_i with $0 \le i \le m$.
- Tag: the authentication tag, it is a single block.

Internal variables

- kn = k ^ nonce
- mpadinfo = mlen & ((1<<64)-1)
- apadinfo = mlen & ((1<<64)-1)
- mpadinfo32 = mlen & ((1<<32)-1)
- apadinfo32 = mlen & ((1<<32)-1)
- apadinfo_swap = (apadinfo>>32)^((apadinfo & 0xFFFFFFFF)<<32)
- PADINFO = ((apadinfo_swap ^ mpadinfo)<<64) ^ (apadinfo32<<32) ^ mpadinfo32 (bytes in little endian order)

Cipher-text and PT_i and CT_i equations:

- $PT_0 = k \wedge Ek(k)$
- $CT_0 = Ek(k)$
- For i=0 to m-1
 - $\circ C_i = CT_i \wedge Ekn(PT_i \wedge P_i)$
 - $\circ PT_{i+1} = P_i \wedge Ekn(PT_i \wedge P_i)$
 - \circ $CT_{i+1} = CT_i \land PT_i$

Tag equations:

- $AT_0 = 0$
- For j=0 to a-1:

$$\circ AT_{j+1} = Ek(AT_j \wedge A_j)$$

- if m == 0
 - \circ MT = k \wedge ((1 << BLOCKSIZE)-1)
 - \circ IT = MT \wedge AT_a
 - \circ TAG = PT_m \wedge Ekn(IT \wedge PADINFO)
- else
 - \circ MT = HSWAP(CT_m) \wedge PT_m
 - \circ IT = MT \wedge AT_a
 - TAG = CT_m ^ Ekn(IT ^ PADINFO)

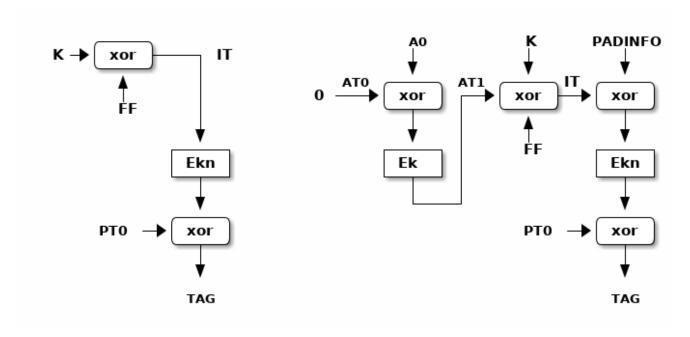


Figure 1. SPAE encryption description, m=0 a=[0,1]

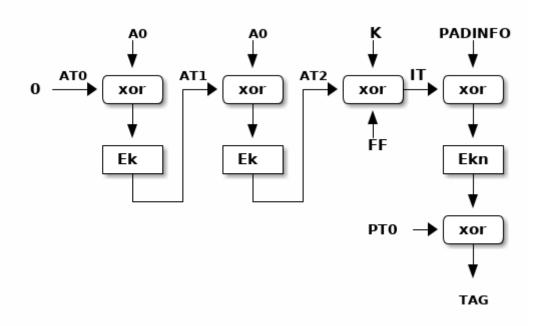


Figure 2. SPAE encryption description, m=0 a=2

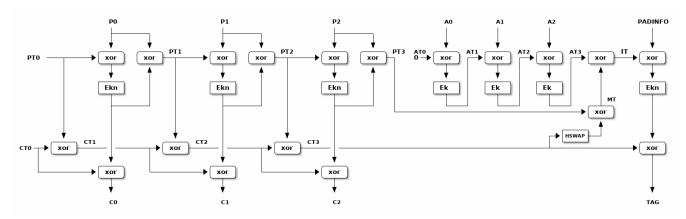


Figure 3. SPAE encryption description, m=3,a=3

SPAE decryption

Inputs

- k: the secret key
- mlen: the output plain text length in bits.
- alen: the associated data length in bits.
- Cipher-text: the encrypted data. It is composed of an integer number ${\bf m}$ of blocks noted C_i with 0 <= i < m.
- ProvidedTag: the authentication tag generated for Message.
- Associated data: the data integrity protected but not encrypted. It is composed of an integer number **a** of blocks noted A_i with 0<=i<a.
- Nonce: the value which was used to generate Message.

NOTE

Associated data is padded with zeros from **alen** to the next full block boundary. This shall be enforced by the implementation.

NOTE

The implementation shall verify that mlen < m * BLOCKSIZE. If it is not the case, the decryption shall be aborted.

Outputs

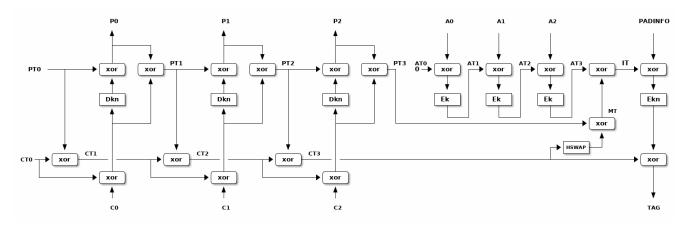
• Plain-text: the decrypted data. It is NOT returned if the integrity check fails, that is if the provided tag is different than the computed tag.

Plain-text and PT_i and CT_i equations:

- $PT_0 = k \wedge Ek(k)$
- $CT_0 = Ek(k)$
- For i=0 to m-1
 - $P_i = PT_i \wedge Dkn(CT_i \wedge C_i)$
 - $PT_{i+1} = P_i \wedge CT_i \wedge C_i$
 - \circ $CT_{i+1} = CT_i \land PT_i$

NOTE

Tag equations are exactly the same as in the encryption



 ${\it Figure~4.~SPAE~decryption~description}$

Design Rational

HSWAP and **PADINFO** encoding

Both the HSWAP operation and the redundant encoding of PADINFO are not really useful from a pure cryptographic point of view. Their purpose is to prevent some DFA on the Dkn operations during decryption. The section on DFA protection gives detailed explanations.

Built in DFA protection

This section discuss the feasibility of a DFA attack on Ek, Ekn and Dkn steps within SPAE. A successful DFA involve getting a pair of Ex or Dx outputs, one without fault and one with a faulty result. Crucially the outputs must be obtained from the same input and the same key. In this section we call such outputs "exploitable pair". DFA attacks are relevant to smart card and other highly secure chips. In this context it is assumed that the implementation has the means to enforce nonce uniqueness for encryption.

Encryption

Assuming the nonce is not in the control of the attacker, each AEAD encryption use a different kn so DFA is possible using outputs belonging to the same AEAD encryption. Within an AEAD encryption, the attacker is not able to get two C_i with the same value or to get the tag equal to a C_i . The attacker is not able to achieve this because that would contradict the security proofs.

The final Ekn used to compute TAG is a special case: a kind of advanced DFA is possible on it. Assuming an injected fault result in a low hamming weight error pattern, an attacker can inject a fault on the final E KN and then try to guess the error pattern by submitting variations of the faulty TAG to the decryption. A successful guess will result in a successful decryption while all other guesses will result in Failure.

To conclude, in SPAE encryption, all Ekn computations can be done without DFA countermeasures except the last one.

Decryption

In decryption the nonce is in the control of the attacker, as a result the reasoning used for the encryption does not hold. The SPAE decryption protects Ek, Ekn and Dkn computation nevertheless by leveraging the tag verification.

The tag is computed from all the outputs of Ek, Ekn and Dkn computation, as a result if there is a faulty result the tag will be incorrect and the output will not be provided to the attacker.

This approach has some limitations. The main reason is that unlike cipher text corruptions, fault injected in E can result in an error pattern with a low hamming weight. For example a fault injected on the last round of AES will typically impact only a single byte.

An attacker can leverage this by targeting the final Ekn operation which produce the TAG. If the faulty TAG can be guessed or brute forced, an attacker may simply inject always the same fault and

submit each time a new guess for the TAG. A DFA in which the attacker guess the fault pattern is certainly an "advanced DFA" we nevertheless consider it a likely attack scenario. To avoid such attack, an implementation need to protect the final Ekn step used to compute the tag.

A fault on the first Dkn propagates to the tag via the PT_i and P_i , and, depending on the number of blocks, via the CT_i . Propagation via the CT_i depends on the number of blocks because the error cancels out every two blocks: The error would be in CT_2 but would disappear in CT_3 since it is also present in PT_2 . At this point it will still propagate further via PT_2 to P_2 and then PT_3 .

This error cancellation phenomenon is the reason for the introduction of the HSWAP operation. Thanks to the HSWAP operation, any error present in both PT_m and CT_m does not cancels out and propagates to IT. The propagation of DFA errors to IT is crucial: it ensure that the resulting faulty TAG cannot be easily guessed. Since IT goes through a call to Ekn, even if a single bit is corrupted the resulting TAG will be impractical to guess.

Faults injected on the penultimate Dkn operation propagates only via PT_m . On its way to the final TAG, the error pattern is xored with PADINFO. An attacker could attempt to manipulate PADINFO in such a way that it would cancel out the error pattern. We mitigate this by formatting PADINFO in such a way that it is unable to cancel typical fault patterns on the late AES rounds. The bytes 0,5,8 and 13 have been chosen because this pattern is easily generated in software: the shift between 0 and 5 is the same as the shift between 8 and 13. A fault in the sbox 0 in the 8th round of AES-128 could disturb byte 0 and 5, but it would also disturb byte 10 and 15.

To conclude, in SPAE decryption, at most one Ekn computation need DFA countermeasures, all other computations of Ek, Ekn and Dkn do not.

Summary of properties

This is a summary of properties as suggested by NIST.

Security Function

Authenticated Encryption with Associated Data (AEAD).

Error Propagation

As in any valid AEAD scheme, the error propagation is infinite.

Synchronization

Synchronization is optional: If the nonce is transmitted along with each cipher-text, there are no synchronization requirements. If it is not sent the receiver must maintain the corresponding value.

Parallelization

Message processing is sequential, associated data processing is sequential. Both can be performed in parallel.

Keying Material Requirements

A single block-cipher key is required.

Counter/IV/Nonce Requirements

A nonce of at most the block size is required.

Memory Requirements

7 blocks are necessary to maintain the state of a running operation:

- 1. kn
- 2. PT_i
- 3. CT_i
- 4. P_i
- 5. C_i
- 6. AT_i
- 7. provided tag (decryption only)

NOTE

Implementation can reduce this by enforcing a strict order of processing. For example, always process associated data first

Pre-processing Capability

- · Block cipher key scheduling
- Associated data can be pre-processed even before choosing the nonce. The resulting AT_j value can be reused unlimited times.
- PT0 and CT0 can be cached rather than computed every time as they depend only on the secret key.

Message Length Requirements

The plain-text can be of arbitrary length however it must be padded to a multiple of the block size. Associated data must be padded to a multiple of the block size. The padding bits must be 0.

Ciphertext Expansion

The cipher-text expansion consist of:

- Tag (at most 1 block)
- Nonce (at most 1 block)
- · Padding bits if message length is not multiple of block size
- Padding bits if associated data is not multiple of block size

Other Characteristics

- SPAE is an "on-line" algorithm: it is possible to process data blocks as they come with constant memory, without knowing how many blocks will be added. (Note that for decryption, like for any AE scheme, this is not entirely true since the output cannot be sent out as long as the tag verification has not been done).
- It uses only a block cipher and xor, so no dedicated hardware accelerator is required other than the one for underlying block cipher.
- DFA attacks targeting the Ex and Dx computations are mostly prevented at algorithmic level. Only the last Ekn computation need implementation level countermeasures.
- SPAE is not patented.

