CFRG
Internet-Draft
Intended status: Informational
Expires: November 10, 2016

S. Gueron
University of Haifa and Intel Corporation
A. Langley
Google
Y. Lindell
Bar Ilan University
May 9, 2016

AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption
draft-irtf-cfrg-gcmsiv-01

Abstract

This memo specifies two authenticated encryption algorithms that are nonce misuse-resistant - that is that they do not fail catastrophically if a nonce is repeated.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 10, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The concept of "Authenticated encryption with additional data" (AEAD [RFC5116]) couples confidentiality and integrity in a single operation that is easier for practitioners to use correctly. The most popular AEAD, AES-GCM [GCM], is seeing widespread use due to its attractive performance.

However, most AEADs suffer catastrophic failures of confidentiality and/or integrity when two distinct messages are encrypted with the same nonce. While the requirements for AEADs specify that the pair of (key, nonce) shall only ever be used once, and thus prohibit this, in practice this is a worry.

Nonce misuse-resistant AEADs do not suffer from this problem. For this class of AEADs, encrypting two messages with the same nonce only discloses whether the messages were equal or not. This is the minimum amount of information that a deterministic algorithm can leak in this situation.

This memo specifies two nonce misuse-resistant AEADs: "AEAD_AES_128_GCM_SIV" and "AEAD_AES_256_GCM_SIV". These AEADs are designed to be able to take advantage of existing hardware support for AES-GCM and can run within 5% of the speed of AES-GCM.

We suggest that these AEADs be considered in any situation where there is the slightest doubt about nonce uniqueness.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. POLYVAL

The GCM-SIV construction is similar to GCM: the block cipher is used in counter mode to encrypt the plaintext and a polynomial authenticator is used to provide integrity. The authenticator in GCM-SIV is called POLYVAL.

POLYVAL, like GHASH, operates in a binary field of size 2^128. The field is defined by the irreducible polynomial x^128 + x^127 + x^126 + x^121 + 1. The sum of any two elements in the field is the result of XORing them. The product of any two elements is calculated using standard (binary) polynomial multiplication followed by reduction modulo the irreducible polynomial.

We define another binary operation on elements of the field: dot(a, b), where dot(a, b) = a * b * x^-128. The value of the field element x^-128 is equal to x^127 + x^124 + x^121 + x^114 + 1. The result, dot(a, b), of this multiplication is another field element.

Polynomials in this field are converted to and from 128-bit strings by taking the least-significant bit of the first byte to be the coefficient of x^0, the most-significant bit of the first byte to the the coefficient of x^7 and so on, until the most-significant bit of the last byte is the coefficient of x^127.

POLYVAL takes a field element, H, and a series of field elements X_1, ..., X_s. Its result is S_s, where S is defined by the iteration S_0 = 0; S_j = dot(S_{j-1} + X_j, H).

We note that POLYVAL(H, X_1, X_2, ...) is equal to ByteSwap(GHASH(x*H, ByteSwap(X_1), ByteSwap(X_2), ...)), where ByteSwap is a function that converts a field element to a 128-bit string, reverses the order of the bytes, and interprets the result as a field element again.

4. Encryption

AES-GCM-SIV encryption takes a 16-byte authentication key, a 16- or 32-byte AES key, a 128-bit nonce, and arbitrary-length plaintext and additional data inputs. It outputs an authenticated ciphertext that will be 16 bytes longer than the plaintext.

If the AES key is 16 bytes long then AES-128 is used throughout and the _record-encryption key_ is defined as the encryption of the nonce using the AES key.

Alternatively, if the AES key is 32 bytes long then AES-256 is used throughout. Encrypting the nonce generates 128 bits of output, but this insufficient with AES-256 because 256 bits are needed. Thus the encryption of the nonce is used as the final 16 bytes of the record-encryption key and those sixteen bytes are encrypted again to generate the first sixteen bytes.

In pseudo-code form:

```
if len(AES-key) == 16 {
  record-encryption-key = AES128(key = AES-key, input = nonce)
} else if len(AES-key) == 32 {
  second-half = AES256(key = AES-key, input = nonce)
  first-half = AES256(key = AES-key, input = second-half)
  record-encryption-key = concatenate(first-half, second-half)
}
```

Define the _length block_ as a 16-byte value that is the concatenation of the 64-bit, little-endian encodings of len(additional_length)*8 and len(plaintext)*8. Pad the plaintext and additional data with zeros until they are each a multiple of 16 bytes, the AES block size. Then X_1, X_2, etc (the series of field elements that are inputs to POLYVAL) are the concatenation of the padded additional data, the padded plaintext and the length block.

Calculate S_s = POLYVAL(authentication_key, X_1, X_2, ...), XOR it with the nonce and then set the most-significant bit of the last byte to zero. Encrypt the result with AES using the record-encryption key to produce the tag.

The ciphertext is produced by using AES in counter mode on the unpadded plaintext. The initial counter block is the tag with the most-significant bit of the last byte set to one. The counter advances by incrementing the first 32 bits interpreted as an unsigned, little-endian integer. The result of the encryption is the resulting ciphertext followed by the tag.

5. Decryption

Decryption takes a 16-byte authentication key, a 16- or 32-byte AES key, a 128-bit nonce, and arbitrary-length ciphertext and additional data inputs. It either fails, or outputs a plaintext that is 16 bytes shorter than the ciphertext.

Firstly, the record-encryption key is derived in the same manner as when encrypting.

If the ciphertext is less than 16 bytes or more than 2^36 + 16 bytes, then fail. Otherwise split the input into the encrypted plaintext and a 16-byte tag. Decrypt the encrypted plaintext with the record-encryption key in counter mode, where the initial counter block is the tag with the most-significant bit of the last byte. The counter advances in the same way as for encryption.

Pad the additional data and plaintext with zeros until they are each a multiple of 16 bytes, the AES block size. Calculate length_block and X_1, X_2, etc as above and compute S_s = POLYVAL(authentication_key, X_1, X_2, ...). Compute the expected tag by XORing S_s and the nonce, setting the most-significant byte of the last byte to zero and encrypting with the record-encryption key. Compare the provided and expected tag values in constant time. If they do not match, fail. Otherwise return the plaintext.

6. AEADs

We define two AEADs, in the format of RFC 5116, that use AES-GCM-SIV: AEAD_AES_128_GCM_SIV and AEAD_AES_256_GCM_SIV. They differ only in the size of the AES key used.

Since the definition of an AEAD requires that the key be a single value we define AEAD_AES_128_GCM_SIV to take a 32-byte key: the first 16 bytes of which are used as the authentication key and the remaining 16 bytes are used as the AES key. Likewise AEAD_AES_256_GCM_SIV takes an 48-byte key: the first 16 bytes are again the authentication key and the remaining 32 bytes is the AES key.

The parameters for AEAD_AES_128_GCM_SIV are then: K_LEN is 32, P_MAX is 2^36, A_MAX is 2^61 - 1, N_MIN and N_MAX are 16 and C_MAX is 2^36 + 16.

The parameters for AEAD_AES_256_GCM_SIV differ only in the key size: K_LEN is 48, P_MAX is 2^36, A_MAX is 2^61 - 1, N_MIN and N_MAX are 16 and C_MAX is 2^36 + 16.

7. Field operation examples

Polynomials in this document will be written as 16-byte values. For example, the sixteen bytes 01000000000000000000000000000492 would represent the polynomial x^127 + x^124 + x^121 + x^114 + 1, which is also the value of x^-128 in this field.

If a = 66e94bd4ef8a2c3b884cfa59ca342b2e and b = ff000000000000000000000000000000 then a+b = 99e94bd4ef8a2c3b884cfa59ca342b2e, a*b = 37856175e9dc9df26ebc6d6171aa0ae9 and dot(a, b) = ebe563401e7e91ea3ad6426b8140c394.

8. Worked example

Consider the encryption of the plaintext "Hello world" with the additional data "example" under key 4f2229294acbdf99c4584ec0e6e23638fab3a110b8ae672eba07d91ba52d6cea using AEAD_AES_128_GCM_SIV. The random nonce that we'll use for this example is 752abad3e0afb5f434dc4310f71f3d21.

The record encryption key will be AES(key = fab3a110b8ae672eba07d91ba52d6cea, data = 752abad3e0afb5f434dc4310f71f3d21) = b55e60e9e8886006db16db23e1e0e103.

The length block contains the encoding of the bit-lengths of the additional data and plaintext, respectively, which are and 56 and 88. Thus length_block is 38000000000000005800000000000000.

The input to POLYVAL is the padded additional data, padded plaintext and then the length block. This is 6578616d706c650000000000000000048656c6c6f20776f726c6400000000005800000000000000038000000000000000.

The POLYVAL key will be the first 16 bytes of the AEAD key, namely 4f2229294acbdf99c4584ec0e6e23638. Calling POLYVAL with that key and the input above results in S_s = 0b9ae2c5bd7fe4dcd17a007d11ac280e. XORing this with the nonce gives 7eb058165dd05128e5a6436de6b3152f.

Before encrypting the most-significant bit of the last byte is cleared. This again gives 7eb058165dd05128e5a6436de6b3152f because that bit happened to be zero already. Encrypting with the record key gives the tag, which is 8e2d69ed54c0997cae05d8b2be1d963e.

In order to form the initial counter block, the most-significant bit of the last byte of the tag is set to one. This gives 8e2d69ed54c0997cae05d8b2be1d96be. Encrypting this with the record key gives the first block of the keystream: efc341b420fda4250c21e8571560d8f9.

The final ciphertext is the result of XORing the plaintext with the keystream and appending the tag. That gives a7a62dd84fddd34a7e4d8c8e2d69ed54c0997cae05d8b2be1d963e.

9. Security Considerations

The AEADs defined in this document calculate fresh AES keys for each nonce. This allows a larger number of plaintexts to be encrypted under a given key. Without this step, each SIV encryption would be like a standard GCM encryption with a random nonce. Since the nonce size for GCM is only 12 bytes, NIST set a limit [GCM] of 2^32 encryptions before the probability of duplicate nonces becomes too high.

The authors felt that, while large, 2^32 wasn't so large that this limit could be safely ignored. For example, consider encrypting the contents of a hard disk where the AEAD record size is 512 bytes, to match the traditional size of a disk sector. This process would have encrypted 2^32 records after processing 2TB, yet hard drives of multiple terabytes are now common.

Deriving fresh AES keys for each nonce eliminates this problem.

If the nonce is fixed then AES-GCM-SIV acts like AES-GCM with a random nonce, with the caveat that identical plaintexts will produce identical ciphertexts. Thus, with a fixed nonce, the 2^32 limit still applies as the number of distinct messages that can be encrypted under a given key. Nonces should be unique and the misuse-resistance of these AEADs should not be depended on to the extent that 2^32 duplicates may occur.

The construction of the record-encryption key in AEAD_AES_256_GCM_SIV cannot result in the first and second halves of the key having the same value. Thus 2^128 of the 2^256 keys cannot occur. We consider this to be insignificant.

A security analysis of a similar scheme appears in [GCM-SIV].

10. IANA Considerations

This document has no actions for IANA.

11. Acknowledgements

The authors would like to thank Uri Blumenthal for his helpful suggestions.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

12.2. Informative References

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST SP-800-38D, November 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>.

[GCM-SIV] Gueron, S. and Y. Lindell, "GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle Per Byte", Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security , 2015, <http://doi.acm.org/10.1145/2810103.2813613>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <http://www.rfc-editor.org/info/rfc5116>.

