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 October 16, 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

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 polynomial multiplication followed by reduction by the irreducible polynomial.

We define another binary operation on elements of the field: dot(a, b), where $\text{dot}(a, b) = a \cdot b \cdot x^{-128}$. The value $x^{-128}$ is equal to $x^{127} + x^{124} + x^{121} + x^{114} + 1$. Since the result of multiplications in the field is defined to be reduced, the result of $\text{dot}(a, b)$ 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 $X_1, \ldots, X_s$. Its result is $S_s$, where $S$ is defined by the iteration $S_0 = 0$; $S_j = \text{dot}(S_{j-1} + X_j, H)$.

We note that POLYVAL($H, X_1, X_2, \ldots$) is equal to $\text{ByteSwap}(\text{GHASH}(x^*H, \text{ByteSwap}(X_1), \text{ByteSwap}(X_2), \ldots))$, where $\text{ByteSwap}$ 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. Simply encrypting the nonce (as done in the case of a 16 bytes key) is now insufficient, because 256 bits of key material are needed. Therefore, AES-256 is used as a Pseudo Random Function to produce the 256 bits record-encryption key. This record-encryption key is defined as the concatenation of the result of encrypting, using the AES key, the nonce with the least-significant bit of the first byte set to zero and then to one.

Define the _length block_ as a 16-byte value that is the concatenation of the 64-bit, little-endian encodings of \( \text{len(additional_length)} \times 8 \) and \( \text{len(plaintext)} \times 8 \). Pad the plaintext and additional data with zeros until they are each a multiple of 16 bytes, the AES block size. Then \( X_1, X_2, \ldots \) (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 \( S_s = \text{POLYVAL(authentication_key, X_1, X_2, \ldots)} \), 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 is the tag with the most-significant bit of the last byte set to one and the first 32 bits set to zero. 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 is the tag with the most-significant bit of the last byte set to one and the first 32 bits set to zero. 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 $\text{length\_block}$ and $X_1, X_2, \text{etc}$ as above and compute $S_s = \text{POLYVAL}(\text{authentication\_key}, X_1, X_2, \text{\ldots})$. 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 01000000000000000000000000492 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 \( a+b = 99e94bd4ef8a2c3b884cfa59ca342b2e \), \( a*b = 3785175e9cd9df26ebc6d6171aa0ae9 \) and \( \text{dot}(a, b) = ebe563401e7e91ea3ad6426b8140c394 \).

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 752abad3e0afbf5f434dc4310f71f3d21.

The record encryption key will be AES(key = fab3a110b8ae672eba07d91ba52d6cea, data = 752abad3e0afbf5f434dc4310f71f3d21) = 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 6578616d706c650000000000000000004865c6c6f20776f726c64000000000005800000000003800000000000000.

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 \( S_s = 0b9ae25bd7fe4dcd17a007d11ac280e \). 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 and a 32-bit, little-endian counter is written to the first four bytes. This gives 0000000054c0997cae05d8b2be1d96be. Encrypting with this record key gives the first block of the keystream: b30b19ed9ba05d29b6aec0146b7fbb19.

The final ciphertext is the result of XORing the plaintext with the keystream and appending the tag. That gives fb6e7581f4802a46c4c2a88e2d69ed54c0997cae05d8b2be1d963e.
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.

It’s worth noting that the $2^{32}$ limit still applies as the number of distinct messages that can be encrypted under a fixed nonce. 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. (Or $2^{31}$ duplicates in the case of AEAD_AES_256_GCM_SIV.)

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

12. References

12.1. Normative References

12.2. Informative References


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_bit_len = 0
L1 blocks AAD(padded) = 0
L2 blocks MSG(padded) = 0

BYTES ORDER
LSB--------------------------MSB
00010203040506070809101112131415

--------------------------------
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
203db3954f8bfbf8cb2f484c9c880d7f
f4ea614bb61dec7099e968b95169b4f
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceead62793dcafed9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbe2cfe547a50a1f771e161633

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
00010203040506070809101112131415