SPAE Test Vectors

```
AES-128, m=0, a=0
SPAE - encryption
           key
          nonce
aes key
         aes din
           aes dout
         = b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
associated data
       PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
       CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
        aes kev
          aes din
          = b'ca2c3704c3b34cd1738d2fe9ec378589'
aes dout
authentication tag = b'6b52a86d2741165af5ad9b4694d978e7'
          = b'6b52a86d2741165af5ad9b4694d978e7'
out
```

```
AES-128, m=0, a=1
SPAE - encryption
             key
nonce
            aes key
            aes din
            aes dout
            = b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
            associated data
         PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
            aes key
aes din
             aes dout
            = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
          IT = b'ecead8da623868a66d1b4402faef1604'
       PADINFO = b'00000000800000000000000080000000'
aes key
            aes din
            = b'ecead8dae23868a66d1b44027aef1604'
aes dout
            = b'25713d88b0dc782a924b38643776bc61'
authentication tag = b'840fa2e1542e22a1146b8ccb4f98410f'
            = b'840fa2e1542e22a1146b8ccb4f98410f'
out
```

```
AES-128, m=1, a=0
SPAE - encryption
             key
            nonce
aes key
            aes din
aes dout
            = b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
            associated data
         PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
            aes key
aes din
            = b'a17e9f69e4f25a8b8620b4af78eefd6d'
            = b'd2654251abb3069a8e3dbc43a4d00332'
aes dout
         C0 = b'731bdd384f415c11081d08ecdc3efe5d'
         PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
         MT = b'd2654251abb3069b8e3dbc43a4d00331'
          IT = b'd2654251abb3069b8e3dbc43a4d00331'
       aes key
aes din
            = b'52654251abb3069b0e3dbc43a4d00331'
aes dout
            = b'8f11c2f7f934270ebbd7c3033fbbabee'
authentication tag = b'8f11c2f7f934270ebbd7c3033fbbabef'
b'731bdd384f415c11081d08ecdc3efe5d8f11c2f7f934270ebbd7c3033fbbabef'
```

```
AES-128, m=2, a=0
SPAE - encryption
            key
            nonce
aes key
            aes din
              b'a17e9f69e4f25a8b8620b4af78eefd6f'
aes dout
message
associated data
         PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
            aes key
            = b'a17e9f69e4f25a8b8620b4af78eefd6d'
aes din
aes dout
            = b'd2654251abb3069a8e3dbc43a4d00332'
         C0 = b'731bdd384f415c11081d08ecdc3efe5d'
         PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
         aes key
aes din
            = b'd2654251abb3069a8e3dbc43a4d00335'
aes dout
            = b'd454792a75871ce616511d13983f9680'
         C1 = b'd454792a75871ce616511d13983f9681'
         PT2 = b'd454792a75871ce616511d13983f9684'
         CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
          MT = b'5a69c569d1571fd6c4345f42338c901e'
          IT = b'5a69c569d1571fd6c4345f42338c901e'
       aes key
aes din
            = b'5a68c569d1571fd6c4355f42338c901e'
            = b'a55abb0d9931f9042644fed6cc8192da'
aes dout
authentication tag = b'773ff95c3282ff9ea8794295685191ea'
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681773ff95c3282ff9ea879
4295685191ea'
```

```
AES-128, m=3, a=0
SPAE - encryption
              key
            nonce
aes key
            aes din
            b'a17e9f69e4f25a8b8620b4af78eefd6f'
aes dout
message
0000000000005'
associated data
          PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
          CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
            aes key
aes din
            = b'a17e9f69e4f25a8b8620b4af78eefd6d'
aes dout
            = b'd2654251abb3069a8e3dbc43a4d00332'
          C0 = b'731bdd384f415c11081d08ecdc3efe5d'
          PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
          aes key
aes din
            = b'd2654251abb3069a8e3dbc43a4d00335'
aes dout
            = b'd454792a75871ce616511d13983f9680'
          C1 = b'd454792a75871ce616511d13983f9681'
          PT2 = b'd454792a75871ce616511d13983f9684'
          CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
aes key
            = b'd454792a75871ce616511d13983f9681'
aes din
aes dout
            = b'9208722da4ac9c0f09b3c7faccc0899a'
          C2 = b'406d307c0f1f9a95878e7bb968108aaa'
          PT3 = b'9208722da4ac9c0f09b3c7faccc0899f'
          CT3 = b'06313b7bde341a7c986ca1503cef95b4'
          MT = b'0a64d37d984309bb0f82fc8112f493e3'
          IT = b'0a64d37d984309bb0f82fc8112f493e3'
       aes key
aes din
            = b'8a65d37d984309bb8f83fc8112f493e3'
aes dout
            = b'a2e95f43f846acd72787210607507a15'
authentication tag = b'a4d864382672b6abbfeb80563bbfefa1'
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaaa4d864382672b6abbfeb80563bbfefa1'
```

```
AES-128, m=3, a=1
SPAE - encryption
              key
nonce
            aes key
            aes din
             aes dout
               b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
0000000000005'
associated data
            PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
          CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
            aes key
aes din
              b'a17e9f69e4f25a8b8620b4af78eefd6d'
            = b'd2654251abb3069a8e3dbc43a4d00332'
aes dout
          C0 = b'731bdd384f415c11081d08ecdc3efe5d'
          PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
          aes key
aes din
            = b'd2654251abb3069a8e3dbc43a4d00335'
aes dout
            = b'd454792a75871ce616511d13983f9680'
          C1 = b'd454792a75871ce616511d13983f9681'
          PT2 = b'd454792a75871ce616511d13983f9684'
          CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
aes key
            aes din
            = b'd454792a75871ce616511d13983f9681'
aes dout
            = b'9208722da4ac9c0f09b3c7faccc0899a'
          C2 = b'406d307c0f1f9a95878e7bb968108aaa'
          PT3 = b'9208722da4ac9c0f09b3c7faccc0899f'
          CT3 = b'06313b7bde341a7c986ca1503cef95b4'
aes key
            aes din
            aes dout
            = b'131527259dc7975992e4bbfd0510e9fa'
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
          MT = b'0a64d37d984309bb0f82fc8112f493e3'
          IT = b'1971f45805849ee29d66477c17e47a19'
       PADINFO = b'80010000800000008001000080000000'
aes key
            = b'9970f45885849ee21d67477c97e47a19'
aes din
            = b'b4e31315c95fa4fdb8c3a38d0b65b744'
aes dout
authentication tag = b'b2d2286e176bbe8120af02dd378a22f0'
out
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaab2d2286e176bbe8120af02dd378a22f0'
```

19

```
AES-128, m=3, a=2
SPAE - encryption
key
            nonce
            aes key
            aes din
            b'a17e9f69e4f25a8b8620b4af78eefd6f'
aes dout
message
0000000000005'
associated data
PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
aes key
            aes din
            = b'a17e9f69e4f25a8b8620b4af78eefd6d'
aes dout
            = b'd2654251abb3069a8e3dbc43a4d00332'
         C0 = b'731bdd384f415c11081d08ecdc3efe5d'
         PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
         aes key
            aes din
            = b'd2654251abb3069a8e3dbc43a4d00335'
            = b'd454792a75871ce616511d13983f9680'
aes dout
         C1 = b'd454792a75871ce616511d13983f9681'
         PT2 = b'd454792a75871ce616511d13983f9684'
         CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
            aes key
aes din
            = b'd454792a75871ce616511d13983f9681'
aes dout
            = b'9208722da4ac9c0f09b3c7faccc0899a'
         C2 = b'406d307c0f1f9a95878e7bb968108aaa'
         PT3 = b'9208722da4ac9c0f09b3c7faccc0899f'
         CT3 = b'06313b7bde341a7c986ca1503cef95b4'
            aes key
            aes din
aes dout
            = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
aes key
            = b'131527259dc7975992e4bbfd0510e9fd'
aes din
aes dout
            = b'dba2c410fd3d0a66d02984fc6e85d61a'
         AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
          MT = b'0a64d37d984309bb0f82fc8112f493e3'
          IT = b'd1c6176d657e03dddfab787d7c7145f9'
       PADINFO = b'80010000000100008001000000010000'
aes key
            aes din
            = b'51c7176d657f03dd5faa787d7c7045f9'
aes dout
            = b'bcc3af37b2c7a9dc1056a31b1f1cda58'
authentication tag = b'baf2944c6cf3b3a0883a024b23f34fec'
out
```

b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e 7bb968108aaabaf2944c6cf3b3a0883a024b23f34fec'

```
AES-128, m=3, a=3
SPAE - encryption
key
           nonce
aes key
           aes din
           aes dout
            b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
0000000000005'
associated data
000000000008'
         PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
aes key
           aes din
           = b'a17e9f69e4f25a8b8620b4af78eefd6d'
aes dout
           = b'd2654251abb3069a8e3dbc43a4d00332'
         C0 = b'731bdd384f415c11081d08ecdc3efe5d'
         PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
         aes key
aes din
           = b'd2654251abb3069a8e3dbc43a4d00335'
aes dout
           = b'd454792a75871ce616511d13983f9680'
         C1 = b'd454792a75871ce616511d13983f9681'
         PT2 = b'd454792a75871ce616511d13983f9684'
         CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
aes key
           aes din
           = b'd454792a75871ce616511d13983f9681'
aes dout
           = b'9208722da4ac9c0f09b3c7faccc0899a'
         C2 = b'406d307c0f1f9a95878e7bb968108aaa'
         PT3 = b'9208722da4ac9c0f09b3c7faccc0899f'
         CT3 = b'06313b7bde341a7c986ca1503cef95b4'
           aes key
           aes din
aes dout
           = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
           aes key
           = b'131527259dc7975992e4bbfd0510e9fd'
aes din
aes dout
           = b'dba2c410fd3d0a66d02984fc6e85d61a'
         AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
           aes key
aes din
           = b'dba2c410fd3d0a66d02984fc6e85d612'
aes dout
           = b'7152d55728d8c03e547ab64cd21531fa'
```

```
AT3 = b'7152d55728d8c03e547ab64cd21531fa'
           MT = b'0a64d37d984309bb0f82fc8112f493e3'
           IT = b'7b36062ab09bc9855bf84acdc0e1a219'
        PADINFO = b'80010000800100008001000080010000'
aes kev
             aes din
             = b'fb37062a309ac985dbf94acd40e0a219'
               b'6037c861f8510ccf6ba9d479d3afb195'
aes dout
authentication tag = b'6606f31a266516b3f3c57529ef402421'
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaa6606f31a266516b3f3c57529ef402421'
SPAE - decryption
               key
nonce
             aes key
             aes din
             aes dout
                b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681406d307c0f1f9a95878e
7bb968108aaa'
associated data
0000000000008'
          PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
          CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
          C0 = b'731bdd384f415c11081d08ecdc3efe5d'
          PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
          C1 = b'd454792a75871ce616511d13983f9681'
          PT2 = b'd454792a75871ce616511d13983f9684'
          CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
          C2 = b'406d307c0f1f9a95878e7bb968108aaa'
          PT3 = b'9208722da4ac9c0f09b3c7faccc0899f'
          CT3 = b'06313b7bde341a7c986ca1503cef95b4'
aes key
             aes din
             aes dout
             = b'131527259dc7975992e4bbfd0510e9fa'
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
             aes key
aes din
             = b'131527259dc7975992e4bbfd0510e9fd'
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
aes dout
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
aes key
             aes din
             = b'dba2c410fd3d0a66d02984fc6e85d612'
aes dout
             = b'7152d55728d8c03e547ab64cd21531fa'
          AT3 = b'7152d55728d8c03e547ab64cd21531fa'
           MT = b'0a64d37d984309bb0f82fc8112f493e3'
           IT = b'7b36062ab09bc9855bf84acdc0e1a219'
```

```
aes dout
           = b'6037c861f8510ccf6ba9d479d3afb195'
authentication tag = b'6606f31a266516b3f3c57529ef402421'
provided tag
           = b'6606f31a266516b3f3c57529ef402421'
out
000000000005'
AES-128, m=3, a=3 padded
SPAE - encryption
           key
nonce
           aes key
           aes din
           aes dout
           = b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
associated data
PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
         CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
           aes key
aes din
           = b'a17e9f69e4f25a8b8620b4af78eefd6d'
           = b'd2654251abb3069a8e3dbc43a4d00332'
aes dout
         C0 = b'731bdd384f415c11081d08ecdc3efe5d'
         PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
         aes key
           aes din
           = b'd2654251abb3069a8e3dbc43a4d00335'
aes dout
           = b'd454792a75871ce616511d13983f9680'
         C1 = b'd454792a75871ce616511d13983f9681'
         PT2 = b'd454792a75871ce616511d13983f9684'
         CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
aes key
           aes din
           = b'dd54792a75871ce616511d13983f9684'
aes dout
           = b'522a8ed2bf8505bea20b42536e64ddb5'
         C2 = b'804fcc83143603242c36fe10cab4de85'
         PT3 = b'5b2a8ed2bf8505bea20b42536e64ddb5'
         CT3 = b'06313b7bde341a7c986ca1503cef95b4'
           aes key
aes din
           aes dout
           = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
           aes key
aes din
           = b'131527259dc7975992e4bbfd0510e9fd'
```

PADINFO = b'80010000800100008001000080010000'

aes key

aes din

```
aes dout
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
             aes key
             = b'd1a9c410fd3d0a66d02984fc6e85d61a'
aes din
aes dout
             = b'd23963e8cabeaa4a76899b5f5e3ee58d'
          AT3 = b'd23963e8cabeaa4a76899b5f5e3ee58d'
           MT = b'c3462f82836a900aa43a7928b050c7c9'
           IT = b'117f4c6a49d43a40d2b3e277ee6e2244'
        PADINFO = b'08010000100100000801000010010000'
aes key
             aes din
             = b'197e4c6a59d53a40dab2e277fe6f2244'
aes dout
             = b'5a13328eaedb78102a7dd30dde463ab2'
authentication tag = b'5c2209f570ef626cb211725de2a9af06'
out
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681804fcc83143603242c36
fe10cab4de855c2209f570ef626cb211725de2a9af06'
SPAE - decryption
key
             nonce
             aes key
aes din
             aes dout
                b'a17e9f69e4f25a8b8620b4af78eefd6f'
message
b'731bdd384f415c11081d08ecdc3efe5dd454792a75871ce616511d13983f9681804fcc83143603242c36
fe10cab4de85'
associated data
PT0 = b'a17e9f69e4f25a8b8620b4af78eefd6e'
          CT0 = b'a17e9f69e4f25a8b8620b4af78eefd6f'
          C0 = b'731bdd384f415c11081d08ecdc3efe5d'
          PT1 = b'd2654251abb3069a8e3dbc43a4d00331'
          C1 = b'd454792a75871ce616511d13983f9681'
          PT2 = b'd454792a75871ce616511d13983f9684'
          CT2 = b'd2654251abb3069a8e3dbc43a4d00330'
          C2 = b'804fcc83143603242c36fe10cab4de85'
          PT3 = b'5b2a8ed2bf8505bea20b42536e64ddb5'
          CT3 = b'06313b7bde341a7c986ca1503cef95b4'
             aes key
aes din
             = b'131527259dc7975992e4bbfd0510e9fa'
aes dout
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
aes key
             aes din
             = b'131527259dc7975992e4bbfd0510e9fd'
aes dout
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
             aes key
             = b'd1a9c410fd3d0a66d02984fc6e85d61a'
aes din
```

```
aes dout
              = b'd23963e8cabeaa4a76899b5f5e3ee58d'
           AT3 = b'd23963e8cabeaa4a76899b5f5e3ee58d'
            MT = b'c3462f82836a900aa43a7928b050c7c9'
            IT = b'117f4c6a49d43a40d2b3e277ee6e2244'
        PADINFO = b'08010000100100000801000010010000'
aes key
               aes din
               = b'197e4c6a59d53a40dab2e277fe6f2244'
               = b'5a13328eaedb78102a7dd30dde463ab2'
aes dout
authentication tag = b'5c2209f570ef626cb211725de2a9af06'
               = b'5c2209f570ef626cb211725de2a9af06'
provided tag
out
```

```
AES-192, m=0, a=0
SPAE - encryption
          key
          nonce
aes key
          aes din
          aes dout
          = b'8bae4efb70d33a9792eea9be70889d72'
message
associated data
        PT0 = b'8bae4efb70d33a9792eea9be70889d72'
        CT0 = b'8bae4efb70d33a9792eea9be70889d72'
         MT = b'ffffffffffffffffffffffffffffff
         aes key
          = b'ffffffffffffffffffffffffffffffff
aes din
          = b'81e625355dbf8e5934b745f5134cdd04'
aes dout
authentication tag = b'0a486bce2d6cb4cea659ec4b63c44076'
          = b'0a486bce2d6cb4cea659ec4b63c44076'
out
```

AES-192, m=0, a=1 SPAE - encryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes dout AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' MT = b'fffffffffffffffffffffffffffffffff IT = b'df28f07820590df0b287003d2007b208' aes key = b'df28f078a0590df0b287003da007b208' aes din aes dout = b'22abc423ccaf24cdf80e3f4e1c670723' authentication tag = b'a9058ad8bc7c1e5a6ae096f06cef9a51' out = b'a9058ad8bc7c1e5a6ae096f06cef9a51'