Appendix A. Test vectors

A.1. AEAD_AES_128_GCM_SIV

```
---------------------- TWO_KEYS     (AAD = 0, MSG = 0)---------

AAD_byte_len = 0
AAD_bit_len  = 0
MSG_byte_len = 0
MSG_bit_len  = 0
padded_AAD_byte_len = 0
padded_MSG_byte_len = 0
L1 blocks AAD(padded)  = 0
L2 blocks MSG(padded)  = 0
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
NONCE =                         03000000000000000000000000000000
```

```
   AAD =
   MSG =
   PADDED_AAD_and_MSG =
   LENBLK =                        00000000000000000000000000000000

   Computing POLYVAL on a
   buffer of 0 blocks + LENBLK.
   POLYVAL =                       00000000000000000000000000000000
   POLYVAL_xor_NONCE  =            03000000000000000000000000000000
   with MSBit cleared =            03000000000000000000000000000000
   TAG =                           fabfd7964630aa6128ee6269f061f08b
   AAD =
   CT  =
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 8)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                              BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
```

```
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =
   MSG =                          0100000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
   LENBLK =                       00000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                      04000000000000809100000000283b1c
   POLYVAL_xor_NONCE  =           07000000000000809100000000283b1c
   with MSBit cleared =           07000000000000809100000000283b1c
   TAG =                          5537355b0a4f4cb05ce77d1b815d7299
   AAD =
   CT  =                          9c9ba00f9686d157
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  5537355b0a4f4cb05ce77d1b815d7299



   -------------------- TWO_KEYS     (AAD = 0, MSG = 12)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
```

```
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        010000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
   LENBLK =                     00000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                    04000000000000040d900000000283b1c
   POLYVAL_xor_NONCE  =         07000000000000040d900000000283b1c
   with MSBit cleared =         07000000000000040d900000000283b1c
   TAG =                        dd55830c690eadd7fd2155b3615470bd
   AAD =
   CT  =                        af21532e06416ab7a902710e
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   dd55830c690eadd7fd2155b3615470bd


   ---------------------- TWO_KEYS     (AAD = 0, MSG = 16)---------

   AAD_byte_len = 0
```

```
   AAD_bit_len  = 0
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =
   MSG =                          01000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
   LENBLK =                       00000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                      04000000000000002301000000283b1c
   POLYVAL_xor_NONCE  =           07000000000000002301000000283b1c
   with MSBit cleared =           07000000000000002301000000283b1c
   TAG =                          147650d36f064f6b5dbbe8f04077d903
   AAD =
   CT  =                          a42b0ef844bd99fb2658e7a93fc8159c
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  147650d36f064f6b5dbbe8f04077d983
```

```
   ---------------------- TWO_KEYS     (AAD = 0, MSG = 32)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 2
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     00000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    01000000000000004602000 0f0507615
   POLYVAL_xor_NONCE  =         02000000000000004602000 0f0507615
   with MSBit cleared =         02000000000000004602000 0f0507615
   TAG =                        78a50cb3f901ee38c588f6662d785a24
   AAD =
   CT  =                        ebb355fb913c781bee9ea36ff920193f
                                80c8aa6d0abd197f039be49616f62e4f
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
```

```
                                c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                78a50cb3f901ee38c588f6662d785aa4
                                79a50cb3f901ee38c588f6662d785aa4


   --------------------- TWO_KEYS     (AAD = 0, MSG = 48)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 3
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   LENBLK =                     00000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                    0e000000000000000650300203e788f7f
   POLYVAL_xor_NONCE  =         0d000000000000000650300203e788f7f
   with MSBit cleared =         0d000000000000000650300203e788f7f
   TAG =                        a75aa62b704e826d984a72184e370598
   AAD =
   CT  =                        5cf01ee258867977c0dd93dc33c9ccaf
                                fcf088d95bb3d17221cfb58f2cd14703
                                068463f2c0a18185cd745bcaf7b72ed5
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e

   **************************
```

APPENDIX

KEY_SCHEDULE (Encryption_Key)
57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

a75aa62b704e826d984a72184e370598
a85aa62b704e826d984a72184e370598
a95aa62b704e826d984a72184e370598

---------- TWO_KEYS (AAD = 0, MSG = 64)---------

AAD_byte_len = 0
AAD_bit_len = 0
MSG_byte_len = 64
MSG_bit_len = 512
padded_AAD_byte_len = 0
padded_MSG_byte_len = 64
L1 blocks AAD(padded) = 0
L2 blocks MSG(padded) = 4