AES-192, m=1, a=0 SPAE - encryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message associated data PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' aes key aes din = b'8bae4efb70d33a9792eea9be70889d71' = b'43b1e6a719f20402208e06a6311e5efe' aes dout C0 = b'c81fa85c69213e95b260af184196c38c' PT1 = b'43b1e6a719f20402208e06a6311e5efd' MT = b'43b1e6a719f20402208e06a6311e5efd' IT = b'43b1e6a719f20402208e06a6311e5efd' aes key aes din = b'c3b1e6a719f20402a08e06a6311e5efd' aes dout = b'0e7b08a95aebdfd7ea11db765594c645' authentication tag = b'0e7b08a95aebdfd7ea11db765594c645' b'c81fa85c69213e95b260af184196c38c0e7b08a95aebdfd7ea11db765594c645'

```
AES-192, m=2, a=0
SPAE - encryption
           key
           nonce
aes key
           aes din
           aes dout
           = b'8bae4efb70d33a9792eea9be70889d72'
message
associated data
         PT0 = b'8bae4efb70d33a9792eea9be70889d72'
         CT0 = b'8bae4efb70d33a9792eea9be70889d72'
           aes key
           = b'8bae4efb70d33a9792eea9be70889d71'
aes din
           = b'43b1e6a719f20402208e06a6311e5efe'
aes dout
         C0 = b'c81fa85c69213e95b260af184196c38c'
         PT1 = b'43b1e6a719f20402208e06a6311e5efd'
         aes key
           aes din
           = b'43b1e6a719f20402208e06a6311e5ef9'
aes dout
           = b'0806f24aeb53018549efa92b80282ff2'
         C1 = b'0806f24aeb53018549efa92b80282ff2'
         PT2 = b'0806f24aeb53018549efa92b80282ff6'
         CT2 = b'43b1e6a719f20402208e06a6311e5efd'
         MT = b'2888f4ecda4d5f780a5e4f8c99da2bf4'
         IT = b'2888f4ecda4d5f780a5e4f8c99da2bf4'
      aes key
aes din
           = b'2889f4ecda4d5f780a5f4f8c99da2bf4'
           = b'd99b015ca2300ab2cacc517f5a240fc6'
aes dout
authentication tag = b'9a2ae7fbbbc20eb0ea4257d96b3a513b'
b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff29a2ae7fbbbc20eb0ea42
57d96b3a513b'
```

AES-192, m=3, a=0 SPAE - encryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message 0000000000005' associated data PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' aes key aes din = b'8bae4efb70d33a9792eea9be70889d71' aes dout = b'43b1e6a719f20402208e06a6311e5efe' C0 = b'c81fa85c69213e95b260af184196c38c' PT1 = b'43b1e6a719f20402208e06a6311e5efd' aes key = b'43b1e6a719f20402208e06a6311e5ef9' aes din aes dout = b'0806f24aeb53018549efa92b80282ff2' C1 = b'0806f24aeb53018549efa92b80282ff2' PT2 = b'0806f24aeb53018549efa92b80282ff6' CT2 = b'43b1e6a719f20402208e06a6311e5efd' aes key = b'0806f24aeb53018549efa92b80282ff3' aes din = b'1ad8331e8a627e5ead03a301a5281ef0' aes dout C2 = b'5969d5b993907a5c8d8da5a79436400d' PT3 = b'1ad8331e8a627e5ead03a301a5281ef5' CT3 = b'4bb714edf2a105876961af8db136710b' MT = b'73b99c933b540f55e6b4b7ec57891b72' IT = b'73b99c933b540f55e6b4b7ec57891b72' aes key aes din = b'f3b89c933b540f5566b5b7ec57891b72' aes dout = b'5060df9fddcc11e2963f4f51b1d723de' authentication tag = b'1bd7cb722f6d1465ff5ee0dc00e152d5' b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff25969d5b993907a5c8d8d a5a79436400d1bd7cb722f6d1465ff5ee0dc00e152d5'

```
AES-192, m=3, a=1
SPAE - encryption
              key
            nonce
aes key
            aes din
            aes dout
            = b'8bae4efb70d33a9792eea9be70889d72'
message
0000000000005'
associated data
            PT0 = b'8bae4efb70d33a9792eea9be70889d72'
         CT0 = b'8bae4efb70d33a9792eea9be70889d72'
            aes key
aes din
            = b'8bae4efb70d33a9792eea9be70889d71'
            = b'43b1e6a719f20402208e06a6311e5efe'
aes dout
         C0 = b'c81fa85c69213e95b260af184196c38c'
         PT1 = b'43b1e6a719f20402208e06a6311e5efd'
         aes key
aes din
            = b'43b1e6a719f20402208e06a6311e5ef9'
aes dout
            = b'0806f24aeb53018549efa92b80282ff2'
         C1 = b'0806f24aeb53018549efa92b80282ff2'
         PT2 = b'0806f24aeb53018549efa92b80282ff6'
         CT2 = b'43b1e6a719f20402208e06a6311e5efd'
            aes key
            = b'0806f24aeb53018549efa92b80282ff3'
aes din
aes dout
            = b'1ad8331e8a627e5ead03a301a5281ef0'
         C2 = b'5969d5b993907a5c8d8da5a79436400d'
         PT3 = b'1ad8331e8a627e5ead03a301a5281ef5'
         CT3 = b'4bb714edf2a105876961af8db136710b'
            aes key
aes din
            = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes dout
         AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
          MT = b'73b99c933b540f55e6b4b7ec57891b72'
          IT = b'536e9314e4f2fd5aabcc482e88715685'
       PADINFO = b'80010000800000008001000080000000'
aes key
            = b'd36f931464f2fd5a2bcd482e08715685'
aes din
            = b'84299adf77455a9210dfaf60508b2b5d'
aes dout
authentication tag = b'cf9e8e3285e45f1579be00ede1bd5a56'
out
b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff25969d5b993907a5c8d8d
a5a79436400dcf9e8e3285e45f1579be00ede1bd5a56'
```

30

```
AES-192, m=3, a=2
SPAE - encryption
           key
           nonce
           aes key
aes din
          = b'8bae4efb70d33a9792eea9be70889d72'
aes dout
message
0000000000005'
associated data
PT0 = b'8bae4efb70d33a9792eea9be70889d72'
         CT0 = b'8bae4efb70d33a9792eea9be70889d72'
aes key
           aes din
           = b'8bae4efb70d33a9792eea9be70889d71'
aes dout
           = b'43b1e6a719f20402208e06a6311e5efe'
         C0 = b'c81fa85c69213e95b260af184196c38c'
         PT1 = b'43b1e6a719f20402208e06a6311e5efd'
         aes key
           aes din
           = b'43b1e6a719f20402208e06a6311e5ef9'
           = b'0806f24aeb53018549efa92b80282ff2'
aes dout
         C1 = b'0806f24aeb53018549efa92b80282ff2'
         PT2 = b'0806f24aeb53018549efa92b80282ff6'
         CT2 = b'43b1e6a719f20402208e06a6311e5efd'
           aes key
aes din
           = b'0806f24aeb53018549efa92b80282ff3'
aes dout
           = b'1ad8331e8a627e5ead03a301a5281ef0'
         C2 = b'5969d5b993907a5c8d8da5a79436400d'
         PT3 = b'1ad8331e8a627e5ead03a301a5281ef5'
         CT3 = b'4bb714edf2a105876961af8db136710b'
           aes key
aes din
           aes dout
           = b'20d70f87dfa6f20f4d78ffc2dff84df7'
         AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes key
           aes din
           = b'20d70f87dfa6f20f4d78ffc2dff84df0'
aes dout
           = b'a212cc453888b0dc36e74edd09d91d9a'
         AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
         MT = b'73b99c933b540f55e6b4b7ec57891b72'
         IT = b'd1ab50d603dcbf89d053f9315e5006e8'
      PADINFO = b'80010000000100008001000000010000'
aes key
           aes din
           = b'51aa50d603ddbf895052f9315e5106e8'
aes dout
           = b'21e9cb744da2f1d3e005894d76be0bcf'
authentication tag = b'6a5edf99bf03f454896426c0c7887ac4'
out
```

b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff25969d5b993907a5c8d8d a5a79436400d6a5edf99bf03f454896426c0c7887ac4'

```
AES-192, m=3, a=3
SPAE - encryption
key
           nonce
aes key
          aes din
          aes dout
          = b'8bae4efb70d33a9792eea9be70889d72'
message
0000000000005'
associated data
000000000008'
        PT0 = b'8bae4efb70d33a9792eea9be70889d72'
        CT0 = b'8bae4efb70d33a9792eea9be70889d72'
aes key
          aes din
          = b'8bae4efb70d33a9792eea9be70889d71'
aes dout
          = b'43b1e6a719f20402208e06a6311e5efe'
        C0 = b'c81fa85c69213e95b260af184196c38c'
        PT1 = b'43b1e6a719f20402208e06a6311e5efd'
        aes key
aes din
          = b'43b1e6a719f20402208e06a6311e5ef9'
aes dout
          = b'0806f24aeb53018549efa92b80282ff2'
        C1 = b'0806f24aeb53018549efa92b80282ff2'
        PT2 = b'0806f24aeb53018549efa92b80282ff6'
        CT2 = b'43b1e6a719f20402208e06a6311e5efd'
aes key
          aes din
          = b'0806f24aeb53018549efa92b80282ff3'
aes dout
          = b'1ad8331e8a627e5ead03a301a5281ef0'
        C2 = b'5969d5b993907a5c8d8da5a79436400d'
        PT3 = b'1ad8331e8a627e5ead03a301a5281ef5'
        CT3 = b'4bb714edf2a105876961af8db136710b'
           aes key
aes din
           = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes dout
        AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
          aes key
           = b'20d70f87dfa6f20f4d78ffc2dff84df0'
aes din
           = b'a212cc453888b0dc36e74edd09d91d9a'
aes dout
        AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
          aes key
aes din
           = b'a212cc453888b0dc36e74edd09d91d92'
aes dout
           = b'efde49ca7eb12fb659c11a2a62e5eee3'
```

AT3 = b'efde49ca7eb12fb659c11a2a62e5eee3' MT = b'73b99c933b540f55e6b4b7ec57891b72' IT = b'9c67d55945e520e3bf75adc6356cf591' PADINFO = b'80010000800100008001000080010000' aes kev aes din = b'1c66d559c5e420e33f74adc6b56df591' = b'3676b2623fbb2b79cd1d4604046aecfb' aes dout authentication tag = b'7dc1a68fcd1a2efea47ce989b55c9df0' b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff25969d5b993907a5c8d8d a5a79436400d7dc1a68fcd1a2efea47ce989b55c9df0' SPAE - decryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff25969d5b993907a5c8d8d a5a79436400d' associated data 0000000000008' PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' C0 = b'c81fa85c69213e95b260af184196c38c' PT1 = b'43b1e6a719f20402208e06a6311e5efd' C1 = b'0806f24aeb53018549efa92b80282ff2' PT2 = b'0806f24aeb53018549efa92b80282ff6' CT2 = b'43b1e6a719f20402208e06a6311e5efd' C2 = b'5969d5b993907a5c8d8da5a79436400d' PT3 = b'1ad8331e8a627e5ead03a301a5281ef5' CT3 = b'4bb714edf2a105876961af8db136710b' aes key aes din aes dout = b'20d70f87dfa6f20f4d78ffc2dff84df7' AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df0' aes dout = b'a212cc453888b0dc36e74edd09d91d9a' AT2 = b'a212cc453888b0dc36e74edd09d91d9a' aes key aes din = b'a212cc453888b0dc36e74edd09d91d92' aes dout = b'efde49ca7eb12fb659c11a2a62e5eee3' AT3 = b'efde49ca7eb12fb659c11a2a62e5eee3' MT = b'73b99c933b540f55e6b4b7ec57891b72'IT = b'9c67d55945e520e3bf75adc6356cf591'

= b'1c66d559c5e420e33f74adc6b56df591' aes din = b'3676b2623fbb2b79cd1d4604046aecfb' aes dout authentication tag = b'7dc1a68fcd1a2efea47ce989b55c9df0' provided tag = b'7dc1a68fcd1a2efea47ce989b55c9df0' out 000000000005' AES-192, m=3, a=3 padded SPAE - encryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message associated data PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' aes key aes din = b'8bae4efb70d33a9792eea9be70889d71' = b'43b1e6a719f20402208e06a6311e5efe' aes dout C0 = b'c81fa85c69213e95b260af184196c38c' PT1 = b'43b1e6a719f20402208e06a6311e5efd' aes key = b'43b1e6a719f20402208e06a6311e5ef9' aes din aes dout = b'0806f24aeb53018549efa92b80282ff2' C1 = b'0806f24aeb53018549efa92b80282ff2' PT2 = b'0806f24aeb53018549efa92b80282ff6' CT2 = b'43b1e6a719f20402208e06a6311e5efd' aes key = b'0106f24aeb53018549efa92b80282ff6' aes din aes dout = b'e6a9d9722a02ee9e9ec758f4b80e73e8' C2 = b'a5183fd533f0ea9cbe495e5289102d15' PT3 = b'efa9d9722a02ee9e9ec758f4b80e73e8' CT3 = b'4bb714edf2a105876961af8db136710b' aes key aes din aes dout = b'20d70f87dfa6f20f4d78ffc2dff84df7' AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df0'