BYTES ORDER
LSB-------------------------MSB
000102030405060708090101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000

```
   LENBLK =                         00000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                        0f000000000000008c04c04c63ad584f
   POLYVAL_xor_NONCE  =             0c000000000000008c04c04c63ad584f
   with MSBit cleared =             0c000000000000008c04c04c63ad584f
   TAG =                            d7f4efe2f6c72e3b8df168cab6b790ab
   AAD =
   CT  =                            442acedd0154ad46741b42ea12bd76b6
                                    6f3f13e79c89e88fc0d0651ab70aa474
                                    226f538c660d95f0867dc65d7c0b0af6
                                    17339e1db42294b52b4ab4fc06234769
   Encryption_Key=                  57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    57d4b7aec8de993e30a6861b61e6ce4e
                                    d85f98411081017f2027876441c1492a
                                    a2647dc2b2e57cbd92c2fbd9d303b2f3
                                    dd5370a46fb60c19fd74f7c02e774533
                                    203db3954f8bbf8cb2ff484c9c880d7f
                                    f4ea614bbb61dec7099e968b95169bf4
                                    93fede61289f00a62101962db4170dd9
                                    2329ebec0bb6eb4a2ab77d679ea070be
                                    437845e748ceaead6279d3cafcd9a374
                                    6d72d75725bc79fa47c5aa30bb1c0944
                                    c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                    d7f4efe2f6c72e3b8df168cab6b790ab
                                    d8f4efe2f6c72e3b8df168cab6b790ab
                                    d9f4efe2f6c72e3b8df168cab6b790ab
                                    daf4efe2f6c72e3b8df168cab6b790ab



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 8)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
```

```
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101121314 15
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =                           01
   MSG =                           0200000000000000
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                   02000000000000000000000000000000
   LENBLK =                        08000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                       13000000000000080910000000f0501631
   POLYVAL_xor_NONCE  =            10000000000000080910000000f0501631
   with MSBit cleared =            10000000000000080910000000f0501631
   TAG =                           633c11b2eee1f65be0e3f1e0c824c5e0
   AAD =                           01
   CT  =                           b3aa6df500d38f0f
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   633c11b2eee1f65be0e3f1e0c824c5e0


   ---------------------- TWO_KEYS     (AAD = 1, MSG = 12)---------

   AAD_byte_len = 1
```

```
   AAD_bit_len  = 8
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01
   MSG =                          020000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000

   LENBLK =                       08000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      13000000000000040d9000000f0501631
   POLYVAL_xor_NONCE  =           10000000000000040d9000000f0501631
   with MSBit cleared =           10000000000000040d9000000f0501631
   TAG =                          f229e75b2c4c3048fc70f163c9aefe0d
   AAD =                          01
   CT  =                          b5bea0352fbe77e5dc84aac4
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  f229e75b2c4c3048fc70f163c9aefe8d
```

```
   ---------------------- TWO_KEYS     (AAD = 1, MSG = 16)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101121314 15
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01
   MSG =                          02000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       08000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      13000000000000000023010000f0501631
   POLYVAL_xor_NONCE  =           10000000000000000023010000f0501631
   with MSBit cleared =           10000000000000000023010000f0501631
   TAG =                          cfb5aa16cdd9d39acc5d99b6eee2c6fc
   AAD =                          01
   CT  =                          86f7d1853ecc302a598c0e054d917a9c
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633
```

```
   CTRBLKS (with MSbit set to 1)

                                 cfb5aa16cdd9d39acc5d99b6eee2c6fc



   -------------------- TWO_KEYS     (AAD = 1, MSG = 32)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 2
                                            BYTES ORDER
                                 LSB-------------------------MSB
                                 000102030405060708091011121314 15
                                 --------------------------------
   K1 = H =                      03000000000000000000000000000000
   K2 = K =                      01000000000000000000000000000000
   NONCE =                       03000000000000000000000000000000
   AAD =                         01
   MSG =                         02000000000000000000000000000000
                                 03000000000000000000000000000000
   PADDED_AAD_and_MSG =          01000000000000000000000000000000
                                 02000000000000000000000000000000
                                 03000000000000000000000000000000
   LENBLK =                      08000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                     1c000000000000000460200203e78ef5b
   POLYVAL_xor_NONCE  =          1f000000000000000460200203e78ef5b
   with MSBit cleared =          1f000000000000000460200203e78ef5b
   TAG =                         8df5606f057468e4b38e89736255ad2d
   AAD =                         01
   CT  =                         a58e74cc44de5637d02d800119da54c1
                                 df3f9f8a1930953819a7d8d1d76f10c0
   Encryption_Key=               57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                 d85f98411081017f2027876441c1492a
                                 a2647dc2b2e57cbd92c2fbd9d303b2f3
```

```
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafcd9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                8df5606f057468e4b38e89736255adad
                                8ef5606f057468e4b38e89736255adad



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 48)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 3
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     08000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                    1d00000000000006503c04c63ad386b
   POLYVAL_xor_NONCE  =         1e00000000000006503c04c63ad386b
   with MSBit cleared =         1e00000000000006503c04c63ad386b
```

```
   TAG =                          b52274e14d6111c74edf5d95855256a2
   AAD =                          01
   CT  =                          9ceaefd1522cc88b1a9dde5f86253b70
                                  309a25c160bb37dc677ed126ce23e7ab
                                  31ea937735d6353af5cf02de8ff5b2ff
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  b52274e14d6111c74edf5d95855256a2
                                  b62274e14d6111c74edf5d95855256a2
                                  b72274e14d6111c74edf5d95855256a2



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 64)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 4
                                              BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01
```

```
   MSG =                          02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
                                  05000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
                                  05000000000000000000000000000000
   LENBLK =                       08000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 5 blocks + LENBLK.
   POLYVAL =                      1b000000000000008c841a01712a376e
   POLYVAL_xor_NONCE  =           18000000000000008c841a01712a376e
   with MSBit cleared =           18000000000000008c841a01712a376e
   TAG =                          668fc00b6b40b4bb0c8d6cdb9730358d
   AAD =                          01
   CT  =                          457e976e1f62be30a2bfb8d8801b7282
                                  8dd5349701b0f93007bcae4c2daed6fa
                                  d91c3ae1751edaf54abf47bb1f0608dd
                                  2961c86e7860dcb75336be054c1ad6cf
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  668fc00b6b40b4bb0c8d6cdb9730358d
                                  678fc00b6b40b4bb0c8d6cdb9730358d
                                  688fc00b6b40b4bb0c8d6cdb9730358d
                                  698fc00b6b40b4bb0c8d6cdb9730358d
```

```
   ---------------------- TWO_KEYS     (AAD = 12, MSG = 4)---------

   AAD_byte_len = 12
   AAD_bit_len  = 96
   MSG_byte_len = 4
   MSG_bit_len  = 32
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101121314 15
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          0100000000000000000000
   MSG =                          02000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       60000000000000002000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      d8000000000000c048000000f050f665
   POLYVAL_xor_NONCE  =           db000000000000c048000000f050f665
   with MSBit cleared =           db000000000000c048000000f050f665
   TAG =                          488346eaebe2d64ffa58e0fa82f8cd43
   AAD =                          0100000000000000000000
   CT  =                          c2b96956
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633
```

```
   CTRBLKS (with MSbit set to 1)

                                 488346eaebe2d64ffa58e0fa82f8cdc3



   -------------------- TWO_KEYS     (AAD = 18, MSG = 20)---------

   AAD_byte_len = 18
   AAD_bit_len  = 144
   MSG_byte_len = 20
   MSG_bit_len  = 160
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                            BYTES ORDER
                                 LSB-------------------------MSB
                                 000102030405060708091011121314 15
                                 --------------------------------
   K1 = H =                      03000000000000000000000000000000
   K2 = K =                      01000000000000000000000000000000
   NONCE =                       03000000000000000000000000000000
   AAD =                         01000000000000000000000000000000
                                 0200
   MSG =                         03000000000000000000000000000000
                                 04000000
   PADDED_AAD_and_MSG =          01000000000000000000000000000000
                                 02000000000000000000000000000000
                                 03000000000000000000000000000000
                                 04000000000000000000000000000000
   LENBLK =                      90000000000000a000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                     08010000000000c06b01c04c63ad9807
   POLYVAL_xor_NONCE  =          0b010000000000c06b01c04c63ad9807
   with MSBit cleared =          0b010000000000c06b01c04c63ad9807
   TAG =                         d010794cfdbbc65ef641b8ccb9c2dda3
   AAD =                         01000000000000000000000000000000
                                 0200
   CT  =                         348bf14b0fe2f8a2c3e843429df6276c
                                 c0e5e688
   Encryption_Key=               57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
```

```
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   d010794cfdbbc65ef641b8ccb9c2dda3
                                   d110794cfdbbc65ef641b8ccb9c2dda3



   ---------------------- TWO_KEYS     (AAD = 20, MSG = 18)---------

   AAD_byte_len = 20
   AAD_bit_len  = 160
   MSG_byte_len = 18
   MSG_bit_len  = 144
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                             BYTES ORDER
                                   LSB--------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =                           01000000000000000000000000000000
                                   02000000
   MSG =                           03000000000000000000000000000000
                                   0400
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                   02000000000000000000000000000000
                                   03000000000000000000000000000000
                                   04000000000000000000000000000000
   LENBLK =                        a0000000000000009000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
```

```
   POLYVAL =                        64010000000000600701c04c63add8de
   POLYVAL_xor_NONCE  =             67010000000000600701c04c63add8de
   with MSBit cleared =             67010000000000600701c04c63add85e
   TAG =                            98e16515942fb8ff9ef108e7ce53a963
   AAD =                            01000000000000000000000000000000
                                    02000000
   CT  =                            f803a8b63ffa8c44a391c7e4ccc31e61
                                    79d1
   Encryption_Key=                  57d4b7aec8de993e30a6861b61e6ce4e

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    57d4b7aec8de993e30a6861b61e6ce4e
                                    d85f98411081017f2027876441c1492a
                                    a2647dc2b2e57cbd92c2fbd9d303b2f3
                                    dd5370a46fb60c19fd74f7c02e774533
                                    203db3954f8bbf8cb2ff484c9c880d7f
                                    f4ea614bbb61dec7099e968b95169bf4
                                    93fede61289f00a62101962db4170dd9
                                    2329ebec0bb6eb4a2ab77d679ea070be
                                    437845e748ceaead6279d3cafcd9a374
                                    6d72d75725bc79fa47c5aa30bb1c0944
                                    c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                    98e16515942fb8ff9ef108e7ce53a9e3
                                    99e16515942fb8ff9ef108e7ce53a9e3



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 0)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 0
   MSG_bit_len  = 0
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 0
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 0
                                              BYTES ORDER
                                    LSB--------------------------MSB
                                    000102030405060708090101121314 15
                                    --------------------------------
   K1 = H =                         03000000000000000000000000000000
   K2 = K =                         01000000000000000000000000000000
```

```
   NONCE =                          03000000000000000000000000000000
   AAD =
   MSG =
   PADDED_AAD_and_MSG =
   LENBLK =                         00000000000000000000000000000000

   Computing POLYVAL on a
   buffer of 0 blocks + LENBLK.
   POLYVAL =                        00000000000000000000000000000000
   POLYVAL_xor_NONCE  =             03000000000000000000000000000000
   with MSBit cleared =             03000000000000000000000000000000
   TAG =                            fabfd7964630aa6128ee6269f061f08b
   AAD =
   CT  =
   Encryption_Key=                  57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =

   TAG' =                           fabfd7964630aa6128ee6269f061f08b

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    57d4b7aec8de993e30a6861b61e6ce4e
                                    d85f98411081017f2027876441c1492a
                                    a2647dc2b2e57cbd92c2fbd9d303b2f3
                                    dd5370a46fb60c19fd74f7c02e774533
                                    203db3954f8bbf8cb2ff484c9c880d7f
                                    f4ea614bbb61dec7099e968b95169bf4
                                    93fede61289f00a62101962db4170dd9
                                    2329ebec0bb6eb4a2ab77d679ea070be
                                    437845e748ceaead6279d3cafcd9a374
                                    6d72d75725bc79fa47c5aa30bb1c0944
                                    c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 8)---------

   AAD_byte_len = 0
```

```
   AAD_bit_len  = 0
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        0100000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
   LENBLK =                     00000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                    04000000000000809100000000283b1c
   POLYVAL_xor_NONCE  =         07000000000000809100000000283b1c
   with MSBit cleared =         07000000000000809100000000283b1c
   TAG =                        5537355b0a4f4cb05ce77d1b815d7299
   AAD =
   CT  =                        9c9ba00f9686d157
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =              0100000000000000

   TAG' =                       5537355b0a4f4cb05ce77d1b815d7299

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
```

```
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafcd9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                5537355b0a4f4cb05ce77d1b815d7299



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 12)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB-------------------------MSB
                                00010203040506070809101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
   LENBLK =                     00000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                    0400000000000040d900000000283b1c