PADINFO = b'80010000800100008001000080010000'

aes key

aes dout = b'a212cc453888b0dc36e74edd09d91d9a' AT2 = b'a212cc453888b0dc36e74edd09d91d9a' aes key = b'a819cc453888b0dc36e74edd09d91d9a' aes din aes dout = b'cb0393bf8cfef645c4ce3af131c85cf1' AT3 = b'cb0393bf8cfef645c4ce3af131c85cf1' MT = b'86c876ff9b349f95d5704c194aaf766f' IT = b'4dcbe54017ca69d011be76e87b672a9e' PADINFO = b'08010000100100000801000010010000' aes key aes din = b'45cae54007cb69d019bf76e86b662a9e' aes dout = b'93ae047bd784e6c5e026f0e9134f68b7' authentication tag = b'd81910962525e34289475f64a27919bc' out b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff2a5183fd533f0ea9cbe49 5e5289102d15d81910962525e34289475f64a27919bc' SPAE - decryption key nonce aes key aes din aes dout = b'8bae4efb70d33a9792eea9be70889d72' message b'c81fa85c69213e95b260af184196c38c0806f24aeb53018549efa92b80282ff2a5183fd533f0ea9cbe49 5e5289102d15' associated data PT0 = b'8bae4efb70d33a9792eea9be70889d72' CT0 = b'8bae4efb70d33a9792eea9be70889d72' C0 = b'c81fa85c69213e95b260af184196c38c' PT1 = b'43b1e6a719f20402208e06a6311e5efd' C1 = b'0806f24aeb53018549efa92b80282ff2' PT2 = b'0806f24aeb53018549efa92b80282ff6' CT2 = b'43b1e6a719f20402208e06a6311e5efd' C2 = b'a5183fd533f0ea9cbe495e5289102d15' PT3 = b'efa9d9722a02ee9e9ec758f4b80e73e8' CT3 = b'4bb714edf2a105876961af8db136710b' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes dout AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df0' aes dout = b'a212cc453888b0dc36e74edd09d91d9a' AT2 = b'a212cc453888b0dc36e74edd09d91d9a' aes key = b'a819cc453888b0dc36e74edd09d91d9a' aes din

```
aes dout
       = b'cb0393bf8cfef645c4ce3af131c85cf1'
           AT3 = b'cb0393bf8cfef645c4ce3af131c85cf1'
           MT = b'86c876ff9b349f95d5704c194aaf766f'
           IT = b'4dcbe54017ca69d011be76e87b672a9e'
        PADINFO = b'08010000100100000801000010010000'
aes key
              = b'45cae54007cb69d019bf76e86b662a9e'
aes din
              = b'93ae047bd784e6c5e026f0e9134f68b7'
aes dout
authentication tag = b'd81910962525e34289475f64a27919bc'
provided tag
              = b'd81910962525e34289475f64a27919bc'
out
```

```
AES-256, m=0, a=0
SPAE - encryption
key
nonce
         aes key
aes din
aes dout
         = b'6b6cfe160a6263631b292f879eeff926'
message
associated data
       PT0 = b'6b6cfe160a6263631b292f879eeff926'
       CT0 = b'6b6cfe160a6263631b292f879eeff926'
        MT = b'ffffffffffffffffffffffffffffffffff
        aes kev
aes din
aes dout
         = b'e53add77473dca2d3345e4165de2a1ca'
authentication tag = b'8e5623614d5fa94e286ccb91c30d58ec'
out
         = b'8e5623614d5fa94e286ccb91c30d58ec'
```

```
AES-256, m=0, a=1
SPAE - encryption
nonce
          aes kev
aes din
          aes dout
          = b'6b6cfe160a6263631b292f879eeff926'
message
PT0 = b'6b6cfe160a6263631b292f879eeff926'
        CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
aes din
aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
        AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
         MT = b'ffffffffffffffffffffffffffffffffff
         IT = b'e2f44cbccf195856cb7d73c0fbb491b3'
      PADINFO = b'00000000800000000000000080000000'
aes key
aes din
          = b'e2f44cbc4f195856cb7d73c07bb491b3'
aes dout = b'206bd8f81b1a05a2a27303a01eab7831'
authentication tag = b'4b0726ee117866c1b95a2c2780448117'
          = b'4b0726ee117866c1b95a2c2780448117'
out
```

```
AES-256, m=1, a=0
SPAE - encryption
nonce
aes kev
aes din
      aes dout
         = b'6b6cfe160a6263631b292f879eeff926'
         message
associated data =
        PT0 = b'6b6cfe160a6263631b292f879eeff926'
        CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
= b'6b6cfe160a6263631b292f879eeff925'
aes din
         = b'afbae5830ff16b339e032164622fc3cb'
aes dout
        C0 = b'c4d61b9505930850852a0ee3fcc03aed'
        PT1 = b'afbae5830ff16b339e032164622fc3c8'
        MT = b'afbae5830ff16b339e032164622fc3c8'
         II = b'afbae5830ff16b339e032164622fc3c8'
      aes key
aes din
          = b'2fbae5830ff16b331e032164622fc3c8'
aes dout
         = b'416e6e055451336a5cd61e387242963a'
authentication tag = b'416e6e055451336a5cd61e387242963a'
b'c4d61b9505930850852a0ee3fcc03aed416e6e055451336a5cd61e387242963a'
```

```
AES-256, m=2, a=0
SPAE - encryption
nonce
           aes kev
aes din
          aes dout
          = b'6b6cfe160a6263631b292f879eeff926'
message
associated data
        PT0 = b'6b6cfe160a6263631b292f879eeff926'
        CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
= b'6b6cfe160a6263631b292f879eeff925'
aes din
aes dout
           = b'afbae5830ff16b339e032164622fc3cb'
        C0 = b'c4d61b9505930850852a0ee3fcc03aed'
        PT1 = b'afbae5830ff16b339e032164622fc3c8'
        aes key
aes din
           = b'afbae5830ff16b339e032164622fc3cc'
          = b'3f1133bcd8b8299843e3d6f35c69ac59'
aes dout
        C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
        PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
        CT2 = b'afbae5830ff16b339e032164622fc3c8'
         MT = b'a11212d8ba97ea50ec5933705398c76e'
         IT = b'a11212d8ba97ea50ec5933705398c76e'
      aes key
aes din
       = b'a11312d8ba97ea50ec5833705398c76e'
aes dout
          = b'08d9bb037d1577588fbc5e9a4e1d8fff'
authentication tag = b'a7635e8072e41c6b11bf7ffe2c324c37'
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac59a7635e8072e41c6b11bf
7ffe2c324c37'
```

```
AES-256, m=3, a=0
SPAE - encryption
nonce
aes kev
aes din
      aes dout
          = b'6b6cfe160a6263631b292f879eeff926'
message
0000000000005'
associated data
         PT0 = b'6b6cfe160a6263631b292f879eeff926'
         CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
aes din
           = b'6b6cfe160a6263631b292f879eeff925'
aes dout
           = b'afbae5830ff16b339e032164622fc3cb'
         C0 = b'c4d61b9505930850852a0ee3fcc03aed'
         PT1 = b'afbae5830ff16b339e032164622fc3c8'
         aes key
aes din
           = b'afbae5830ff16b339e032164622fc3cc'
aes dout
           = b'3f1133bcd8b8299843e3d6f35c69ac59'
         C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
         PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
         CT2 = b'afbae5830ff16b339e032164622fc3c8'
aes key
aes din
           = b'3f1133bcd8b8299843e3d6f35c69ac58'
aes dout
           = b'3957a49c7a8134d97c24c3b9456c1a9a'
         C2 = b'96ed411f75705feae227e2dd2743d952'
         PT3 = b'3957a49c7a8134d97c24c3b9456c1a9f'
         CT3 = b'90abd63fd74942abdde0f7973e466f95'
         MT = b'e4b7530b44c75b4cec8f158692255834'
         IT = b'e4b7530b44c75b4cec8f158692255834'
      aes kev
aes din
        = b'64b6530b44c75b4c6c8e158692255834'
          = b'14a92c31c2d8097bb0c304108d99d9f9'
aes dout
authentication tag = b'8402fa0e15914bd06d23f387b3dfb66c'
out
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac5996ed411f75705feae227
e2dd2743d9528402fa0e15914bd06d23f387b3dfb66c'
```

```
AES-256, m=3, a=1
SPAE - encryption
nonce
aes kev
aes din
          aes dout
          = b'6b6cfe160a6263631b292f879eeff926'
message
0000000000005'
PT0 = b'6b6cfe160a6263631b292f879eeff926'
        CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
aes din
          = b'6b6cfe160a6263631b292f879eeff925'
aes dout
          = b'afbae5830ff16b339e032164622fc3cb'
        C0 = b'c4d61b9505930850852a0ee3fcc03aed'
        PT1 = b'afbae5830ff16b339e032164622fc3c8'
        aes key
aes din
          = b'afbae5830ff16b339e032164622fc3cc'
aes dout
          = b'3f1133bcd8b8299843e3d6f35c69ac59'
        C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
        PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
        CT2 = b'afbae5830ff16b339e032164622fc3c8'
aes key
aes din
          = b'3f1133bcd8b8299843e3d6f35c69ac58'
aes dout
          = b'3957a49c7a8134d97c24c3b9456c1a9a'
        C2 = b'96ed411f75705feae227e2dd2743d952'
        PT3 = b'3957a49c7a8134d97c24c3b9456c1a9f'
        CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes kev
aes din
          aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
        AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
        MT = b'e4b7530b44c75b4cec8f158692255834'
        IT = b'f9bce0487421fce5d80d99b9966e3678'
      PADINFO = b'80010000800000008001000080000000'
aes key
= b'79bde048f421fce5580c99b9166e3678'
aes din
```

```
authentication tag = b'805906fcd91ba05d0d1533c5fa4fedfb'
out
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac5996ed411f75705feae227
e2dd2743d952805906fcd91ba05d0d1533c5fa4fedfb'
AES-256, m=3, a=2
SPAE - encryption
key
nonce
aes key
aes din
aes dout
         = b'6b6cfe160a6263631b292f879eeff926'
message
000000000005'
associated data
PT0 = b'6b6cfe160a6263631b292f879eeff926'
        CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
= b'6b6cfe160a6263631b292f879eeff925'
aes din
          = b'afbae5830ff16b339e032164622fc3cb'
aes dout
        C0 = b'c4d61b9505930850852a0ee3fcc03aed'
        PT1 = b'afbae5830ff16b339e032164622fc3c8'
        aes key
aes din
          = b'afbae5830ff16b339e032164622fc3cc'
aes dout
          = b'3f1133bcd8b8299843e3d6f35c69ac59'
        C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
        PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
        CT2 = b'afbae5830ff16b339e032164622fc3c8'
aes kev
aes din
          = b'3f1133bcd8b8299843e3d6f35c69ac58'
aes dout
          = b'3957a49c7a8134d97c24c3b9456c1a9a'
        C2 = b'96ed411f75705feae227e2dd2743d952'
        PT3 = b'3957a49c7a8134d97c24c3b9456c1a9f'
        CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes key
aes din
          aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
```

= b'10f2d0c30e52e2f6d0f5c452c409826e'

aes dout

aes dout = b'7063c6b5464200d250052782e699945a' AT2 = b'7063c6b5464200d250052782e699945a' MT = b'e4b7530b44c75b4cec8f158692255834' IT = b'94d495be02855b9ebc8a320474bccc6e' PADINFO = b'80010000000100008001000000010000' aes kev = b'14d595be02845b9e3c8b320474bdcc6e' aes din = b'a3811d2250abedf0cd5a64cca0e4fc7f' aes dout authentication tag = b'332acb1d87e2af5b10ba935b9ea293ea' out b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac5996ed411f75705feae227 e2dd2743d952332acb1d87e2af5b10ba935b9ea293ea' AES-256, m=3, a=3 SPAE - encryption nonce aes kev aes din aes dout = b'6b6cfe160a6263631b292f879eeff926' message 0000000000005' associated data 000000000008' PT0 = b'6b6cfe160a6263631b292f879eeff926' CT0 = b'6b6cfe160a6263631b292f879eeff926' aes kev aes din = b'6b6cfe160a6263631b292f879eeff925' aes dout = b'afbae5830ff16b339e032164622fc3cb' C0 = b'c4d61b9505930850852a0ee3fcc03aed' PT1 = b'afbae5830ff16b339e032164622fc3c8' aes key aes din = b'afbae5830ff16b339e032164622fc3cc' aes dout = b'3f1133bcd8b8299843e3d6f35c69ac59' C1 = b'3f1133bcd8b8299843e3d6f35c69ac59' PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'

AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'

= b'1d0bb34330e6a7a934828c3f044b6e4b'

aes key

aes din

```
CT2 = b'afbae5830ff16b339e032164622fc3c8'
aes key
aes din
            = b'3f1133bcd8b8299843e3d6f35c69ac58'
aes dout
            = b'3957a49c7a8134d97c24c3b9456c1a9a'
         C2 = b'96ed411f75705feae227e2dd2743d952'
         PT3 = b'3957a49c7a8134d97c24c3b9456c1a9f'
         CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes key
aes din
            aes dout
            = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
aes din
            = b'1d0bb34330e6a7a934828c3f044b6e4b'
aes dout
            = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7063c6b5464200d250052782e6999452'
aes dout
            = b'2fa5cb037e60bc50a204a5a6a43a240e'
         AT3 = b'2fa5cb037e60bc50a204a5a6a43a240e'
          MT = b'e4b7530b44c75b4cec8f158692255834'
          IT = b'cb1298083aa7e71c4e8bb020361f7c3a'
       PADTNFO = b'80010000800100008001000080010000'
aes key
aes din
      = b'4b139808baa6e71cce8ab020b61e7c3a'
aes dout
           = b'dfaea2022be859c74a25a52bb394996f'
authentication tag = b'4f05743dfca11b6c97c552bc8dd2f6fa'
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac5996ed411f75705feae227
e2dd2743d9524f05743dfca11b6c97c552bc8dd2f6fa'
SPAE - decryption
kev
nonce
            aes key
aes din
            aes dout
            = b'6b6cfe160a6263631b292f879eeff926'
message
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac5996ed411f75705feae227
e2dd2743d952'
associated data
000000000008'
         PT0 = b'6b6cfe160a6263631b292f879eeff926'
         CT0 = b'6b6cfe160a6263631b292f879eeff926'
```

```
C0 = b'c4d61b9505930850852a0ee3fcc03aed'
          PT1 = b'afbae5830ff16b339e032164622fc3c8'
          C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
          PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
          CT2 = b'afbae5830ff16b339e032164622fc3c8'
          C2 = b'96ed411f75705feae227e2dd2743d952'
          PT3 = b'3957a49c7a8134d97c24c3b9456c1a9f'
          CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes key
aes din
            aes dout
            = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
= b'1d0bb34330e6a7a934828c3f044b6e4b'
aes din
aes dout
            = b'7063c6b5464200d250052782e699945a'
          AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7063c6b5464200d250052782e6999452'
aes dout
            = b'2fa5cb037e60bc50a204a5a6a43a240e'
          AT3 = b'2fa5cb037e60bc50a204a5a6a43a240e'
          MT = b'e4b7530b44c75b4cec8f158692255834'
          IT = b'cb1298083aa7e71c4e8bb020361f7c3a'
       PADTNFO = b'80010000800100008001000080010000'
aes key
aes din
            = b'4b139808baa6e71cce8ab020b61e7c3a'
aes dout
            = b'dfaea2022be859c74a25a52bb394996f'
authentication tag = b'4f05743dfca11b6c97c552bc8dd2f6fa'
provided tag
            = b'4f05743dfca11b6c97c552bc8dd2f6fa'
out
0000000000005'
AES-256, m=3, a=3 padded
SPAE - encryption
key
```

```
associated data
PT0 = b'6b6cfe160a6263631b292f879eeff926'
         CT0 = b'6b6cfe160a6263631b292f879eeff926'
aes key
aes din
           = b'6b6cfe160a6263631b292f879eeff925'
aes dout
           = b'afbae5830ff16b339e032164622fc3cb'
         C0 = b'c4d61b9505930850852a0ee3fcc03aed'
         PT1 = b'afbae5830ff16b339e032164622fc3c8'
         aes key
\mathsf{h}'
aes din
           = b'afbae5830ff16b339e032164622fc3cc'
aes dout
           = b'3f1133bcd8b8299843e3d6f35c69ac59'
         C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
         PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
         CT2 = b'afbae5830ff16b339e032164622fc3c8'
aes key
aes din
           = b'361133bcd8b8299843e3d6f35c69ac5d'
           = b'56cf704751fd282229490cbe2d802a8c'
aes dout
         C2 = b'f97595c45e0c4311b74a2dda4fafe944'
         PT3 = b'5fcf704751fd282229490cbe2d802a8c'
         CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes key
aes din
           aes dout
           = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
aes din
           = b'1d0bb34330e6a7a934828c3f044b6e4b'
aes dout
           = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
           = b'7a68c6b5464200d250052782e699945a'
aes dout
           = b'60b5faaac58c24e040efa51309f8474f'
         AT3 = b'60b5faaac58c24e040efa51309f8474f'
         MT = b'822f87d06fbb47b7b9e2da81fac96827'
         IT = b'e29a7d7aaa376357f90d7f92f3312f68'
      PADINFO = b'08010000100100000801000010010000'
aes key
aes din
      = b'ea9b7d7aba366357f10c7f92e3302f68'
aes dout
           = b'573c2c5e74902b22efa70244691fb89a'
```

```
authentication tag = b'c797fa61a3d969893247f5d35759d70f'
out
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac59f97595c45e0c4311b74a
2dda4fafe944c797fa61a3d969893247f5d35759d70f'
SPAE - decryption
key
nonce
aes key
aes din
           = b'6b6cfe160a6263631b292f879eeff926'
aes dout
message
b'c4d61b9505930850852a0ee3fcc03aed3f1133bcd8b8299843e3d6f35c69ac59f97595c45e0c4311b74a
2dda4fafe944'
associated data
PT0 = b'6b6cfe160a6263631b292f879eeff926'
         CT0 = b'6b6cfe160a6263631b292f879eeff926'
         C0 = b'c4d61b9505930850852a0ee3fcc03aed'
         PT1 = b'afbae5830ff16b339e032164622fc3c8'
         C1 = b'3f1133bcd8b8299843e3d6f35c69ac59'
         PT2 = b'3f1133bcd8b8299843e3d6f35c69ac5d'
         CT2 = b'afbae5830ff16b339e032164622fc3c8'
         C2 = b'f97595c45e0c4311b74a2dda4fafe944'
         PT3 = b'5fcf704751fd282229490cbe2d802a8c'
         CT3 = b'90abd63fd74942abdde0f7973e466f95'
aes key
            =
aes din
            = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes dout
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes kev
aes din
            = b'1d0bb34330e6a7a934828c3f044b6e4b'
            = b'7063c6b5464200d250052782e699945a'
aes dout
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7a68c6b5464200d250052782e699945a'
aes dout
            = b'60b5faaac58c24e040efa51309f8474f'
         AT3 = b'60b5faaac58c24e040efa51309f8474f'
          MT = b'822f87d06fbb47b7b9e2da81fac96827'
          IT = b'e29a7d7aaa376357f90d7f92f3312f68'
       PADINFO = b'08010000100100000801000010010000'
aes key
```

Conservative variant: CSPAE

In SPAE the key used for the block cipher calls is the result of the xor between the secret key and the nonce. This allows to mix the nonce with every block at minimal cost however this is unusual, all major mode of operations use the secret key directly. Due to this novel aspect, SPAE may be considered an experimental proposition rather than a drop in replacement in real world applications. This section describes a more conservative variant dubbed CSPAE. The differences are minimal so implementers may support both without significant overhead.

NOTE

When the nonce are null, CSPAE is equivalent to SPAE.

Differences with SPAE

kn equation

In CSPAE, the block cipher is always using the secret key directly. The nonce is injected in PT0 instead.

kn = k

CTO and PTO

In CSPAE, CTO and PTO are values which depends on the nonce, as a result they cannot be precomputed anymore.

 $CT0 = Ek(nonce \wedge k)$

 $PT0 = nonce \wedge k \wedge Ek(nonce \wedge k)$

Built in DFA protection

CSPAE has the same level of DFA protection as SPAE. This section discuss the feasibility of a DFA attack on Ek, Ekn and Dkn steps within CSPAE.

Encryption

Assuming the nonce is not in the control of the attacker, C_i are unique to each computation. It follows that the C_i can't be used for a DFA since the attacker cannot get any exploitable pair.

The final Ekn must be protected for the same reason as in SPAE.

To conclude, in CSPAE encryption, all Ek and Ekn computations can be done without DFA countermeasures except the last one.

Decryption

When m > 0, the argumentation is exactly the same as SPAE. When m = 0, DFA is not possible for the simple reason that there is no output.

To conclude, in CSPAE decryption, all Ek and Ekn computations can be done without DFA countermeasures except the last one.

CSPAE Test Vectors

```
AES-128, m=0, a=0
CSPAE - encryption
           key
         nonce
aes key
         aes din
           aes dout
         = b'd0017f493d6d576c9ea7d5683209ff18'
message
associated data
       PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
       CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
        aes kev
          aes din
          = b'dbed0d38f8bea1f0b67ee1b20af95397'
aes dout
authentication tag = b'0bec7271c5d3f69c28d934da38f0ac8c'
          = b'0bec7271c5d3f69c28d934da38f0ac8c'
out
```

```
AES-128, m=0, a=1
CSPAE - encryption
              key
nonce
            aes key
            aes din
            aes dout
            = b'd0017f493d6d576c9ea7d5683209ff18'
message
            associated data
         PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
         CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
            aes key
aes din
            aes dout
            = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
          IT = b'ecead8da623868a66d1b4402faef1604'
       PADINFO = b'00000000800000000000000080000000'
aes key
            aes din
            = b'ecead8dae23868a66d1b44027aef1604'
aes dout
            = b'a46174d4bbea6b8e073dbc40df933e49'
authentication tag = b'74600b9d86873ce2999a6928ed9ac152'
            = b'74600b9d86873ce2999a6928ed9ac152'
out
```

```
AES-128, m=1, a=0
CSPAE - encryption
             key
            nonce
aes key
           aes din
aes dout
           = b'd0017f493d6d576c9ea7d5683209ff18'
message
            associated data
         PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
         CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
            aes key
aes din
           = b'd0017f493d6d576c9ea7d5683209ff18'
            = b'7f07f972c337e1984ed92642c9a845f2'
aes dout
         CO = b'af06863bfe5ab6f4d07ef32afba1baea'
         PT1 = b'7f07f972c337e1984ed92642c9a845f1'
         MT = b'7f07f972c337e19b4ed92642c9a845f1'
          IT = b'7f07f972c337e19b4ed92642c9a845f1'
       aes key
aes din
            = b'ff07f972c337e19bced92642c9a845f1'
aes dout
            = b'69d6f0bbc6c56a135b4cb34b6752c7be'
authentication tag = b'69d6f0bbc6c56a135b4cb34b6752c7bd'
b'af06863bfe5ab6f4d07ef32afba1baea69d6f0bbc6c56a135b4cb34b6752c7bd'
```

```
AES-128, m=2, a=0
CSPAE - encryption
              key
            nonce
aes key
            aes din
            b'd0017f493d6d576c9ea7d5683209ff18'
aes dout
message
associated data
          PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
            aes key
            = b'd0017f493d6d576c9ea7d5683209ff18'
aes din
aes dout
            = b'7f07f972c337e1984ed92642c9a845f2'
          CO = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          aes key
aes din
            = b'7f07f972c337e1984ed92642c9a845f5'
aes dout
            = b'ecd2adc6b87c84f9a9f079b100f5bc95'
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
          MT = b'a20b8b8471d4c10bd6f780c3c3c25d09'
          IT = b'a20b8b8471d4c10bd6f780c3c3c25d09'
       aes key
aes din
            = b'a20a8b8471d4c10bd6f680c3c3c25d09'
            = b'a13e552da31911c2b25e0fd1f44ffd4c'
aes dout
authentication tag = b'de39ac5f602ef05afc8729933de7b8be'
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96de39ac5f602ef05afc87
29933de7b8be '
```

```
AES-128, m=3, a=0
CSPAE - encryption
              key
nonce
            aes key
            aes din
            b'd0017f493d6d576c9ea7d5683209ff18'
aes dout
message
0000000000005'
associated data
          PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
            aes key
aes din
            = b'd0017f493d6d576c9ea7d5683209ff18'
            = b'7f07f972c337e1984ed92642c9a845f2'
aes dout
          CO = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          aes key
aes din
            = b'7f07f972c337e1984ed92642c9a845f5'
aes dout
            = b'ecd2adc6b87c84f9a9f079b100f5bc95'
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
aes key
            = b'ecd2adc6b87c84f9a9f079b100f5bc94'
aes din
aes dout
            = b'47d31c0a851c88f4e977f3d42a555111'
          C2 = b'38d4e578462b696ca7aed596e3fd14e3'
          PT3 = b'47d31c0a851c88f4e977f3d42a555114'
          CT3 = b'93d554b47b4b6561e7295ff3c95df963'
          MT = b'a0fa43f94c4171977aa2a760511e3475'
          IT = b'a0fa43f94c4171977aa2a760511e3475'
       aes key
aes din
            = b'20fb43f94c417197faa3a760511e3475'
aes dout
            = b'4e68088b3e38235c4f3d1a4b057fe289'
authentication tag = b'ddbd5c3f4573463da81445b8cc221bea'
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3ddbd5c3f4573463da81445b8cc221bea'
```

```
AES-128, m=3, a=1
CSPAE - encryption
              key
nonce
             aes key
             aes din
             aes dout
               b'd0017f493d6d576c9ea7d5683209ff18'
message
0000000000005'
associated data
             PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
             aes key
aes din
            = b'd0017f493d6d576c9ea7d5683209ff18'
            = b'7f07f972c337e1984ed92642c9a845f2'
aes dout
          CO = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          aes key
aes din
             = b'7f07f972c337e1984ed92642c9a845f5'
aes dout
            = b'ecd2adc6b87c84f9a9f079b100f5bc95'
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
aes key
            aes din
            = b'ecd2adc6b87c84f9a9f079b100f5bc94'
aes dout
             = b'47d31c0a851c88f4e977f3d42a555111'
          C2 = b'38d4e578462b696ca7aed596e3fd14e3'
          PT3 = b'47d31c0a851c88f4e977f3d42a555114'
          CT3 = b'93d554b47b4b6561e7295ff3c95df963'
             aes key
aes din
             aes dout
             = b'131527259dc7975992e4bbfd0510e9fa'
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
          MT = b'a0fa43f94c4171977aa2a760511e3475'
          IT = b'b3ef64dcd186e6cee8461c9d540edd8f'
       PADINFO = b'80010000800000008001000080000000'
aes key
             = b'33ee64dc5186e6ce68471c9dd40edd8f'
aes din
             = b'2c87c6d626a1c1c7a29ed2b459730e7c'
aes dout
authentication tag = b'bf5292625deaa4a645b78d47902ef71f'
out
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3bf5292625deaa4a645b78d47902ef71f'
```

55

```
AES-128, m=3, a=2
CSPAE - encryption
key
            nonce
            aes key
            aes din
            b'd0017f493d6d576c9ea7d5683209ff18'
aes dout
message
0000000000005'
associated data
PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
aes key
            aes din
            = b'd0017f493d6d576c9ea7d5683209ff18'
aes dout
            = b'7f07f972c337e1984ed92642c9a845f2'
           Ρ0
          C0 = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          aes key
            aes din
            = b'7f07f972c337e1984ed92642c9a845f5'
            = b'ecd2adc6b87c84f9a9f079b100f5bc95'
aes dout
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
            aes key
aes din
            = b'ecd2adc6b87c84f9a9f079b100f5bc94'
aes dout
            = b'47d31c0a851c88f4e977f3d42a555111'
          C2 = b'38d4e578462b696ca7aed596e3fd14e3'
          PT3 = b'47d31c0a851c88f4e977f3d42a555114'
          CT3 = b'93d554b47b4b6561e7295ff3c95df963'
            aes key
aes din
            aes dout
            = b'131527259dc7975992e4bbfd0510e9fa'
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
aes key
            = b'131527259dc7975992e4bbfd0510e9fd'
aes din
aes dout
            = b'dba2c410fd3d0a66d02984fc6e85d61a'
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
          MT = b'a0fa43f94c4171977aa2a760511e3475'
          IT = b'7b5887e9b17c7bf1aa8b239c3f9be26f'
       PADINFO = b'80010000000100008001000000010000'
aes key
            aes din
            = b'fb5987e9b17d7bf12a8a239c3f9ae26f'
aes dout
            = b'1b43f37caf9d80e49216e13ca18cd70a'
authentication tag = b'8896a7c8d4d6e585753fbecf68d12e69'
out
```