   POLYVAL_xor_NONCE  =         0700000000000040d900000000283b1c
   with MSBit cleared =         0700000000000040d900000000283b1c
   TAG =                        dd55830c690eadd7fd2155b3615470bd
   AAD =
   CT  =                        af21532e06416ab7a902710e
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =              01000000000000000000000
```

```
   TAG' =                          dd55830c690eadd7fd2155b3615470bd

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   dd55830c690eadd7fd2155b3615470bd



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 16)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                               BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101121314 15
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =
   MSG =                           01000000000000000000000000000000
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
   LENBLK =                        00000000000000008000000000000000

   Computing POLYVAL on a
```

```
   buffer of 1 blocks + LENBLK.
   POLYVAL =                        040000000000000002301000000283b1c
   POLYVAL_xor_NONCE  =             070000000000000002301000000283b1c
   with MSBit cleared =             070000000000000002301000000283b1c
   TAG =                            147650d36f064f6b5dbbe8f04077d903
   AAD =
   CT  =                            a42b0ef844bd99fb2658e7a93fc8159c
   Encryption_Key=                  57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                  01000000000000000000000000000000

   TAG' =                           147650d36f064f6b5dbbe8f04077d903

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)    57d4b7aec8de993e30a6861b61e6ce4e
                                    d85f98411081017f2027876441c1492a
                                    a2647dc2b2e57cbd92c2fbd9d303b2f3
                                    dd5370a46fb60c19fd74f7c02e774533
                                    203db3954f8bbf8cb2ff484c9c880d7f
                                    f4ea614bbb61dec7099e968b95169bf4
                                    93fede61289f00a62101962db4170dd9
                                    2329ebec0bb6eb4a2ab77d679ea070be
                                    437845e748ceaead6279d3cafcd9a374
                                    6d72d75725bc79fa47c5aa30bb1c0944
                                    c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                    147650d36f064f6b5dbbe8f04077d983



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 32)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 0
```

```
   L2 blocks MSG(padded)  = 2
                                        BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101121314 15
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =
   MSG =                           01000000000000000000000000000000
                                   02000000000000000000000000000000

   PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                   02000000000000000000000000000000
   LENBLK =                        00000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                       0100000000000000046020000f0507615
   POLYVAL_xor_NONCE  =            0200000000000000046020000f0507615
   with MSBit cleared =            0200000000000000046020000f0507615
   TAG =                           78a50cb3f901ee38c588f6662d785a24
   AAD =
   CT  =                           ebb355fb913c781bee9ea36ff920193f
                                   80c8aa6d0abd197f039be49616f62e4f
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                 01000000000000000000000000000000
                                   02000000000000000000000000000000

   TAG' =                          78a50cb3f901ee38c588f6662d785a24

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
```

```
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  78a50cb3f901ee38c588f6662d785aa4
                                  79a50cb3f901ee38c588f6662d785aa4



   --------------------- TWO_KEYS     (AAD = 0, MSG = 48)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 3
                                             BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =
   MSG =                          01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
   LENBLK =                       00000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                      0e000000000000000650300203e788f7f
   POLYVAL_xor_NONCE  =           0d000000000000000650300203e788f7f
   with MSBit cleared =           0d000000000000000650300203e788f7f
   TAG =                          a75aa62b704e826d984a72184e370598
   AAD =
   CT  =                          5cf01ee258867977c0dd93dc33c9ccaf
                                  fcf088d95bb3d17221cfb58f2cd14703
                                  068463f2c0a18185cd745bcaf7b72ed5
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e
```

```
   Performing Decryption and
   Authentication:

   Decrypted MSG =                 010000000000000000000000000000000
                                   020000000000000000000000000000000
                                   030000000000000000000000000000000

   TAG' =                          a75aa62b704e826d984a72184e370598

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   a75aa62b704e826d984a72184e370598
                                   a85aa62b704e826d984a72184e370598
                                   a95aa62b704e826d984a72184e370598



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 64)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 4
                                               BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
```

```
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =
   MSG =                           01000000000000000000000000000000
                                   02000000000000000000000000000000
                                   03000000000000000000000000000000
                                   04000000000000000000000000000000
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                   02000000000000000000000000000000
                                   03000000000000000000000000000000
                                   04000000000000000000000000000000
   LENBLK =                        00000000000000000020000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                       0f000000000000008c04c04c63ad584f
   POLYVAL_xor_NONCE  =            0c000000000000008c04c04c63ad584f
   with MSBit cleared =            0c000000000000008c04c04c63ad584f
   TAG =                           d7f4efe2f6c72e3b8df168cab6b790ab
   AAD =
   CT  =                           442acedd0154ad46741b42ea12bd76b6
                                   6f3f13e79c89e88fc0d0651ab70aa474
                                   226f538c660d95f0867dc65d7c0b0af6
                                   17339e1db42294b52b4ab4fc06234769
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                 01000000000000000000000000000000
                                   02000000000000000000000000000000
                                   03000000000000000000000000000000
                                   04000000000000000000000000000000

   TAG' =                          d7f4efe2f6c72e3b8df168cab6b790ab

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
```

```
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafcd9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                d7f4efe2f6c72e3b8df168cab6b790ab
                                d8f4efe2f6c72e3b8df168cab6b790ab
                                d9f4efe2f6c72e3b8df168cab6b790ab
                                daf4efe2f6c72e3b8df168cab6b790ab



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 8)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB--------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        0200000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     08000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    13000000000000080910000000f0501631
   POLYVAL_xor_NONCE  =         10000000000000080910000000f0501631
   with MSBit cleared =         10000000000000080910000000f0501631
   TAG =                        633c11b2eee1f65be0e3f1e0c824c5e0
   AAD =                        01
   CT  =                        b3aa6df500d38f0f
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e
```

```
   Performing Decryption and
   Authentication:

   Decrypted MSG =                0200000000000000

   TAG' =                         633c11b2eee1f65be0e3f1e0c824c5e0

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  633c11b2eee1f65be0e3f1e0c824c5e0



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 12)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                                BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01
```

```
   MSG =                          02000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       08000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      1300000000000040d9000000f0501631
   POLYVAL_xor_NONCE  =           1000000000000040d9000000f0501631
   with MSBit cleared =           1000000000000040d9000000f0501631
   TAG =                          f229e75b2c4c3048fc70f163c9aefe0d
   AAD =                          01
   CT  =                          b5bea0352fbe77e5dc84aac4
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                02000000000000000000000

   TAG' =                         f229e75b2c4c3048fc70f163c9aefe0d

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  f229e75b2c4c3048fc70f163c9aefe8d


   ---------------------- TWO_KEYS     (AAD = 1, MSG = 16)---------

   AAD_byte_len = 1
```

```
   AAD_bit_len  = 8
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01
   MSG =                          02000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000

   LENBLK =                       08000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      13000000000000000023010000f0501631
   POLYVAL_xor_NONCE  =           10000000000000000023010000f0501631
   with MSBit cleared =           10000000000000000023010000f0501631
   TAG =                          cfb5aa16cdd9d39acc5d99b6eee2c6fc
   AAD =                          01
   CT  =                          86f7d1853ecc302a598c0e054d917a9c
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                02000000000000000000000000000000

   TAG' =                         cfb5aa16cdd9d39acc5d99b6eee2c6fc

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
```

```
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafcd9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                cfb5aa16cdd9d39acc5d99b6eee2c6fc



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 32)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 2
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   LENBLK =                     08000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                    1c00000000000000460200203e78ef5b
   POLYVAL_xor_NONCE  =         1f00000000000000460200203e78ef5b
   with MSBit cleared =         1f00000000000000460200203e78ef5b
   TAG =                        8df5606f057468e4b38e89736255ad2d
   AAD =                        01
   CT  =                        a58e74cc44de5637d02d800119da54c1
                                df3f9f8a1930953819a7d8d1d76f10c0
   Encryption_Key=              57d4b7aec8de993e30a6861b61e6ce4e
```

```
   Performing Decryption and
   Authentication:

   Decrypted MSG =                 020000000000000000000000000000000
                                   030000000000000000000000000000000

   TAG' =                          8df5606f057468e4b38e89736255ad2d

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   8df5606f057468e4b38e89736255adad
                                   8ef5606f057468e4b38e89736255adad



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 48)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 3
                                             BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        030000000000000000000000000000000
   K2 = K =                        010000000000000000000000000000000
```

```
   NONCE =                          030000000000000000000000000000
   AAD =                            01
   MSG =                            020000000000000000000000000000000
                                    030000000000000000000000000000000
                                    040000000000000000000000000000000
   PADDED_AAD_and_MSG =             010000000000000000000000000000000
                                    020000000000000000000000000000000
                                    030000000000000000000000000000000
                                    040000000000000000000000000000000
   LENBLK =                         080000000000000080010000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                        1d00000000000006503c04c63ad386b
   POLYVAL_xor_NONCE  =             1e00000000000006503c04c63ad386b
   with MSBit cleared =             1e00000000000006503c04c63ad386b
   TAG =                            b52274e14d6111c74edf5d95855256a2
   AAD =                            01
   CT  =                            9ceaefd1522cc88b1a9dde5f86253b70
                                    309a25c160bb37dc677ed126ce23e7ab
                                    31ea937735d6353af5cf02de8ff5b2ff
   Encryption_Key=                  57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                  020000000000000000000000000000000
                                    030000000000000000000000000000000
                                    040000000000000000000000000000000

   TAG' =                           b52274e14d6111c74edf5d95855256a2

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    57d4b7aec8de993e30a6861b61e6ce4e
                                    d85f98411081017f2027876441c1492a
                                    a2647dc2b2e57cbd92c2fbd9d303b2f3
                                    dd5370a46fb60c19fd74f7c02e774533
                                    203db3954f8bbf8cb2ff484c9c880d7f
                                    f4ea614bbb61dec7099e968b95169bf4
                                    93fede61289f00a62101962db4170dd9
                                    2329ebec0bb6eb4a2ab77d679ea070be
                                    437845e748ceaead6279d3cafcd9a374
                                    6d72d75725bc79fa47c5aa30bb1c0944
                                    c773ccbde2cfb547a50a1f771e161633
```

```
   CTRBLKS (with MSbit set to 1)

                                b52274e14d6111c74edf5d95855256a2
                                b62274e14d6111c74edf5d95855256a2
                                b72274e14d6111c74edf5d95855256a2



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 64)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 4
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
                                05000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
                                05000000000000000000000000000000
   LENBLK =                     08000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 5 blocks + LENBLK.
   POLYVAL =                    1b000000000000008c841a01712a376e
   POLYVAL_xor_NONCE  =         18000000000000008c841a01712a376e
   with MSBit cleared =         18000000000000008c841a01712a376e
   TAG =                        668fc00b6b40b4bb0c8d6cdb9730358d
   AAD =                        01
   CT  =                        457e976e1f62be30a2bfb8d8801b7282
                                8dd5349701b0f93007bcae4c2daed6fa
                                d91c3ae1751edaf54abf47bb1f0608dd
                                2961c86e7860dcb75336be054c1ad6cf
```

```
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                 02000000000000000000000000000000
                                   03000000000000000000000000000000
                                   04000000000000000000000000000000
                                   05000000000000000000000000000000

   TAG' =                          668fc00b6b40b4bb0c8d6cdb9730358d

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   668fc00b6b40b4bb0c8d6cdb9730358d
                                   678fc00b6b40b4bb0c8d6cdb9730358d
                                   688fc00b6b40b4bb0c8d6cdb9730358d
                                   698fc00b6b40b4bb0c8d6cdb9730358d



   ---------------------- TWO_KEYS     (AAD = 12, MSG = 4)---------

   AAD_byte_len = 12
   AAD_bit_len  = 96
   MSG_byte_len = 4
   MSG_bit_len  = 32
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
```

```
                                        BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =                           01000000000000000000000
   MSG =                           02000000
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                   02000000000000000000000000000000

   LENBLK =                        60000000000000002000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                       d8000000000000c048000000f050f665
   POLYVAL_xor_NONCE  =            db000000000000c048000000f050f665
   with MSBit cleared =            db000000000000c048000000f050f665
   TAG =                           488346eaebe2d64ffa58e0fa82f8cd43
   AAD =                           01000000000000000000000
   CT  =                           c2b96956
   Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                 02000000

   TAG' =                          488346eaebe2d64ffa58e0fa82f8cd43

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)
```