b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae d596e3fd14e38896a7c8d4d6e585753fbecf68d12e69'

```
AES-128, m=3, a=3
CSPAE - encryption
            key
           nonce
aes key
           aes din
           aes dout
           = b'd0017f493d6d576c9ea7d5683209ff18'
message
0000000000005'
associated data
000000000008'
         PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
         CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
aes key
           aes din
           = b'd0017f493d6d576c9ea7d5683209ff18'
aes dout
           = b'7f07f972c337e1984ed92642c9a845f2'
         CO = b'af06863bfe5ab6f4d07ef32afba1baea'
         PT1 = b'7f07f972c337e1984ed92642c9a845f1'
         aes key
aes din
           = b'7f07f972c337e1984ed92642c9a845f5'
aes dout
           = b'ecd2adc6b87c84f9a9f079b100f5bc95'
         C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
         PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
         CT2 = b'7f07f972c337e1984ed92642c9a845f2'
aes key
           aes din
           = b'ecd2adc6b87c84f9a9f079b100f5bc94'
aes dout
           = b'47d31c0a851c88f4e977f3d42a555111'
         C2 = b'38d4e578462b696ca7aed596e3fd14e3'
         PT3 = b'47d31c0a851c88f4e977f3d42a555114'
         CT3 = b'93d554b47b4b6561e7295ff3c95df963'
           aes key
aes din
           = b'131527259dc7975992e4bbfd0510e9fa'
aes dout
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
           aes key
           = b'131527259dc7975992e4bbfd0510e9fd'
aes din
           = b'dba2c410fd3d0a66d02984fc6e85d61a'
aes dout
         AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
           aes key
aes din
           = b'dba2c410fd3d0a66d02984fc6e85d612'
aes dout
           = b'7152d55728d8c03e547ab64cd21531fa'
```

```
AT3 = b'7152d55728d8c03e547ab64cd21531fa'
           MT = b'a0fa43f94c4171977aa2a760511e3475'
           IT = b'd1a896ae6499b1a92ed8112c830b058f'
        PADINFO = b'80010000800100008001000080010000'
aes key
             aes din
             = b'51a996aee498b1a9aed9112c030a058f'
               b'88f91460c26ad09f448b9880ff2f8fd0'
aes dout
authentication tag = b'1b2c40d4b921b5fea3a2c773367276b3'
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e31b2c40d4b921b5fea3a2c773367276b3'
CSPAE - decryption
               key
nonce
             aes key
             aes din
             aes dout
                b'd0017f493d6d576c9ea7d5683209ff18'
message
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc9638d4e578462b696ca7ae
d596e3fd14e3'
associated data
0000000000008'
          PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
          CO = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
          C2 = b'38d4e578462b696ca7aed596e3fd14e3'
          PT3 = b'47d31c0a851c88f4e977f3d42a555114'
          CT3 = b'93d554b47b4b6561e7295ff3c95df963'
aes key
             aes din
aes dout
             = b'131527259dc7975992e4bbfd0510e9fa'
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
             aes key
aes din
             = b'131527259dc7975992e4bbfd0510e9fd'
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
aes dout
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
aes key
             aes din
             = b'dba2c410fd3d0a66d02984fc6e85d612'
aes dout
             = b'7152d55728d8c03e547ab64cd21531fa'
          AT3 = b'7152d55728d8c03e547ab64cd21531fa'
           MT = b'a0fa43f94c4171977aa2a760511e3475'
           IT = b'd1a896ae6499b1a92ed8112c830b058f'
```

```
aes dout
           = b'88f91460c26ad09f448b9880ff2f8fd0'
authentication tag = b'1b2c40d4b921b5fea3a2c773367276b3'
provided tag
           = b'1b2c40d4b921b5fea3a2c773367276b3'
out
000000000005'
AES-128, m=3, a=3 padded
CSPAE - encryption
           key
nonce
           aes key
           aes din
           aes dout
           = b'd0017f493d6d576c9ea7d5683209ff18'
message
associated data
PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
         CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
           aes key
           = b'd0017f493d6d576c9ea7d5683209ff18'
aes din
           = b'7f07f972c337e1984ed92642c9a845f2'
aes dout
         CO = b'af06863bfe5ab6f4d07ef32afba1baea'
         PT1 = b'7f07f972c337e1984ed92642c9a845f1'
         aes key
           aes din
           = b'7f07f972c337e1984ed92642c9a845f5'
aes dout
           = b'ecd2adc6b87c84f9a9f079b100f5bc95'
         C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
         PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
         CT2 = b'7f07f972c337e1984ed92642c9a845f2'
aes key
           aes din
           = b'e5d2adc6b87c84f9a9f079b100f5bc91'
aes dout
           = b'da47a26436ecc7baaf102ba9605a1c91'
         C2 = b'a5405b16f5db2622e1c90deba9f25963'
         PT3 = b'd347a26436ecc7baaf102ba9605a1c91'
         CT3 = b'93d554b47b4b6561e7295ff3c95df963'
           aes key
aes din
           aes dout
           = b'131527259dc7975992e4bbfd0510e9fa'
         AT1 = b'131527259dc7975992e4bbfd0510e9fa'
           aes key
aes din
           = b'131527259dc7975992e4bbfd0510e9fd'
```

PADINFO = b'80010000800100008001000080010000'

= b'0000000000000000000000000000000001'
= b'51a996aee498b1a9aed9112c030a058f'

aes key

aes din

```
aes dout
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
             aes key
             = b'd1a9c410fd3d0a66d02984fc6e85d61a'
aes din
aes dout
             = b'd23963e8cabeaa4a76899b5f5e3ee58d'
          AT3 = b'd23963e8cabeaa4a76899b5f5e3ee58d'
           MT = b'346efd97ffb13ed93cc57f1d1b1179f0'
           IT = b'e6579e7f350f94934a4ce442452f9c7d'
        PADINFO = b'08010000100100000801000010010000'
aes key
             aes din
             = b'ee569e7f250e9493424de442552e9c7d'
aes dout
             = b'756108597b6c61abc0856698b15d82ba'
authentication tag = b'e6b45ced002704ca27ac396b78007bd9'
out
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96a5405b16f5db2622e1c9
Odeba9f25963e6b45ced002704ca27ac396b78007bd9'
CSPAE - decryption
key
             nonce
             aes key
             aes din
             aes dout
                b'd0017f493d6d576c9ea7d5683209ff18'
message
b'af06863bfe5ab6f4d07ef32afba1baeaecd2adc6b87c84f9a9f079b100f5bc96a5405b16f5db2622e1c9
0deba9f25963'
associated data
PT0 = b'd0017f493d6d576c9ea7d5683209ff1b'
          CT0 = b'd0017f493d6d576c9ea7d5683209ff18'
          CO = b'af06863bfe5ab6f4d07ef32afba1baea'
          PT1 = b'7f07f972c337e1984ed92642c9a845f1'
          C1 = b'ecd2adc6b87c84f9a9f079b100f5bc96'
          PT2 = b'ecd2adc6b87c84f9a9f079b100f5bc91'
          CT2 = b'7f07f972c337e1984ed92642c9a845f2'
          C2 = b'a5405b16f5db2622e1c90deba9f25963'
          PT3 = b'd347a26436ecc7baaf102ba9605a1c91'
          CT3 = b'93d554b47b4b6561e7295ff3c95df963'
             aes key
aes din
             = b'131527259dc7975992e4bbfd0510e9fa'
aes dout
          AT1 = b'131527259dc7975992e4bbfd0510e9fa'
aes key
             aes din
             = b'131527259dc7975992e4bbfd0510e9fd'
aes dout
             = b'dba2c410fd3d0a66d02984fc6e85d61a'
          AT2 = b'dba2c410fd3d0a66d02984fc6e85d61a'
             aes key
             = b'd1a9c410fd3d0a66d02984fc6e85d61a'
aes din
```

```
aes dout
              = b'd23963e8cabeaa4a76899b5f5e3ee58d'
           AT3 = b'd23963e8cabeaa4a76899b5f5e3ee58d'
            MT = b'346efd97ffb13ed93cc57f1d1b1179f0'
            IT = b'e6579e7f350f94934a4ce442452f9c7d'
        PADINFO = b'08010000100100000801000010010000'
aes key
               aes din
               = b'ee569e7f250e9493424de442552e9c7d'
               = b'756108597b6c61abc0856698b15d82ba'
aes dout
authentication tag = b'e6b45ced002704ca27ac396b78007bd9'
               = b'e6b45ced002704ca27ac396b78007bd9'
provided tag
out
```

```
AES-192, m=0, a=0
CSPAE - encryption
          key
          nonce
aes key
          aes din
          aes dout
          = b'dc71a551158e10bd27d2030c806eae28'
message
associated data
        PT0 = b'dc71a551158e10bd27d2030c806eae2a'
        CT0 = b'dc71a551158e10bd27d2030c806eae28'
         MT = b'ffffffffffffffffffffffffffffff
         aes key
          = b'fffffffffffffffffffffffffffffffff
aes din
          = b'66b5ba5bc01294706d7f25a682248c88'
aes dout
authentication tag = b'bac41f0ad59c84cd4aad26aa024a22a2'
          = b'bac41f0ad59c84cd4aad26aa024a22a2'
out
```

AES-192, m=0, a=1 CSPAE - encryption key nonce aes key aes din aes dout = b'dc71a551158e10bd27d2030c806eae28' message PT0 = b'dc71a551158e10bd27d2030c806eae2a' CT0 = b'dc71a551158e10bd27d2030c806eae28' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes dout AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' MT = b'fffffffffffffffffffffffffffffffff IT = b'df28f07820590df0b287003d2007b208' aes key = b'df28f078a0590df0b287003da007b208' aes din aes dout = b'e658aedd4468c1830f3a1bdcdc7a5973' authentication tag = b'3a290b8c51e6d13e28e818d05c14f759' out = b'3a290b8c51e6d13e28e818d05c14f759'

AES-192, m=1, a=0 CSPAE - encryption key nonce aes key aes din aes dout = b'dc71a551158e10bd27d2030c806eae28' message associated data PT0 = b'dc71a551158e10bd27d2030c806eae2a' CT0 = b'dc71a551158e10bd27d2030c806eae28' aes key aes din = b'dc71a551158e10bd27d2030c806eae29' = b'28f49bc54af068d7bf745a06d02c9039' aes dout C0 = b'f4853e945f7e786a98a6590a50423e11' PT1 = b'28f49bc54af068d7bf745a06d02c903a' MT = b'28f49bc54af068d5bf745a06d02c903a' IT = b'28f49bc54af068d5bf745a06d02c903a' aes key aes din = b'a8f49bc54af068d53f745a06d02c903a' aes dout = b'4ac763ff05ca6685ef34d7818e6d9ef1' authentication tag = b'4ac763ff05ca6685ef34d7818e6d9ef3' b'f4853e945f7e786a98a6590a50423e114ac763ff05ca6685ef34d7818e6d9ef3'

```
AES-192, m=2, a=0
CSPAE - encryption
           key
           nonce
aes key
           aes din
           = b'dc71a551158e10bd27d2030c806eae28'
aes dout
message
associated data
         PT0 = b'dc71a551158e10bd27d2030c806eae2a'
         CT0 = b'dc71a551158e10bd27d2030c806eae28'
           aes key
           = b'dc71a551158e10bd27d2030c806eae29'
aes din
           = b'28f49bc54af068d7bf745a06d02c9039'
aes dout
         C0 = b'f4853e945f7e786a98a6590a50423e11'
         PT1 = b'28f49bc54af068d7bf745a06d02c903a'
         aes key
           aes din
           = b'28f49bc54af068d7bf745a06d02c903e'
           = b'84ecb88ceef9228d01ec92ea0e629e6d'
aes dout
         C1 = b'84ecb88ceef9228d01ec92ea0e629e6f'
         PT2 = b'84ecb88ceef9228d01ec92ea0e629e69'
         CT2 = b'28f49bc54af068d7bf745a06d02c9038'
         MT = b'3b98e28a3ed5b2b52918092f4492f6be'
         IT = b'3b98e28a3ed5b2b52918092f4492f6be'
      aes key
aes din
           = b'3b99e28a3ed5b2b52919092f4492f6be'
           = b'388ff82480548c3d9ba0f5faedd81498'
aes dout
authentication tag = b'107b63e1caa4e4ea24d4affc3df484a0'
b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f107b63e1caa4e4ea24d4
affc3df484a0'
```

AES-192, m=3, a=0 CSPAE - encryption key nonce aes key aes din = b'dc71a551158e10bd27d2030c806eae28' aes dout message 0000000000005' associated data PT0 = b'dc71a551158e10bd27d2030c806eae2a' CT0 = b'dc71a551158e10bd27d2030c806eae28' aes key aes din = b'dc71a551158e10bd27d2030c806eae29' = b'28f49bc54af068d7bf745a06d02c9039' aes dout C0 = b'f4853e945f7e786a98a6590a50423e11' PT1 = b'28f49bc54af068d7bf745a06d02c903a' aes key aes din = b'28f49bc54af068d7bf745a06d02c903e' aes dout = b'84ecb88ceef9228d01ec92ea0e629e6d' C1 = b'84ecb88ceef9228d01ec92ea0e629e6f' PT2 = b'84ecb88ceef9228d01ec92ea0e629e69' CT2 = b'28f49bc54af068d7bf745a06d02c9038' aes key = b'84ecb88ceef9228d01ec92ea0e629e6c' aes din = b'6a36ea0044bc5e80d711a892584b8fb7' aes dout C2 = b'42c271c50e4c36576865f29488671f8f' PT3 = b'6a36ea0044bc5e80d711a892584b8fb2' CT3 = b'ac182349a4094a5abe98c8ecde4e0e51' MT = b'd4ae22ec9af250d17b098bdbfc42c5e8' IT = b'd4ae22ec9af250d17b098bdbfc42c5e8' aes key aes din = b'54af22ec9af250d1fb088bdbfc42c5e8' aes dout = b'82e013716823534ef979a74e4b754bda' authentication tag = b'2ef83038cc2a191447e16fa2953b458b' b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f42c271c50e4c36576865 f29488671f8f2ef83038cc2a191447e16fa2953b458b'

```
AES-192, m=3, a=1
CSPAE - encryption
            key
            nonce
aes key
            aes din
            aes dout
            = b'dc71a551158e10bd27d2030c806eae28'
message
0000000000005'
associated data
            PT0 = b'dc71a551158e10bd27d2030c806eae2a'
         CT0 = b'dc71a551158e10bd27d2030c806eae28'
            aes key
aes din
            = b'dc71a551158e10bd27d2030c806eae29'
            = b'28f49bc54af068d7bf745a06d02c9039'
aes dout
         C0 = b'f4853e945f7e786a98a6590a50423e11'
         PT1 = b'28f49bc54af068d7bf745a06d02c903a'
         aes key
aes din
            = b'28f49bc54af068d7bf745a06d02c903e'
aes dout
            = b'84ecb88ceef9228d01ec92ea0e629e6d'
         C1 = b'84ecb88ceef9228d01ec92ea0e629e6f'
         PT2 = b'84ecb88ceef9228d01ec92ea0e629e69'
         CT2 = b'28f49bc54af068d7bf745a06d02c9038'
            aes key
aes din
            = b'84ecb88ceef9228d01ec92ea0e629e6c'
aes dout
            = b'6a36ea0044bc5e80d711a892584b8fb7'
         C2 = b'42c271c50e4c36576865f29488671f8f'
         PT3 = b'6a36ea0044bc5e80d711a892584b8fb2'
         CT3 = b'ac182349a4094a5abe98c8ecde4e0e51'
            aes key
aes din
            = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes dout
         AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
          MT = b'd4ae22ec9af250d17b098bdbfc42c5e8'
          IT = b'f4792d6b4554a2de3671741923ba881f'
       PADINFO = b'80010000800000008001000080000000'
aes key
            = b'74782d6bc554a2deb6707419a3ba881f'
aes din
            = b'16d2bfa8050803e015debb9762b742a9'
aes dout
authentication tag = b'baca9ce1a10149baab46737bbcf94cf8'
out
b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f42c271c50e4c36576865
f29488671f8fbaca9ce1a10149baab46737bbcf94cf8'
```

66

```
AES-192, m=3, a=2
CSPAE - encryption
           key
           nonce
aes key
           aes din
           = b'dc71a551158e10bd27d2030c806eae28'
aes dout
message
0000000000005'
associated data
PT0 = b'dc71a551158e10bd27d2030c806eae2a'
         CT0 = b'dc71a551158e10bd27d2030c806eae28'
aes key
           aes din
           = b'dc71a551158e10bd27d2030c806eae29'
aes dout
           = b'28f49bc54af068d7bf745a06d02c9039'
         C0 = b'f4853e945f7e786a98a6590a50423e11'
         PT1 = b'28f49bc54af068d7bf745a06d02c903a'
         aes key
           aes din
           = b'28f49bc54af068d7bf745a06d02c903e'
           = b'84ecb88ceef9228d01ec92ea0e629e6d'
aes dout
         C1 = b'84ecb88ceef9228d01ec92ea0e629e6f'
         PT2 = b'84ecb88ceef9228d01ec92ea0e629e69'
         CT2 = b'28f49bc54af068d7bf745a06d02c9038'
           aes key
aes din
           = b'84ecb88ceef9228d01ec92ea0e629e6c'
aes dout
           = b'6a36ea0044bc5e80d711a892584b8fb7'
         C2 = b'42c271c50e4c36576865f29488671f8f'
         PT3 = b'6a36ea0044bc5e80d711a892584b8fb2'
         CT3 = b'ac182349a4094a5abe98c8ecde4e0e51'
           aes key
aes din
           aes dout
           = b'20d70f87dfa6f20f4d78ffc2dff84df7'
         AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes key
           aes din
           = b'20d70f87dfa6f20f4d78ffc2dff84df0'
aes dout
           = b'a212cc453888b0dc36e74edd09d91d9a'
         AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
         MT = b'd4ae22ec9af250d17b098bdbfc42c5e8'
         IT = b'76bceea9a27ae00d4deec506f59bd872'
      PADINFO = b'80010000000100008001000000010000'
aes key
           aes din
           = b'f6bdeea9a27be00dcdefc506f59ad872'
aes dout
           = b'745b200c37e2d21ff3591693852d524c'
authentication tag = b'd843034593eb98454dc1de7f5b635c1d'
out
```

```
AES-192, m=3, a=3
CSPAE - encryption
           key
          nonce
aes key
          aes din
          aes dout
          = b'dc71a551158e10bd27d2030c806eae28'
message
0000000000005'
associated data
000000000008'
        PT0 = b'dc71a551158e10bd27d2030c806eae2a'
        CT0 = b'dc71a551158e10bd27d2030c806eae28'
aes key
          aes din
          = b'dc71a551158e10bd27d2030c806eae29'
          = b'28f49bc54af068d7bf745a06d02c9039'
aes dout
        C0 = b'f4853e945f7e786a98a6590a50423e11'
        PT1 = b'28f49bc54af068d7bf745a06d02c903a'
        aes key
aes din
           = b'28f49bc54af068d7bf745a06d02c903e'
aes dout
          = b'84ecb88ceef9228d01ec92ea0e629e6d'
        C1 = b'84ecb88ceef9228d01ec92ea0e629e6f'
        PT2 = b'84ecb88ceef9228d01ec92ea0e629e69'
        CT2 = b'28f49bc54af068d7bf745a06d02c9038'
           aes key
aes din
          = b'84ecb88ceef9228d01ec92ea0e629e6c'
aes dout
          = b'6a36ea0044bc5e80d711a892584b8fb7'
        C2 = b'42c271c50e4c36576865f29488671f8f'
        PT3 = b'6a36ea0044bc5e80d711a892584b8fb2'
        CT3 = b'ac182349a4094a5abe98c8ecde4e0e51'
           aes key
           aes din
           = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes dout
        AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
          aes key
           = b'20d70f87dfa6f20f4d78ffc2dff84df0'
aes din
           = b'a212cc453888b0dc36e74edd09d91d9a'
aes dout
        AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
          aes key
aes din
           = b'a212cc453888b0dc36e74edd09d91d92'
aes dout
           = b'efde49ca7eb12fb659c11a2a62e5eee3'
```

AT3 = b'efde49ca7eb12fb659c11a2a62e5eee3' MT = b'd4ae22ec9af250d17b098bdbfc42c5e8' IT = b'3b706b26e4437f6722c891f19ea72b0b' PADINFO = b'80010000800100008001000080010000' aes key aes din = b'bb716b2664427f67a2c991f11ea62b0b' = b'cac82909122fcc6ae015ad9d527bdf8c' aes dout authentication tag = b'66d00a40b62686305e8d65718c35d1dd' b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f42c271c50e4c36576865 f29488671f8f66d00a40b62686305e8d65718c35d1dd' CSPAE - decryption kev nonce aes key aes din aes dout b'dc71a551158e10bd27d2030c806eae28' message b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f42c271c50e4c36576865 f29488671f8f' associated data 0000000000008' PT0 = b'dc71a551158e10bd27d2030c806eae2a' CT0 = b'dc71a551158e10bd27d2030c806eae28' C0 = b'f4853e945f7e786a98a6590a50423e11' PT1 = b'28f49bc54af068d7bf745a06d02c903a' C1 = b'84ecb88ceef9228d01ec92ea0e629e6f' PT2 = b'84ecb88ceef9228d01ec92ea0e629e69' CT2 = b'28f49bc54af068d7bf745a06d02c9038' C2 = b'42c271c50e4c36576865f29488671f8f'PT3 = b'6a36ea0044bc5e80d711a892584b8fb2' CT3 = b'ac182349a4094a5abe98c8ecde4e0e51' aes key aes din aes dout = b'20d70f87dfa6f20f4d78ffc2dff84df7' AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df0' aes dout = b'a212cc453888b0dc36e74edd09d91d9a' AT2 = b'a212cc453888b0dc36e74edd09d91d9a' aes key aes din = b'a212cc453888b0dc36e74edd09d91d92' aes dout = b'efde49ca7eb12fb659c11a2a62e5eee3' AT3 = b'efde49ca7eb12fb659c11a2a62e5eee3' MT = b'd4ae22ec9af250d17b098bdbfc42c5e8' IT = b'3b706b26e4437f6722c891f19ea72b0b'

aes din = b'bb716b2664427f67a2c991f11ea62b0b' = b'cac82909122fcc6ae015ad9d527bdf8c' aes dout authentication tag = b'66d00a40b62686305e8d65718c35d1dd' provided tag = b'66d00a40b62686305e8d65718c35d1dd' out 000000000005' AES-192, m=3, a=3 padded CSPAE - encryption key nonce aes key aes din aes dout = b'dc71a551158e10bd27d2030c806eae28' message associated data PT0 = b'dc71a551158e10bd27d2030c806eae2a' CT0 = b'dc71a551158e10bd27d2030c806eae28' aes key aes din = b'dc71a551158e10bd27d2030c806eae29' = b'28f49bc54af068d7bf745a06d02c9039' aes dout C0 = b'f4853e945f7e786a98a6590a50423e11' PT1 = b'28f49bc54af068d7bf745a06d02c903a' aes key = b'28f49bc54af068d7bf745a06d02c903e' aes din aes dout = b'84ecb88ceef9228d01ec92ea0e629e6d' C1 = b'84ecb88ceef9228d01ec92ea0e629e6f' PT2 = b'84ecb88ceef9228d01ec92ea0e629e69' CT2 = b'28f49bc54af068d7bf745a06d02c9038' aes key = b'8decb88ceef9228d01ec92ea0e629e69' aes din aes dout = b'275b3ef03ef37a77fc62ec71eb9cd328' C2 = b'0fafa535740312a04316b6773bb04310' PT3 = b'2e5b3ef03ef37a77fc62ec71eb9cd328' CT3 = b'ac182349a4094a5abe98c8ecde4e0e51' aes key aes din aes dout = b'20d70f87dfa6f20f4d78ffc2dff84df7' AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7' aes key aes din = b'20d70f87dfa6f20f4d78ffc2dff84df0'

PADINFO = b'80010000800100008001000080010000'