488346eaebe2d64ffa58e0fa82f8cdc3

---------- TWO_KEYS (AAD = 18, MSG = 20)---------

AAD_byte_len = 18
AAD_bit_len = 144
MSG_byte_len = 20
MSG_bit_len = 160
padded_AAD_byte_len = 32
padded_MSG_byte_len = 32
L1 blocks AAD(padded) = 2
L2 blocks MSG(padded) = 2

BYTES ORDER
LSB-------------------------MSB
000102030405060708090101121314 15

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
0200
MSG = 03000000000000000000000000000000
04000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 90000000000000a000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 08010000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b010000000000c06b01c04c63ad9807
with MSBit cleared = 0b010000000000c06b01c04c63ad9807
TAG = d010794cfdbbc65ef641b8ccb9c2dda3
AAD = 01000000000000000000000000000000
0200
CT = 348bf14b0fe2f8a2c3e843429df6276c
c0e5e688
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

Performing Decryption and
Authentication:

Decrypted MSG = 03000000000000000000000000000000
04000000

```
   TAG' =                          d010794cfdbbc65ef641b8ccb9c2dda3

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)   57d4b7aec8de993e30a6861b61e6ce4e
                                   d85f98411081017f2027876441c1492a
                                   a2647dc2b2e57cbd92c2fbd9d303b2f3
                                   dd5370a46fb60c19fd74f7c02e774533
                                   203db3954f8bbf8cb2ff484c9c880d7f
                                   f4ea614bbb61dec7099e968b95169bf4
                                   93fede61289f00a62101962db4170dd9
                                   2329ebec0bb6eb4a2ab77d679ea070be
                                   437845e748ceaead6279d3cafcd9a374
                                   6d72d75725bc79fa47c5aa30bb1c0944
                                   c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                   d010794cfdbbc65ef641b8ccb9c2dda3
                                   d110794cfdbbc65ef641b8ccb9c2dda3



   ---------------------- TWO_KEYS     (AAD = 20, MSG = 18)---------

   AAD_byte_len = 20
   AAD_bit_len  = 160
   MSG_byte_len = 18
   MSG_bit_len  = 144
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                             BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =                           01000000000000000000000000000000
                                   02000000
   MSG =                           03000000000000000000000000000000
                                   0400
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
```

```
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
   LENBLK =                       a0000000000000090000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                      640100000000000600701c04c63add8de
   POLYVAL_xor_NONCE  =           670100000000000600701c04c63add8de
   with MSBit cleared =           670100000000000600701c04c63add85e
   TAG =                          98e16515942fb8ff9ef108e7ce53a963
   AAD =                          01000000000000000000000000000000
                                  02000000
   CT  =                          f803a8b63ffa8c44a391c7e4ccc31e61
                                  79d1
   Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

   Performing Decryption and
   Authentication:

   Decrypted MSG =                03000000000000000000000000000000
                                  0400

   TAG' =                         98e16515942fb8ff9ef108e7ce53a963

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                  d85f98411081017f2027876441c1492a
                                  a2647dc2b2e57cbd92c2fbd9d303b2f3
                                  dd5370a46fb60c19fd74f7c02e774533
                                  203db3954f8bbf8cb2ff484c9c880d7f
                                  f4ea614bbb61dec7099e968b95169bf4
                                  93fede61289f00a62101962db4170dd9
                                  2329ebec0bb6eb4a2ab77d679ea070be
                                  437845e748ceaead6279d3cafcd9a374
                                  6d72d75725bc79fa47c5aa30bb1c0944
                                  c773ccbde2cfb547a50a1f771e161633

   CTRBLKS (with MSbit set to 1)

                                  98e16515942fb8ff9ef108e7ce53a9e3
                                  99e16515942fb8ff9ef108e7ce53a9e3
```