aes key

```
aes dout
             = b'a212cc453888b0dc36e74edd09d91d9a'
          AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
aes key
             = b'a819cc453888b0dc36e74edd09d91d9a'
aes din
aes dout
             = b'cb0393bf8cfef645c4ce3af131c85cf1'
          AT3 = b'cb0393bf8cfef645c4ce3af131c85cf1'
          MT = b'90c3f61ce0bd7426507acf384f959972'
          IT = b'5bc065a36c43826394b4f5c97e5dc583'
       PADINFO = b'08010000100100000801000010010000'
aes key
             aes din
             = b'53c165a37c4282639cb5f5c96e5cc583'
             = b'109df4b49fd46f8e32b876177297f1ca'
aes dout
authentication tag = b'bc85d7fd3bdd25d48c20befbacd9ff9b'
out
b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f0fafa535740312a04316
b6773bb04310bc85d7fd3bdd25d48c20befbacd9ff9b'
CSPAE - decryption
key
             nonce
             aes key
aes din
             aes dout
            = b'dc71a551158e10bd27d2030c806eae28'
message
b'f4853e945f7e786a98a6590a50423e1184ecb88ceef9228d01ec92ea0e629e6f0fafa535740312a04316
b6773bb04310'
associated data
PT0 = b'dc71a551158e10bd27d2030c806eae2a'
          CT0 = b'dc71a551158e10bd27d2030c806eae28'
          C0 = b'f4853e945f7e786a98a6590a50423e11'
          PT1 = b'28f49bc54af068d7bf745a06d02c903a'
          C1 = b'84ecb88ceef9228d01ec92ea0e629e6f'
          PT2 = b'84ecb88ceef9228d01ec92ea0e629e69'
          CT2 = b'28f49bc54af068d7bf745a06d02c9038'
          C2 = b'0fafa535740312a04316b6773bb04310'
          PT3 = b'2e5b3ef03ef37a77fc62ec71eb9cd328'
          CT3 = b'ac182349a4094a5abe98c8ecde4e0e51'
             aes key
aes din
             aes dout
             = b'20d70f87dfa6f20f4d78ffc2dff84df7'
          AT1 = b'20d70f87dfa6f20f4d78ffc2dff84df7'
aes key
             aes din
             = b'20d70f87dfa6f20f4d78ffc2dff84df0'
aes dout
             = b'a212cc453888b0dc36e74edd09d91d9a'
          AT2 = b'a212cc453888b0dc36e74edd09d91d9a'
             aes key
             = b'a819cc453888b0dc36e74edd09d91d9a'
aes din
```

```
aes dout
       = b'cb0393bf8cfef645c4ce3af131c85cf1'
           AT3 = b'cb0393bf8cfef645c4ce3af131c85cf1'
           MT = b'90c3f61ce0bd7426507acf384f959972'
            IT = b'5bc065a36c43826394b4f5c97e5dc583'
        PADINFO = b'08010000100100000801000010010000'
aes key
              aes din
              = b'53c165a37c4282639cb5f5c96e5cc583'
              = b'109df4b49fd46f8e32b876177297f1ca'
aes dout
authentication tag = b'bc85d7fd3bdd25d48c20befbacd9ff9b'
              = b'bc85d7fd3bdd25d48c20befbacd9ff9b'
provided tag
out
```

```
AES-256, m=0, a=0
CSPAE - encryption
nonce
          aes key
aes din
aes dout
          = b'59976dafc8624bcf50214183c21d8df1'
message
associated data
        PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
        MT = b'ffffffffffffffffffffffffffffffffff
        aes kev
= b'fffffffffffffffffffffffffffffffff
aes din
aes dout
         = b'fe8925e4e8383d4b13efbe853900ac65'
authentication tag = b'a71e484b205a768443ceff06fb1d2196'
out
          = b'a71e484b205a768443ceff06fb1d2196'
```

```
AES-256, m=0, a=1
CSPAE - encryption
nonce
          aes kev
aes din
          aes dout
          = b'59976dafc8624bcf50214183c21d8df1'
message
PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
aes din
aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
        AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
         MT = b'ffffffffffffffffffffffffffffffffff
         IT = b'e2f44cbccf195856cb7d73c0fbb491b3'
      PADINFO = b'00000000800000000000000080000000'
aes key
aes din
          = b'e2f44cbc4f195856cb7d73c07bb491b3'
aes dout = b'862c4f8d70ae681152afb42d7a7cac01'
authentication tag = b'dfbb2222b8cc23de028ef5aeb86121f2'
          = b'dfbb2222b8cc23de028ef5aeb86121f2'
out
```

```
AES-256, m=1, a=0
CSPAE - encryption
nonce
aes kev
aes din
         aes dout
         = b'59976dafc8624bcf50214183c21d8df1'
         message
associated data =
        PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
= b'59976dafc8624bcf50214183c21d8df0'
aes din
         = b'873c83002e3bf2faa738a17b5efa0bca'
aes dout
        C0 = b'deabeeafe659b935f719e0f89ce7863b'
        PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
        MT = b'873c83002e3bf2f8a738a17b5efa0bc9'
         IT = b'873c83002e3bf2f8a738a17b5efa0bc9'
      aes key
aes din
          = b'073c83002e3bf2f82738a17b5efa0bc9'
aes dout = b'd5721fbe44273b5e7c8ffee48470db09'
authentication tag = b'd5721fbe44273b5e7c8ffee48470db0b'
b'deabeeafe659b935f719e0f89ce7863bd5721fbe44273b5e7c8ffee48470db0b'
```

```
AES-256, m=2, a=0
CSPAE - encryption
nonce
           aes kev
aes din
          aes dout
          = b'59976dafc8624bcf50214183c21d8df1'
message
associated data
        PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
= b'59976dafc8624bcf50214183c21d8df0'
aes din
aes dout
          = b'873c83002e3bf2faa738a17b5efa0bca'
        C0 = b'deabeeafe659b935f719e0f89ce7863b'
        PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
        aes key
aes din
           = b'873c83002e3bf2faa738a17b5efa0bcd'
aes dout
          = b'1a5a13760976028df384528a95b5fecb'
        C1 = b'1a5a13760976028df384528a95b5fec9'
        PT2 = b'1a5a13760976028df384528a95b5fecf'
        CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
         MT = b'bd62b20d578c094674b8d18abb8e0c35'
         IT = b'bd62b20d578c094674b8d18abb8e0c35'
      aes key
aes din
       = b'bd63b20d578c094674b9d18abb8e0c35'
aes dout = b'8f346cf185dd4a2292daca0284cfcc9a'
authentication tag = b'0808eff1abe6b8d835e26b79da35c751'
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec90808eff1abe6b8d835e2
6b79da35c751'
```

```
AES-256, m=3, a=0
CSPAE - encryption
nonce
           aes kev
aes din
       aes dout
          = b'59976dafc8624bcf50214183c21d8df1'
message
0000000000005'
associated data
         PT0 = b'59976dafc8624bcf50214183c21d8df3'
         CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
aes din
           = b'59976dafc8624bcf50214183c21d8df0'
aes dout
           = b'873c83002e3bf2faa738a17b5efa0bca'
         C0 = b'deabeeafe659b935f719e0f89ce7863b'
         PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
         aes key
aes din
           = b'873c83002e3bf2faa738a17b5efa0bcd'
aes dout
           = b'1a5a13760976028df384528a95b5fecb'
         C1 = b'1a5a13760976028df384528a95b5fec9'
         PT2 = b'1a5a13760976028df384528a95b5fecf'
         CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
aes key
aes din
           = b'1a5a13760976028df384528a95b5feca'
aes dout
           = b'a99fa75546c0b75eb7839a5016c06d77'
         C2 = b'2ea3245568fb45a410bb3b2b483a66bc'
         PT3 = b'a99fa75546c0b75eb7839a5016c06d72'
         CT3 = b'9d669076274df07754bcf3f1cb4ff504'
         MT = b'fd2354a48d8f425a2ae50a26318d9d05'
         IT = b'fd2354a48d8f425a2ae50a26318d9d05'
      aes kev
aes din
        = b'7d2254a48d8f425aaae40a26318d9d05'
aes dout
          = b'bc8d4fe22f1eb1863aee2daef443fa87'
authentication tag = b'21ebdf94085341f16e52de5f3f0c0f83'
out
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec92ea3245568fb45a410bb
3b2b483a66bc21ebdf94085341f16e52de5f3f0c0f83'
```

```
AES-256, m=3, a=1
CSPAE - encryption
nonce
aes kev
aes din
          aes dout
          = b'59976dafc8624bcf50214183c21d8df1'
message
0000000000005'
PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
aes din
          = b'59976dafc8624bcf50214183c21d8df0'
aes dout
          = b'873c83002e3bf2faa738a17b5efa0bca'
        C0 = b'deabeeafe659b935f719e0f89ce7863b'
        PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
        aes key
aes din
          = b'873c83002e3bf2faa738a17b5efa0bcd'
aes dout
          = b'1a5a13760976028df384528a95b5fecb'
        C1 = b'1a5a13760976028df384528a95b5fec9'
        PT2 = b'1a5a13760976028df384528a95b5fecf'
        CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
aes key
aes din
          = b'1a5a13760976028df384528a95b5feca'
aes dout
          = b'a99fa75546c0b75eb7839a5016c06d77'
        C2 = b'2ea3245568fb45a410bb3b2b483a66bc'
        PT3 = b'a99fa75546c0b75eb7839a5016c06d72'
        CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes kev
aes din
          aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
        AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
        MT = b'fd2354a48d8f425a2ae50a26318d9d05'
        IT = b'e028e7e7bd69e5f31e67861935c6f349'
      PADINFO = b'80010000800000008001000080000000'
aes key
= b'6029e7e73d69e5f39e668619b5c6f349'
aes din
```

```
authentication tag = b'a1c3608ac9089594d3ee5af725a84acb'
out
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec92ea3245568fb45a410bb
3b2b483a66bca1c3608ac9089594d3ee5af725a84acb'
AES-256, m=3, a=2
CSPAE - encryption
key
nonce
aes key
aes din
          = b'59976dafc8624bcf50214183c21d8df1'
aes dout
message
000000000005'
associated data
PT0 = b'59976dafc8624bcf50214183c21d8df3'
        CT0 = b'59976dafc8624bcf50214183c21d8df1'
aes key
= b'59976dafc8624bcf50214183c21d8df0'
aes din
          = b'873c83002e3bf2faa738a17b5efa0bca'
aes dout
        C0 = b'deabeeafe659b935f719e0f89ce7863b'
        PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
        aes key
aes din
          = b'873c83002e3bf2faa738a17b5efa0bcd'
aes dout
          = b'1a5a13760976028df384528a95b5fecb'
        C1 = b'1a5a13760976028df384528a95b5fec9'
        PT2 = b'1a5a13760976028df384528a95b5fecf'
        CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
aes kev
aes din
          = b'1a5a13760976028df384528a95b5feca'
          = b'a99fa75546c0b75eb7839a5016c06d77'
aes dout
        C2 = b'2ea3245568fb45a410bb3b2b483a66bc'
        PT3 = b'a99fa75546c0b75eb7839a5016c06d72'
        CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes key
aes din
          aes dout
          = b'1d0bb34330e6a7a934828c3f044b6e4c'
```

= b'3ca5f0fcee4565e38752a906eee7bfcf'

aes dout

= b'1d0bb34330e6a7a934828c3f044b6e4b' aes din aes dout = b'7063c6b5464200d250052782e699945a' AT2 = b'7063c6b5464200d250052782e699945a' MT = b'fd2354a48d8f425a2ae50a26318d9d05' IT = b'8d409211cbcd42887ae02da4d714095f' PADINFO = b'80010000000100008001000000010000' aes kev = b'0d419211cbcc4288fae12da4d715095f' aes din = b'ca20ca6d95056497d7760a1a6e61bdda' aes dout authentication tag = b'57465a1bb24894e083caf9eba52e48de' out b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec92ea3245568fb45a410bb 3b2b483a66bc57465a1bb24894e083caf9eba52e48de' AES-256, m=3, a=3CSPAE - encryption nonce aes kev aes din aes dout = b'59976dafc8624bcf50214183c21d8df1' message 0000000000005' associated data 000000000008' PT0 = b'59976dafc8624bcf50214183c21d8df3' CT0 = b'59976dafc8624bcf50214183c21d8df1' aes kev aes din = b'59976dafc8624bcf50214183c21d8df0' aes dout = b'873c83002e3bf2faa738a17b5efa0bca' C0 = b'deabeeafe659b935f719e0f89ce7863b' PT1 = b'873c83002e3bf2faa738a17b5efa0bc9' aes key aes din = b'873c83002e3bf2faa738a17b5efa0bcd' aes dout = b'1a5a13760976028df384528a95b5fecb' C1 = b'1a5a13760976028df384528a95b5fec9' PT2 = b'1a5a13760976028df384528a95b5fecf'

AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'

aes key

```
CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
aes key
aes din
            = b'1a5a13760976028df384528a95b5feca'
aes dout
            = b'a99fa75546c0b75eb7839a5016c06d77'
         C2 = b'2ea3245568fb45a410bb3b2b483a66bc'
         PT3 = b'a99fa75546c0b75eb7839a5016c06d72'
         CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes key
aes din
            aes dout
            = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
aes din
            = b'1d0bb34330e6a7a934828c3f044b6e4b'
aes dout
            = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7063c6b5464200d250052782e6999452'
aes dout
            = b'2fa5cb037e60bc50a204a5a6a43a240e'
         AT3 = b'2fa5cb037e60bc50a204a5a6a43a240e'
          MT = b'fd2354a48d8f425a2ae50a26318d9d05'
          IT = b'd2869fa7f3effe0a88e1af8095b7b90b'
       PADINFO = b'80010000800100008001000080010000'
aes key
aes din = b'52879fa773eefe0a08e0af8015b6b90b'
aes dout
           = b'd11c6f65be8b169f0ef0dcc08e8b9dab'
authentication tag = b'4c7aff1399c6e6e85a4c2f3145c468af'
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec92ea3245568fb45a410bb
3b2b483a66bc4c7aff1399c6e6e85a4c2f3145c468af'
CSPAE - decryption
kev
nonce
aes key
aes din
            aes dout
            = b'59976dafc8624bcf50214183c21d8df1'
message
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec92ea3245568fb45a410bb
3b2b483a66bc'
associated data
000000000008'
         PT0 = b'59976dafc8624bcf50214183c21d8df3'
         CTO = b'59976dafc8624bcf50214183c21d8df1'
```

```
C0 = b'deabeeafe659b935f719e0f89ce7863b'
         PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
         C1 = b'1a5a13760976028df384528a95b5fec9'
         PT2 = b'1a5a13760976028df384528a95b5fecf'
         CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
         C2 = b'2ea3245568fb45a410bb3b2b483a66bc'
         PT3 = b'a99fa75546c0b75eb7839a5016c06d72'
         CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes kev
aes din
            aes dout
            = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
= b'1d0bb34330e6a7a934828c3f044b6e4b'
aes din
aes dout
            = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7063c6b5464200d250052782e6999452'
aes dout
            = b'2fa5cb037e60bc50a204a5a6a43a240e'
         AT3 = b'2fa5cb037e60bc50a204a5a6a43a240e'
          MT = b'fd2354a48d8f425a2ae50a26318d9d05'
          IT = b'd2869fa7f3effe0a88e1af8095b7b90b'
       PADTNFO = b'80010000800100008001000080010000'
aes key
aes din
            = b'52879fa773eefe0a08e0af8015b6b90b'
aes dout
            = b'd11c6f65be8b169f0ef0dcc08e8b9dab'
authentication tag = b'4c7aff1399c6e6e85a4c2f3145c468af'
provided tag
            = b'4c7aff1399c6e6e85a4c2f3145c468af'
out
0000000000005'
AES-256, m=3, a=3 padded
CSPAE - encryption
key
```

```
associated data
PT0 = b'59976dafc8624bcf50214183c21d8df3'
         CTO = b'59976dafc8624bcf50214183c21d8df1'
aes key
aes din
           = b'59976dafc8624bcf50214183c21d8df0'
aes dout
           = b'873c83002e3bf2faa738a17b5efa0bca'
         C0 = b'deabeeafe659b935f719e0f89ce7863b'
         PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
         aes key
aes din
           = b'873c83002e3bf2faa738a17b5efa0bcd'
aes dout
           = b'1a5a13760976028df384528a95b5fecb'
         C1 = b'1a5a13760976028df384528a95b5fec9'
         PT2 = b'1a5a13760976028df384528a95b5fecf'
         CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
aes key
aes din
           = b'135a13760976028df384528a95b5fecf'
aes dout
           = b'284a0269b2d1cf432d37582c7d7ee367'
         C2 = b'af7681699cea3db98a0ff9572384e8ac'
         PT3 = b'214a0269b2d1cf432d37582c7d7ee367'
         CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes key
aes din
           aes dout
           = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes key
aes din
           = b'1d0bb34330e6a7a934828c3f044b6e4b'
aes dout
           = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
           = b'7a68c6b5464200d250052782e699945a'
aes dout
           = b'60b5faaac58c24e040efa51309f8474f'
         AT3 = b'60b5faaac58c24e040efa51309f8474f'
         MT = b'75f6f198799e3a47b051c85a5a331310'
         IT = b'15430b32bc121ea7f0be6d4953cb545f'
      PADINFO = b'08010000100100000801000010010000'
aes key
aes din
      = b'1d420b32ac131ea7f8bf6d4943ca545f'
aes dout
           = b'68a8e4c6c721307dbd848febf4634d3e'
```

```
authentication tag = b'f5ce74b0e06cc00ae9387c1a3f2cb83a'
out
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec9af7681699cea3db98a0f
f9572384e8acf5ce74b0e06cc00ae9387c1a3f2cb83a'
CSPAE - decryption
key
nonce
aes key
aes din
           = b'59976dafc8624bcf50214183c21d8df1'
aes dout
message
b'deabeeafe659b935f719e0f89ce7863b1a5a13760976028df384528a95b5fec9af7681699cea3db98a0f
f9572384e8ac'
associated data
PT0 = b'59976dafc8624bcf50214183c21d8df3'
         CT0 = b'59976dafc8624bcf50214183c21d8df1'
         C0 = b'deabeeafe659b935f719e0f89ce7863b'
         PT1 = b'873c83002e3bf2faa738a17b5efa0bc9'
         C1 = b'1a5a13760976028df384528a95b5fec9'
         PT2 = b'1a5a13760976028df384528a95b5fecf'
         CT2 = b'873c83002e3bf2faa738a17b5efa0bcb'
         C2 = b'af7681699cea3db98a0ff9572384e8ac'
         PT3 = b'214a0269b2d1cf432d37582c7d7ee367'
         CT3 = b'9d669076274df07754bcf3f1cb4ff504'
aes key
            =
aes din
            aes dout
           = b'1d0bb34330e6a7a934828c3f044b6e4c'
         AT1 = b'1d0bb34330e6a7a934828c3f044b6e4c'
aes kev
aes din
            = b'1d0bb34330e6a7a934828c3f044b6e4b'
aes dout
            = b'7063c6b5464200d250052782e699945a'
         AT2 = b'7063c6b5464200d250052782e699945a'
aes key
aes din
            = b'7a68c6b5464200d250052782e699945a'
aes dout
            = b'60b5faaac58c24e040efa51309f8474f'
         AT3 = b'60b5faaac58c24e040efa51309f8474f'
          MT = b'75f6f198799e3a47b051c85a5a331310'
          IT = b'15430b32bc121ea7f0be6d4953cb545f'
       PADINFO = b'08010000100100000801000010010000'
aes key
```