A.2. AEAD_AES_256_GCM_SIV

```
---------------------- TWO_KEYS     (AAD = 0, MSG = 0)---------

AAD_byte_len = 0
AAD_bit_len  = 0
MSG_byte_len = 0
MSG_bit_len  = 0
padded_AAD_byte_len = 0
padded_MSG_byte_len = 0
L1 blocks AAD(padded)  = 0
L2 blocks MSG(padded)  = 0
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
                                00000000000000000000000000000000

NONCE =                         03000000000000000000000000000000
AAD =
MSG =
PADDED_AAD_and_MSG =
LENBLK =                        00000000000000000000000000000000

Computing POLYVAL on a
buffer of 0 blocks + LENBLK.
POLYVAL =                       00000000000000000000000000000000
POLYVAL_xor_NONCE  =            03000000000000000000000000000000
with MSBit cleared =            03000000000000000000000000000000
TAG =                           9f32298b78fb3a5e42a41f9ec395a8a0
AAD =
CT  =
Encryption_Key =                5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

**************************
         APPENDIX
**************************
KEY_SCHEDULE (Encryption_Key)   01000000000000000000000000000000
                                00000000000000000000000000000000
                                63636363636363636363636363636363
                                fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                2c8d8d8dd77676762c8d8d8dd7767676
                                525454625f5b5b6d313737013c38380e
                                c78a8a2610fcfc503c7171ddeb0707ab
                                9f91368bc0ca6de6f1fd5ae7cdc562e9
```

```
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 8)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                            BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =
   MSG =                          0100000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
   LENBLK =                       00000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                      04000000000000809100000000283b1c
   POLYVAL_xor_NONCE  =           07000000000000809100000000283b1c
   with MSBit cleared =           07000000000000809100000000283b1c
   TAG =                          ca9daafe8fe6f1f97d5d37780af4d423
   AAD =
   CT  =                          403c53d07ec9ff2c
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
```

```
   **************************
   KEY_SCHEDULE (Encryption_Key)   010000000000000000000000000000000
                                   000000000000000000000000000000000
                                   636363636363636363636363636363636
                                   fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                   6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                   2c8d8d8dd77676762c8d8d8dd7767676
                                   525454625f5b5b6d313737013c38380e
                                   c78a8a2610fcfc503c7171ddeb0707ab
                                   9f91368bc0ca6de6f1fd5ae7cdc562e9
                                   7a2c20386ad0dc6856a1adb5bda6aa1e
                                   ab3d44f16bf729179a0a73f057cf1119
                                   21a6a2ec4b767e841dd7d331a071792f
                                   288b5111437c7806d9760bf68eb91aef
                                   38f0003373867eb76e51ad86ce20d4a9
                                   dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                   ca9daafe8fe6f1f97d5d37780af4d4a3



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 12)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                              BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        030000000000000000000000000000000
   K2 = K =                        010000000000000000000000000000000
                                   000000000000000000000000000000000

   NONCE =                         030000000000000000000000000000000
   AAD =
   MSG =                           010000000000000000000000
   PADDED_AAD_and_MSG =            010000000000000000000000000000000
   LENBLK =                        000000000000000060000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
```

```
   POLYVAL =                        040000000000040d900000000283b1c
   POLYVAL_xor_NONCE  =             070000000000040d900000000283b1c
   with MSBit cleared =             070000000000040d900000000283b1c
   TAG =                            675861642d6f7c42973d470843868600
   AAD =
   CT  =                            0a5bcaa698b9cc0bc78383cf
   Encryption_Key =                 5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    010000000000000000000000000000000
                                    000000000000000000000000000000000
                                    636363636363636363636363636363636
                                    fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                    6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                    2c8d8d8dd77676762c8d8d8dd7767676
                                    525454625f5b5b6d313737013c38380e
                                    c78a8a2610fcfc503c7171ddeb0707ab
                                    9f91368bc0ca6de6f1fd5ae7cdc562e9
                                    7a2c20386ad0dc6856a1adb5bda6aa1e
                                    ab3d44f16bf729179a0a73f057cf1119
                                    21a6a2ec4b767e841dd7d331a071792f
                                    288b5111437c7806d9760bf68eb91aef
                                    38f0003373867eb76e51ad86ce20d4a9
                                    dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                    675861642d6f7c42973d470843868680



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 16)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                              BYTES ORDER
                                    LSB--------------------------MSB
                                    000102030405060708090101112131415
                                    --------------------------------
```

```
   K1 = H =                         03000000000000000000000000000000
   K2 = K =                         01000000000000000000000000000000
                                    00000000000000000000000000000000
   NONCE =                          03000000000000000000000000000000
   AAD =
   MSG =                            01000000000000000000000000000000
   PADDED_AAD_and_MSG =             01000000000000000000000000000000
   LENBLK =                         00000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                        040000000000000023010000000283b1c
   POLYVAL_xor_NONCE  =             070000000000000023010000000283b1c
   with MSBit cleared =             070000000000000023010000000283b1c
   TAG =                            255656d6213ddf996629d0c9db7c6332
   AAD =
   CT  =                            dfde1d2f762281c138f9d6d09203a270
   Encryption_Key =                 5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    01000000000000000000000000000000
                                    00000000000000000000000000000000
                                    63636363636363636363636363636363
                                    fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                    6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                    2c8d8d8dd77676762c8d8d8dd7767676
                                    525454625f5b5b6d313737013c38380e
                                    c78a8a2610fcfc503c7171ddeb0707ab
                                    9f91368bc0ca6de6f1fd5ae7cdc562e9
                                    7a2c20386ad0dc6856a1adb5bda6aa1e
                                    ab3d44f16bf729179a0a73f057cf1119
                                    21a6a2ec4b767e841dd7d331a071792f
                                    288b5111437c7806d9760bf68eb91aef
                                    38f0003373867eb76e51ad86ce20d4a9
                                    dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                    255656d6213ddf996629d0c9db7c63b2


   ---------------------- TWO_KEYS     (AAD = 0, MSG = 32)---------

   AAD_byte_len = 0
```

```
   AAD_bit_len  = 0
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 2
                                        BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =
   MSG =                          01000000000000000000000000000000
                                  02000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       00000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      01000000000000004602000f0507615
   POLYVAL_xor_NONCE  =           02000000000000004602000f0507615
   with MSBit cleared =           02000000000000004602000f0507615
   TAG =                          796e2bdd844cff0aac06f4b85a36d66b
   AAD =
   CT  =                          c680d1f9a3f2807ce9debce4bf670a98
                                  680619480f725d06ed91dbcbad65d07a
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  01000000000000000000000000000000
                                  00000000000000000000000000000000
                                  63636363636363636363636363636363
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
```

```
                                21a6a2ec4b767e841dd7d331a071792f
                                288b5111437c7806d9760bf68eb91aef
                                38f0003373867eb76e51ad86ce20d4a9
                                dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                796e2bdd844cff0aac06f4b85a36d6eb
                                7a6e2bdd844cff0aac06f4b85a36d6eb



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 48)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 3
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   LENBLK =                     00000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                    0e000000000000000650300203e788f7f
   POLYVAL_xor_NONCE  =         0d000000000000000650300203e788f7f
   with MSBit cleared =         0d000000000000000650300203e788f7f
   TAG =                        0457372a01c505a8718751a8f4c07958
   AAD =
   CT  =                        f5e1b0e6f6113e5d4a87ff54d0c6994e
                                d1d702f63a63c9f132a7317bdb085dd8
```

```
                                  856fba3e70f5ebe2857de62946bd984b
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  010000000000000000000000000000000
                                  000000000000000000000000000000000
                                  636363636363636363636363636363636
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                  0457372a01c505a8718751a8f4c079d8
                                  0557372a01c505a8718751a8f4c079d8
                                  0657372a01c505a8718751a8f4c079d8



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 64)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 4
                                             BYTES ORDER
                                  LSB--------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       030000000000000000000000000000000
   K2 = K =                       010000000000000000000000000000000
                                  000000000000000000000000000000000
```

```
   NONCE =                          03000000000000000000000000000000
   AAD =
   MSG =                            01000000000000000000000000000000
                                    02000000000000000000000000000000
                                    03000000000000000000000000000000
                                    04000000000000000000000000000000
   PADDED_AAD_and_MSG =             01000000000000000000000000000000
                                    02000000000000000000000000000000
                                    03000000000000000000000000000000
                                    04000000000000000000000000000000
   LENBLK =                         00000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                        0f000000000000008c04c04c63ad584f
   POLYVAL_xor_NONCE  =             0c000000000000008c04c04c63ad584f
   with MSBit cleared =             0c000000000000008c04c04c63ad584f
   TAG =                            0b188a792d0a940e66f50e37bf7f9810
   AAD =
   CT  =                            f32c3b7315f699ee449b3709fbd109fd
                                    c1726c48a8c48c5b19268372bc83919f
                                    9a717c2b7b042d33a75e4d0806c05f63
                                    5ad443dc419749efe8c4dec48f6d4254
   Encryption_Key =                 5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)    01000000000000000000000000000000
                                    00000000000000000000000000000000
                                    63636363636363636363636363636363
                                    fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                    6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                    2c8d8d8dd77676762c8d8d8dd7767676
                                    525454625f5b5b6d313737013c38380e
                                    c78a8a2610fcfc503c7171ddeb0707ab
                                    9f91368bc0ca6de6f1fd5ae7cdc562e9
                                    7a2c20386ad0dc6856a1adb5bda6aa1e
                                    ab3d44f16bf729179a0a73f057cf1119
                                    21a6a2ec4b767e841dd7d331a071792f
                                    288b5111437c7806d9760bf68eb91aef
                                    38f0003373867eb76e51ad86ce20d4a9
                                    dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                    0b188a792d0a940e66f50e37bf7f9890
```

```
                                0c188a792d0a940e66f50e37bf7f9890
                                0d188a792d0a940e66f50e37bf7f9890
                                0e188a792d0a940e66f50e37bf7f9890


   --------------------- TWO_KEYS     (AAD = 1, MSG = 8)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        0200000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     08000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    13000000000000080910000000f0501631
   POLYVAL_xor_NONCE  =         10000000000000080910000000f0501631
   with MSBit cleared =         10000000000000080910000000f0501631
   TAG =                        6bc14bd99e1dc3de41371ee4012d84be
   AAD =                        01
   CT  =                        7b10160344fec6cb
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)01000000000000000000000000000000
                                00000000000000000000000000000000
                                63636363636363636363636363636363
                                fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
```

```
                                6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                2c8d8d8dd77676762c8d8d8dd7767676
                                525454625f5b5b6d313737013c38380e
                                c78a8a2610fcfc503c7171ddeb0707ab
                                9f91368bc0ca6de6f1fd5ae7cdc562e9
                                7a2c20386ad0dc6856a1adb5bda6aa1e
                                ab3d44f16bf729179a0a73f057cf1119
                                21a6a2ec4b767e841dd7d331a071792f
                                288b5111437c7806d9760bf68eb91aef
                                38f0003373867eb76e51ad86ce20d4a9
                                dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                6bc14bd99e1dc3de41371ee4012d84be



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 12)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        020000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     08000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    1300000000000040d9000000f0501631
   POLYVAL_xor_NONCE  =         1000000000000040d9000000f0501631
   with MSBit cleared =         1000000000000040d9000000f0501631
   TAG =                        0707868473db0caa87ea08f1c44352c0
```

```
   AAD =                          01
   CT  =                          75ffe5c8403db5fb479bc58b
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  010000000000000000000000000000000
                                  000000000000000000000000000000000
                                  636363636363636363636363636363636
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                  0707868473db0caa87ea08f1c44352c0



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 16)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                                BYTES ORDER
                                  LSB--------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       030000000000000000000000000000000
   K2 = K =                       010000000000000000000000000000000
                                  000000000000000000000000000000000

   NONCE =                        030000000000000000000000000000000
```

```
   AAD =                          01
   MSG =                          02000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       08000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      13000000000000000023010000f0501631
   POLYVAL_xor_NONCE  =           10000000000000000023010000f0501631
   with MSBit cleared =           10000000000000000023010000f0501631
   TAG =                          35c13a7848f4f53530aeff0176344e05
   AAD =                          01
   CT  =                          a11196c1e68a743668290f75ed2f3bab
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  01000000000000000000000000000000
                                  00000000000000000000000000000000
                                  63636363636363636363636363636363
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                  35c13a7848f4f53530aeff0176344e85



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 32)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 32
   MSG_bit_len  = 256
```

```
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 2
                                        BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000

   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000

   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000

   LENBLK =                     08000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                    1c00000000000000460200203e78ef5b
   POLYVAL_xor_NONCE  =         1f00000000000000460200203e78ef5b
   with MSBit cleared =         1f00000000000000460200203e78ef5b
   TAG =                        900c57b053eac0245bb488688b3e0f5e
   AAD =                        01
   CT  =                        c0a77a0fd04b3e590a924d938167ffe7
                                659cd00ab7110b191376f8d8204e8f0d

   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  01000000000000000000000000000000
                                  00000000000000000000000000000000
                                  63636363636363636363636363636363
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
```

```
                                38f0003373867eb76e51ad86ce20d4a9
                                dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                900c57b053eac0245bb488688b3e0fde
                                910c57b053eac0245bb488688b3e0fde



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 48)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 3
                                            BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708091011121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     08000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                    1d00000000000006503c04c63ad386b
   POLYVAL_xor_NONCE  =         1e00000000000006503c04c63ad386b
   with MSBit cleared =         1e00000000000006503c04c63ad386b
   TAG =                        12b64759e738e2d0cf178cba52a9f1eb
   AAD =                        01
   CT  =                        4e5ec0cac887e6fa1473f19c7978eec8
                                a56c912d7a7505a35f96a41ad89bbf45
                                2adaebf19add7e50cec3776b97d22e29
```

```
   Encryption_Key =                5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   01000000000000000000000000000000
                                   00000000000000000000000000000000
                                   63636363636363636363636363636363
                                   fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                   6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                   2c8d8d8dd77676762c8d8d8dd7767676
                                   525454625f5b5b6d313737013c38380e
                                   c78a8a2610fcfc503c7171ddeb0707ab
                                   9f91368bc0ca6de6f1fd5ae7cdc562e9
                                   7a2c20386ad0dc6856a1adb5bda6aa1e
                                   ab3d44f16bf729179a0a73f057cf1119
                                   21a6a2ec4b767e841dd7d331a071792f
                                   288b5111437c7806d9760bf68eb91aef
                                   38f0003373867eb76e51ad86ce20d4a9
                                   dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                   12b64759e738e2d0cf178cba52a9f1eb
                                   13b64759e738e2d0cf178cba52a9f1eb
                                   14b64759e738e2d0cf178cba52a9f1eb



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 64)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 4
                                              BYTES ORDER
                                   LSB--------------------------MSB
                                   00010203040506070809101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
                                   00000000000000000000000000000000

   NONCE =                         03000000000000000000000000000000
```

```
   AAD =                          01
   MSG =                          02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
                                  05000000000000000000000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
                                  05000000000000000000000000000000
   LENBLK =                       08000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 5 blocks + LENBLK.
   POLYVAL =                      1b000000000000008c841a01712a376e
   POLYVAL_xor_NONCE  =           18000000000000008c841a01712a376e
   with MSBit cleared =           18000000000000008c841a01712a376e
   TAG =                          4df7461010574a2c5a5f8c428c9a05a8
   AAD =                          01
   CT  =                          ed5596b2ac560cace49f593154576284
                                  7608cc1cd4be937778e4bc1542ce749c
                                  ef0de63e87dda60a0d58c39d40698b31
                                  c4bb87167c528a8db89975496c1586c7
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  01000000000000000000000000000000
                                  00000000000000000000000000000000
                                  63636363636363636363636363636363
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                  4df7461010574a2c5a5f8c428c9a05a8
```

```
                                4ef7461010574a2c5a5f8c428c9a05a8
                                4ff7461010574a2c5a5f8c428c9a05a8
                                50f7461010574a2c5a5f8c428c9a05a8


   ---------------------- TWO_KEYS     (AAD = 12, MSG = 4)---------

   AAD_byte_len = 12
   AAD_bit_len  = 96
   MSG_byte_len = 4
   MSG_bit_len  = 32
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        010000000000000000000000
   MSG =                        02000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     60000000000000002000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    d8000000000000c048000000f050f665
   POLYVAL_xor_NONCE  =         db000000000000c048000000f050f665
   with MSBit cleared =         db000000000000c048000000f050f665
   TAG =                        ff5ad2f9cbb36b1237cdbd63afb89d36
   AAD =                        010000000000000000000000
   CT  =                        7904ab1d
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)01000000000000000000000000000000
                                00000000000000000000000000000000
                                63636363636363636363636363636363
                                fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
```

```
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                  ff5ad2f9cbb36b1237cdbd63afb89db6



   ---------------------- TWO_KEYS     (AAD = 18, MSG = 20)---------

   AAD_byte_len = 18
   AAD_bit_len  = 144
   MSG_byte_len = 20
   MSG_bit_len  = 160
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                             BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01000000000000000000000000000000
                                  0200
   MSG =                          03000000000000000000000000000000
                                  04000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
   LENBLK =                       9000000000000000a000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
```

```
   POLYVAL =                       08010000000000c06b01c04c63ad9807
   POLYVAL_xor_NONCE  =            0b010000000000c06b01c04c63ad9807
   with MSBit cleared =            0b010000000000c06b01c04c63ad9807
   TAG =                           19ff544d26d5f871b697767d0e1b7881
   AAD =                           01000000000000000000000000000000
                                   0200
   CT  =                           e6daeb5dd348a30936888ae23cc38783
                                   378c7134
   Encryption_Key =                5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   01000000000000000000000000000000
                                   00000000000000000000000000000000
                                   63636363636363636363636363636363
                                   fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                   6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                   2c8d8d8dd77676762c8d8d8dd7767676
                                   525454625f5b5b6d313737013c38380e
                                   c78a8a2610fcfc503c7171ddeb0707ab
                                   9f91368bc0ca6de6f1fd5ae7cdc562e9
                                   7a2c20386ad0dc6856a1adb5bda6aa1e
                                   ab3d44f16bf729179a0a73f057cf1119
                                   21a6a2ec4b767e841dd7d331a071792f
                                   288b5111437c7806d9760bf68eb91aef
                                   38f0003373867eb76e51ad86ce20d4a9
                                   dfc3829a9cbffa9c45c9f16acb70eb85

   CTRBLKS (with MSbit set to 1)

                                   19ff544d26d5f871b697767d0e1b7881
                                   1aff544d26d5f871b697767d0e1b7881



   ---------------------- TWO_KEYS     (AAD = 20, MSG = 18)---------

   AAD_byte_len = 20
   AAD_bit_len  = 160
   MSG_byte_len = 18
   MSG_bit_len  = 144
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                              BYTES ORDER
```

```
                                LSB-------------------------MSB
                                000102030405060708091011121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000

   NONCE =                      03000000000000000000000000000000
   AAD =                        01000000000000000000000000000000
                                02000000

   MSG =                        03000000000000000000000000000000
                                0400

   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     a0000000000000009000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                    640100000000000600701c04c63add8de
   POLYVAL_xor_NONCE  =         670100000000000600701c04c63add8de
   with MSBit cleared =         670100000000000600701c04c63add85e
   TAG =                        474ed2b302caba5f9460075bf577d777
   AAD =                        01000000000000000000000000000000
                                02000000
   CT  =                        1887531c24feb67e83067aa634f4106f
                                9580
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  01000000000000000000000000000000
                                  00000000000000000000000000000000
                                  63636363636363636363636363636363
                                  fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
                                  6e6c6c6c0d0f0f0f6e6c6c6c0d0f0f0f
                                  2c8d8d8dd77676762c8d8d8dd7767676
                                  525454625f5b5b6d313737013c38380e
                                  c78a8a2610fcfc503c7171ddeb0707ab
                                  9f91368bc0ca6de6f1fd5ae7cdc562e9
                                  7a2c20386ad0dc6856a1adb5bda6aa1e
                                  ab3d44f16bf729179a0a73f057cf1119
                                  21a6a2ec4b767e841dd7d331a071792f
                                  288b5111437c7806d9760bf68eb91aef
                                  38f0003373867eb76e51ad86ce20d4a9
                                  dfc3829a9cbffa9c45c9f16acb70eb85
```

```
   CTRBLKS (with MSbit set to 1)

                                 474ed2b302caba5f9460075bf577d7f7
                                 484ed2b302caba5f9460075bf577d7f7



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 0)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 0
   MSG_bit_len  = 0
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 0
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 0
                                           BYTES ORDER
                                 LSB--------------------------MSB
                                 000102030405060708090101112131415
                                 --------------------------------
   K1 = H =                      03000000000000000000000000000000
   K2 = K =                      01000000000000000000000000000000
                                 00000000000000000000000000000000

   NONCE =                       03000000000000000000000000000000
   AAD =
   MSG =
   PADDED_AAD_and_MSG =
   LENBLK =                      00000000000000000000000000000000

   Computing POLYVAL on a
   buffer of 0 blocks + LENBLK.
   POLYVAL =                     00000000000000000000000000000000
   POLYVAL_xor_NONCE  =          03000000000000000000000000000000
   with MSBit cleared =          03000000000000000000000000000000
   TAG =                         9f32298b78fb3a5e42a41f9ec395a8a0
   AAD =
   CT  =
   Encryption_Key =              5f377914db056de594bd23b0f07076be
                                 c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =

   TAG' =                        9f32298b78fb3a5e42a41f9ec395a8a0
```

```
   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae
                                   49d19dab92d4f04e0669d3fef619a540
                                   8a5333c671cace9aa502cb4651853ee8
                                   dc63067a4eb7f63448de25cabec7808a
                                   2495feb8555f3022f05dfb64a1d8c58c
                                   b9c56248f772947cbfacb1b6016b313c
                                   58ea39530db50971fde8f2155c303799
                                   b55f8c02422d187efd81a9c8fcea98f4
                                   e86d7fece5d8769d183084884400b311
                                   c6320e19841f1667799ebfaf8574275b
                                   7fffb3d59a27c548821741c0c617f2d1
                                   16bb30ad92a426caeb3a99656e4ebe3e
                                   e0d01d677af7d82ff8e099ef3ef76b3e
                                   3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 8)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                              BYTES ORDER
                                   LSB-------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
                                   00000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
   AAD =
   MSG =                           0100000000000000
   PADDED_AAD_and_MSG =            01000000000000000000000000000000
   LENBLK =                        00000000000000004000000000000000
```

```
   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                        040000000000008091000000000283b1c
   POLYVAL_xor_NONCE  =             070000000000008091000000000283b1c
   with MSBit cleared =             070000000000008091000000000283b1c
   TAG =                            ca9daafe8fe6f1f97d5d37780af4d423
   AAD =
   CT  =                            403c53d07ec9ff2c
   Encryption_Key =                 5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                  0100000000000000

   TAG' =                           ca9daafe8fe6f1f97d5d37780af4d423

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)    5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae
                                    49d19dab92d4f04e0669d3fef619a540
                                    8a5333c671cace9aa502cb4651853ee8
                                    dc63067a4eb7f63448de25cabec7808a
                                    2495feb8555f3022f05dfb64a1d8c58c
                                    b9c56248f772947cbfacb1b6016b313c
                                    58ea39530db50971fde8f2155c303799
                                    b55f8c02422d187efd81a9c8fcea98f4
                                    e86d7fece5d8769d183084884400b311
                                    c6320e19841f1667799ebfaf8574275b
                                    7fffb3d59a27c548821741c0c617f2d1
                                    16bb30ad92a426caeb3a99656e4ebe3e
                                    e0d01d677af7d82ff8e099ef3ef76b3e
                                    3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                    ca9daafe8fe6f1f97d5d37780af4d4a3


   --------------------- TWO_KEYS     (AAD = 0, MSG = 12)---------

   AAD_byte_len = 0
```

```
   AAD_bit_len  = 0
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                        BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
   LENBLK =                     00000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                    040000000000040d900000000283b1c
   POLYVAL_xor_NONCE  =         070000000000040d900000000283b1c
   with MSBit cleared =         070000000000040d900000000283b1c
   TAG =                        675861642d6f7c42973d470843868600
   AAD =
   CT  =                        0a5bcaa698b9cc0bc78383cf
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              01000000000000000000000

   TAG' =                       675861642d6f7c42973d470843868600

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae
                                   49d19dab92d4f04e0669d3fef619a540
                                   8a5333c671cace9aa502cb4651853ee8
                                   dc63067a4eb7f63448de25cabec7808a
```

```
                                2495feb8555f3022f05dfb64a1d8c58c
                                b9c56248f772947cbfacb1b6016b313c
                                58ea39530db50971fde8f2155c303799
                                b55f8c02422d187efd81a9c8fcea98f4
                                e86d7fece5d8769d183084884400b311
                                c6320e19841f1667799ebfaf8574275b
                                7fffb3d59a27c548821741c0c617f2d1
                                16bb30ad92a426caeb3a99656e4ebe3e
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                675861642d6f7c42973d470843868680



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 16)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 1
                                            BYTES ORDER
                                LSB--------------------------MSB
                                00010203040506070809101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
   LENBLK =                     00000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 1 blocks + LENBLK.
   POLYVAL =                    04000000000000002301000000283b1c
   POLYVAL_xor_NONCE  =         07000000000000002301000000283b1c
   with MSBit cleared =         07000000000000002301000000283b1c
   TAG =                        255656d6213ddf996629d0c9db7c6332
   AAD =
   CT  =                        dfde1d2f762281c138f9d6d09203a270
```

```
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                01000000000000000000000000000000

   TAG' =                         255656d6213ddf996629d0c9db7c6332

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
                                  e0d01d677af7d82ff8e099ef3ef76b3e
                                  3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                  255656d6213ddf996629d0c9db7c63b2



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 32)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 32
   MSG_bit_len  = 256
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 2
                                              BYTES ORDER
```

```
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000

   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000

   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000

   LENBLK =                     00000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    01000000000000004602000 0f0507615
   POLYVAL_xor_NONCE  =         02000000000000004602000 0f0507615
   with MSBit cleared =         02000000000000004602000 0f0507615
   TAG =                        796e2bdd844cff0aac06f4b85a36d66b
   AAD =
   CT  =                        c680d1f9a3f2807ce9debce4bf670a98
                                680619480f725d06ed91dbcbad65d07a

   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              01000000000000000000000000000000
                                02000000000000000000000000000000

   TAG' =                       796e2bdd844cff0aac06f4b85a36d66b

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae
                                   49d19dab92d4f04e0669d3fef619a540
                                   8a5333c671cace9aa502cb4651853ee8
                                   dc63067a4eb7f63448de25cabec7808a
                                   2495feb8555f3022f05dfb64a1d8c58c
                                   b9c56248f772947cbfacb1b6016b313c
                                   58ea39530db50971fde8f2155c303799
                                   b55f8c02422d187efd81a9c8fcea98f4
```

```
                                e86d7fece5d8769d183084884400b311
                                c6320e19841f1667799ebfaf8574275b
                                7fffb3d59a27c548821741c0c617f2d1
                                16bb30ad92a426caeb3a99656e4ebe3e
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                796e2bdd844cff0aac06f4b85a36d6eb
                                7a6e2bdd844cff0aac06f4b85a36d6eb



   ---------------------- TWO_KEYS     (AAD = 0, MSG = 48)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 3
                                            BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
   LENBLK =                     00000000000000008001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                    0e0000000000000650300203e788f7f
   POLYVAL_xor_NONCE  =         0d0000000000000650300203e788f7f
   with MSBit cleared =         0d0000000000000650300203e788f7f
   TAG =                        0457372a01c505a8718751a8f4c07958
   AAD =
```

```
   CT  =                          f5e1b0e6f6113e5d4a87ff54d0c6994e
                                  d1d702f63a63c9f132a7317bdb085dd8
                                  856fba3e70f5ebe2857de62946bd984b
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000

   TAG' =                         0457372a01c505a8718751a8f4c07958

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
                                  e0d01d677af7d82ff8e099ef3ef76b3e
                                  3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                  0457372a01c505a8718751a8f4c079d8
                                  0557372a01c505a8718751a8f4c079d8
                                  0657372a01c505a8718751a8f4c079d8


   ---------------------- TWO_KEYS     (AAD = 0, MSG = 64)---------

   AAD_byte_len = 0
   AAD_bit_len  = 0
```

```
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 0
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 0
   L2 blocks MSG(padded)  = 4
                                        BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =
   MSG =                        01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     00000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                    0f000000000000008c04c04c63ad584f
   POLYVAL_xor_NONCE  =         0c000000000000008c04c04c63ad584f
   with MSBit cleared =         0c000000000000008c04c04c63ad584f
   TAG =                        0b188a792d0a940e66f50e37bf7f9810
   AAD =
   CT  =                        f32c3b7315f699ee449b3709fbd109fd
                                c1726c48a8c48c5b19268372bc83919f
                                9a717c2b7b042d33a75e4d0806c05f63
                                5ad443dc419749efe8c4dec48f6d4254
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000

   TAG' =                       0b188a792d0a940e66f50e37bf7f9810
```

```
   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae
                                   49d19dab92d4f04e0669d3fef619a540
                                   8a5333c671cace9aa502cb4651853ee8
                                   dc63067a4eb7f63448de25cabec7808a
                                   2495feb8555f3022f05dfb64a1d8c58c
                                   b9c56248f772947cbfacb1b6016b313c
                                   58ea39530db50971fde8f2155c303799
                                   b55f8c02422d187efd81a9c8fcea98f4
                                   e86d7fece5d8769d183084884400b311
                                   c6320e19841f1667799ebfaf8574275b
                                   7fffb3d59a27c548821741c0c617f2d1
                                   16bb30ad92a426caeb3a99656e4ebe3e
                                   e0d01d677af7d82ff8e099ef3ef76b3e
                                   3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                   0b188a792d0a940e66f50e37bf7f9890
                                   0c188a792d0a940e66f50e37bf7f9890
                                   0d188a792d0a940e66f50e37bf7f9890
                                   0e188a792d0a940e66f50e37bf7f9890



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 8)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 8
   MSG_bit_len  = 64
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                              BYTES ORDER
                                   LSB--------------------------MSB
                                   000102030405060708090101112131415
                                   --------------------------------
   K1 = H =                        03000000000000000000000000000000
   K2 = K =                        01000000000000000000000000000000
                                   00000000000000000000000000000000
   NONCE =                         03000000000000000000000000000000
```

```
   AAD =                          01
   MSG =                          0200000000000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       08000000000000004000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      13000000000000080910000000f0501631
   POLYVAL_xor_NONCE  =           10000000000000080910000000f0501631
   with MSBit cleared =           10000000000000080910000000f0501631
   TAG =                          6bc14bd99e1dc3de41371ee4012d84be
   AAD =                          01
   CT  =                          7b10160344fec6cb
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                0200000000000000

   TAG' =                         6bc14bd99e1dc3de41371ee4012d84be

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
                                  e0d01d677af7d82ff8e099ef3ef76b3e
                                  3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                  6bc14bd99e1dc3de41371ee4012d84be
```

```
   ---------------------- TWO_KEYS     (AAD = 1, MSG = 12)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 12
   MSG_bit_len  = 96
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     08000000000000006000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    1300000000000040d9000000f0501631
   POLYVAL_xor_NONCE  =         1000000000000040d9000000f0501631
   with MSBit cleared =         1000000000000040d9000000f0501631
   TAG =                        0707868473db0caa87ea08f1c44352c0
   AAD =                        01
   CT  =                        75ffe5c8403db5fb479bc58b
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              02000000000000000000000

   TAG' =                       0707868473db0caa87ea08f1c44352c0

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
```

```
                                c88735cffb99fd5cd4c805dcf487f5ae
                                49d19dab92d4f04e0669d3fef619a540
                                8a5333c671cace9aa502cb4651853ee8
                                dc63067a4eb7f63448de25cabec7808a
                                2495feb8555f3022f05dfb64a1d8c58c
                                b9c56248f772947cbfacb1b6016b313c
                                58ea39530db50971fde8f2155c303799
                                b55f8c02422d187efd81a9c8fcea98f4
                                e86d7fece5d8769d183084884400b311
                                c6320e19841f1667799ebfaf8574275b
                                7fffb3d59a27c548821741c0c617f2d1
                                16bb30ad92a426caeb3a99656e4ebe3e
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                0707868473db0caa87ea08f1c44352c0



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 16)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 16
   MSG_bit_len  = 128
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                            BYTES ORDER
                                LSB-------------------------MSB
                                00010203040506070809101112131415
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
   LENBLK =                     08000000000000008000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                    13000000000000000230100000f0501631
```

```
   POLYVAL_xor_NONCE  =           10000000000000023010000f0501631
   with MSBit cleared =           10000000000000023010000f0501631
   TAG =                          35c13a7848f4f53530aeff0176344e05
   AAD =                          01
   CT  =                          a11196c1e68a743668290f75ed2f3bab
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                02000000000000000000000000000000

   TAG' =                         35c13a7848f4f53530aeff0176344e05

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
                                  e0d01d677af7d82ff8e099ef3ef76b3e
                                  3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                  35c13a7848f4f53530aeff0176344e85



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 32)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 32
   MSG_bit_len  = 256
```

```
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 2
                                          BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000

   NONCE =                        03000000000000000000000000000000
   AAD =                          01
   MSG =                          02000000000000000000000000000000
                                  03000000000000000000000000000000

   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000

   LENBLK =                       08000000000000000001000000000000

   Computing POLYVAL on a
   buffer of 3 blocks + LENBLK.
   POLYVAL =                      1c00000000000000460200203e78ef5b
   POLYVAL_xor_NONCE  =           1f00000000000000460200203e78ef5b
   with MSBit cleared =           1f00000000000000460200203e78ef5b
   TAG =                          900c57b053eac0245bb488688b3e0f5e
   AAD =                          01
   CT  =                          c0a77a0fd04b3e590a924d938167ffe7
                                  659cd00ab7110b191376f8d8204e8f0d
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                02000000000000000000000000000000
                                  03000000000000000000000000000000

   TAG' =                         900c57b053eac0245bb488688b3e0f5e

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
```

```
                                8a5333c671cace9aa502cb4651853ee8
                                dc63067a4eb7f63448de25cabec7808a
                                2495feb8555f3022f05dfb64a1d8c58c
                                b9c56248f772947cbfacb1b6016b313c
                                58ea39530db50971fde8f2155c303799
                                b55f8c02422d187efd81a9c8fcea98f4
                                e86d7fece5d8769d183084884400b311
                                c6320e19841f1667799ebfaf8574275b
                                7fffb3d59a27c548821741c0c617f2d1
                                16bb30ad92a426caeb3a99656e4ebe3e
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                900c57b053eac0245bb488688b3e0fde
                                910c57b053eac0245bb488688b3e0fde



   ---------------------- TWO_KEYS     (AAD = 1, MSG = 48)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 48
   MSG_bit_len  = 384
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 48
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 3
                                           BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     08000000000000008001000000000000
```

```
   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                        1d00000000000006503c04c63ad386b
   POLYVAL_xor_NONCE  =             1e00000000000006503c04c63ad386b
   with MSBit cleared =             1e00000000000006503c04c63ad386b
   TAG =                            12b64759e738e2d0cf178cba52a9f1eb
   AAD =                            01
   CT  =                            4e5ec0cac887e6fa1473f19c7978eec8
                                    a56c912d7a7505a35f96a41ad89bbf45
                                    2adaebf19add7e50cec3776b97d22e29
   Encryption_Key =                 5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                  02000000000000000000000000000000
                                    03000000000000000000000000000000
                                    04000000000000000000000000000000

   TAG' =                           12b64759e738e2d0cf178cba52a9f1eb

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)    5f377914db056de594bd23b0f07076be
                                    c88735cffb99fd5cd4c805dcf487f5ae
                                    49d19dab92d4f04e0669d3fef619a540
                                    8a5333c671cace9aa502cb4651853ee8
                                    dc63067a4eb7f63448de25cabec7808a
                                    2495feb8555f3022f05dfb64a1d8c58c
                                    b9c56248f772947cbfacb1b6016b313c
                                    58ea39530db50971fde8f2155c303799
                                    b55f8c02422d187efd81a9c8fcea98f4
                                    e86d7fece5d8769d183084884400b311
                                    c6320e19841f1667799ebfaf8574275b
                                    7fffb3d59a27c548821741c0c617f2d1
                                    16bb30ad92a426caeb3a99656e4ebe3e
                                    e0d01d677af7d82ff8e099ef3ef76b3e
                                    3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                    12b64759e738e2d0cf178cba52a9f1eb
                                    13b64759e738e2d0cf178cba52a9f1eb
                                    14b64759e738e2d0cf178cba52a9f1eb
```

```
   ---------------------- TWO_KEYS     (AAD = 1, MSG = 64)---------

   AAD_byte_len = 1
   AAD_bit_len  = 8
   MSG_byte_len = 64
   MSG_bit_len  = 512
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 64
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 4
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01
   MSG =                        02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
                                05000000000000000000000000000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
                                05000000000000000000000000000000
   LENBLK =                     08000000000000000002000000000000

   Computing POLYVAL on a
   buffer of 5 blocks + LENBLK.
   POLYVAL =                    1b000000000000008c841a01712a376e
   POLYVAL_xor_NONCE  =         18000000000000008c841a01712a376e
   with MSBit cleared =         18000000000000008c841a01712a376e
   TAG =                        4df7461010574a2c5a5f8c428c9a05a8
   AAD =                        01
   CT  =                        ed5596b2ac560cace49f593154576284
                                7608cc1cd4be937778e4bc1542ce749c
                                ef0de63e87dda60a0d58c39d40698b31
                                c4bb87167c528a8db89975496c1586c7
   Encryption_Key =             5f377914db056de594bd23b0f07076be
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              02000000000000000000000000000000
```

```
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
                                  05000000000000000000000000000000

   TAG' =                         4df7461010574a2c5a5f8c428c9a05a8

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
                                  e0d01d677af7d82ff8e099ef3ef76b3e
                                  3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                  4df7461010574a2c5a5f8c428c9a05a8
                                  4ef7461010574a2c5a5f8c428c9a05a8
                                  4ff7461010574a2c5a5f8c428c9a05a8
                                  50f7461010574a2c5a5f8c428c9a05a8



   ---------------------- TWO_KEYS     (AAD = 12, MSG = 4)---------

   AAD_byte_len = 12
   AAD_bit_len  = 96
   MSG_byte_len = 4
   MSG_bit_len  = 32
   padded_AAD_byte_len = 16
   padded_MSG_byte_len = 16
   L1 blocks AAD(padded)  = 1
   L2 blocks MSG(padded)  = 1
                                             BYTES ORDER
                                  LSB-------------------------MSB
```

```
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000
   NONCE =                        03000000000000000000000000000000
   AAD =                          01000000000000000000000
   MSG =                          02000000
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
   LENBLK =                       60000000000000002000000000000000

   Computing POLYVAL on a
   buffer of 2 blocks + LENBLK.
   POLYVAL =                      d8000000000000c048000000f050f665
   POLYVAL_xor_NONCE  =           db000000000000c048000000f050f665
   with MSBit cleared =           db000000000000c048000000f050f665
   TAG =                          ff5ad2f9cbb36b1237cdbd63afb89d36
   AAD =                          01000000000000000000000
   CT  =                          7904ab1d
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                02000000

   TAG' =                         ff5ad2f9cbb36b1237cdbd63afb89d36

   TAG comparison PASSED!!!

   ***************************
            APPENDIX
   ***************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
                                  dc63067a4eb7f63448de25cabec7808a
                                  2495feb8555f3022f05dfb64a1d8c58c
                                  b9c56248f772947cbfacb1b6016b313c
                                  58ea39530db50971fde8f2155c303799
                                  b55f8c02422d187efd81a9c8fcea98f4
                                  e86d7fece5d8769d183084884400b311
                                  c6320e19841f1667799ebfaf8574275b
                                  7fffb3d59a27c548821741c0c617f2d1
                                  16bb30ad92a426caeb3a99656e4ebe3e
```

```
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                ff5ad2f9cbb36b1237cdbd63afb89db6


   ---------------------- TWO_KEYS     (AAD = 18, MSG = 20)---------

   AAD_byte_len = 18
   AAD_bit_len  = 144
   MSG_byte_len = 20
   MSG_bit_len  = 160
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
                                          BYTES ORDER
                                LSB-------------------------MSB
                                000102030405060708090101121314 15
                                --------------------------------
   K1 = H =                     03000000000000000000000000000000
   K2 = K =                     01000000000000000000000000000000
                                00000000000000000000000000000000
   NONCE =                      03000000000000000000000000000000
   AAD =                        01000000000000000000000000000000
                                0200
   MSG =                        03000000000000000000000000000000
                                04000000
   PADDED_AAD_and_MSG =         01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
   LENBLK =                     9000000000000000a000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                    08010000000000c06b01c04c63ad9807
   POLYVAL_xor_NONCE  =         0b010000000000c06b01c04c63ad9807
   with MSBit cleared =         0b010000000000c06b01c04c63ad9807
   TAG =                        19ff544d26d5f871b697767d0e1b7881
   AAD =                        01000000000000000000000000000000
                                0200
   CT  =                        e6daeb5dd348a30936888ae23cc38783
                                378c7134
   Encryption_Key =             5f377914db056de594bd23b0f07076be
```

```
                                c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =              03000000000000000000000000000000
                                04000000

   TAG' =                       19ff544d26d5f871b697767d0e1b7881

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)   5f377914db056de594bd23b0f07076be
                                   c88735cffb99fd5cd4c805dcf487f5ae
                                   49d19dab92d4f04e0669d3fef619a540
                                   8a5333c671cace9aa502cb4651853ee8
                                   dc63067a4eb7f63448de25cabec7808a
                                   2495feb8555f3022f05dfb64a1d8c58c
                                   b9c56248f772947cbfacb1b6016b313c
                                   58ea39530db50971fde8f2155c303799
                                   b55f8c02422d187efd81a9c8fcea98f4
                                   e86d7fece5d8769d183084884400b311
                                   c6320e19841f1667799ebfaf8574275b
                                   7fffb3d59a27c548821741c0c617f2d1
                                   16bb30ad92a426caeb3a99656e4ebe3e
                                   e0d01d677af7d82ff8e099ef3ef76b3e
                                   3ec4821fac60a4d5475a3db02914838e

   CTRBLKS (with MSbit set to 1)

                                19ff544d26d5f871b697767d0e1b7881
                                1aff544d26d5f871b697767d0e1b7881



   ---------------------- TWO_KEYS     (AAD = 20, MSG = 18)---------

   AAD_byte_len = 20
   AAD_bit_len  = 160
   MSG_byte_len = 18
   MSG_bit_len  = 144
   padded_AAD_byte_len = 32
   padded_MSG_byte_len = 32
   L1 blocks AAD(padded)  = 2
   L2 blocks MSG(padded)  = 2
```

```
                                        BYTES ORDER
                                  LSB-------------------------MSB
                                  000102030405060708090101112131415
                                  --------------------------------
   K1 = H =                       03000000000000000000000000000000
   K2 = K =                       01000000000000000000000000000000
                                  00000000000000000000000000000000

   NONCE =                        03000000000000000000000000000000
   AAD =                          01000000000000000000000000000000
                                  02000000
   MSG =                          03000000000000000000000000000000
                                  0400
   PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                  02000000000000000000000000000000
                                  03000000000000000000000000000000
                                  04000000000000000000000000000000
   LENBLK =                       a0000000000000009000000000000000

   Computing POLYVAL on a
   buffer of 4 blocks + LENBLK.
   POLYVAL =                      640100000000000600701c04c63add8de
   POLYVAL_xor_NONCE  =           670100000000000600701c04c63add8de
   with MSBit cleared =           670100000000000600701c04c63add85e
   TAG =                          474ed2b302caba5f9460075bf577d777
   AAD =                          01000000000000000000000000000000
                                  02000000
   CT  =                          1887531c24feb67e83067aa634f4106f
                                  9580
   Encryption_Key =               5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae

   Performing Decryption and
   Authentication:

   Decrypted MSG =                03000000000000000000000000000000
                                  0400

   TAG' =                         474ed2b302caba5f9460075bf577d777

   TAG comparison PASSED!!!

   **************************
            APPENDIX
   **************************
   KEY_SCHEDULE (Encryption_Key)  5f377914db056de594bd23b0f07076be
                                  c88735cffb99fd5cd4c805dcf487f5ae
                                  49d19dab92d4f04e0669d3fef619a540
                                  8a5333c671cace9aa502cb4651853ee8
```

```
                                dc63067a4eb7f63448de25cabec7808a
                                2495feb8555f3022f05dfb64a1d8c58c
                                b9c56248f772947cbfacb1b6016b313c
                                58ea39530db50971fde8f2155c303799
                                b55f8c02422d187efd81a9c8fcea98f4
                                e86d7fece5d8769d183084884400b311
                                c6320e19841f1667799ebfaf8574275b
                                7fffb3d59a27c548821741c0c617f2d1
                                16bb30ad92a426caeb3a99656e4ebe3e
                                e0d01d677af7d82ff8e099ef3ef76b3e
                                3ec4821fac60a4d5475a3db02914838e
```

CTRBLKS (with MSbit set to 1)

```
                                474ed2b302caba5f9460075bf577d7f7
                                484ed2b302caba5f9460075bf577d7f7
```

Authors' Addresses

Shay Gueron
University of Haifa and Intel Corporation
Abba Khoushy Ave 199
Haifa 3498838
Israel

Email: shay@math.haifa.ac.il

Adam Langley
Google
345 Spear St
San Francisco, CA 94105
US

Email: agl@google.com

Yehuda Lindell
Bar Ilan University
Bar Ilan University
Ramat Gan 5290002
Israel

Email: Yehuda.Lindell@biu.ac.il