---------------------
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000000000000000000000
Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL = 04000000000000809100000000283b1c
POLYVAL_xor_NONCE = 07000000000000809100000000283b1c
with MSBit cleared = 07000000000000809100000000283b1c
TAG = 5537355b0a4f4cb05ce77d1b815d7299
AAD =
CT = 3b0f5baabe526e9f
Encryption_Key = 57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cb92c2fbfd9d303b2f3
dd5370a46fb60c1f7d7f7c02774533
203db3954f8b8f8cb2ff84c9c8807f7
f4ea614bb61dec7099e968b95169bf4
93fed61289f00a62101962db4170dd9
2329ebec0bb6eb42ab777d79e707be
437845e748ceead6279d3cafcd9374
6d72d57525bc79fa47c5a30bb1c0944
c773ccbbe2cf547a50a7f771e61633

CTRBLKS (with MSbit set to 1)
0000000000a4f4cb05ce77d1b815d7299

--------------------- 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 = 01000000000000000000000000000000
MSG = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 00000000000000000000000000000000
LENBLK = 00000000000000006000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL = 0400000000000040d900000000283b1c
POLYVAL_xor_NONCE = 0700000000000040d900000000283b1c
with MSBit cleared = 0700000000000040d900000000283b1c
TAG = dd55830c690eadd7fd215b315470bd
AAD = 9391b4122fcccfe6b60ec40ab
Encryption_Key = 57d4b7ae8de993e30a6861b61e6ce4e

******************************************************************
APPENDIX
******************************************************************

APPENDIX

KEY_SCHEDULE (Encryption_Key) 57d4b7ae8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57c9d2c2fdf9d30b2f3
dd5370a46fb60c19fd7f7c0e774533
203db3954f8bbf8cb2ff484c9e880d7f
f4ea614b661dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb42a2ab77d679ea070be
437845e748ceaead6279d3ca4c39a374
6d72d75725bc79fa47c5aa30bb1c0944
c773cccbd2cfb547a50af771e161633

CTRBLKS (with MSbit set to 1)

00000000690eadd7fd215b315470bd

--------------------- 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

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

Computing POLYVAL on a buffer of 1 blocks + LENBLK.
POLYVAL = 04000000000000000230100000283b1c
POLYVAL_xor_NONCE = 07000000000000000230100000283b1c
with MSBit cleared = 147650d36f064f6b5dbbe8f04077d903
AAD = 565e4a931280ecdece8620abcf90b65e
Encryption_Key = 57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db395f8bbf8cb2ff484c9c880d7f
f4ea614bb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748cead6279d3cafcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbe2cfb547a50af771e161633

CTRBLKS (with MSbit set to 1) 000000006f064f6b5dbbe8f04077d983

-------------- 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
00010203040506070809101112131415

-----------------------------
K1 = H =
03000000000000000000000000000000

K2 = K =
01000000000000000000000000000000

NONCE =
03000000000000000000000000000000

AAD =
01000000000000000000000000000000

MSG =
02000000000000000000000000000000

PADDDED_AAD_and_MSG =
01000000000000000000000000000000

LENBLK =
02000000000000000000000000000000

08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL =
01000000000000000000000000000000

POLYVAL_xor_NONCE =
02000000000000000000000000000000

with MSBit cleared =
02000000000000000000000000000000

TAG =
78a50cb3f901ee38c588f6662d785a24

AAD =
9b1d2ba7d2d3a02efeec18d03be2b56

CT =
1753b147ae642183f2c4bbd72e4ed8e1

Encryption_Key=
57d4b7aec8de993e30a6861b61e6ce4e

**************************************************************
APPENDIX
**************************************************************

KEY_SCHEDULE (Encryption_Key)
57d4b7aec8de993e30a6861b61e6ce4e

d85f98411081017f2027876441c1492a
a2647dc2b2e57cb92c2fbd9d303b2f3

dd5370a46fb60c19fd74f7c02e774533

203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec70999e968b95169bf4
93feced61289f00a62101962db4170dd9
2329ebec0bb6eb42a2ab77d679ea070be
437845e748ceead6279d3cacf9a374

6d72d75725bc79fa47c5aa30bb1c0944
c773ccbe2cfb547a50af771e161633

CTRBLKS (with MSbit set to 1)
000000000f901ee38c588f6662d785aa4
01000000f901ee38c588f6662d785aa4
AAAAAAAAAAAAAAAA

--------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
MSG =
02000000000000000000000000000000
03000000000000000000000000000000
PADDLED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
LENBLK =
00000000000000000000000000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.

POLYVAL =
0e00000000000000650300203e788f7f
POLYVAL_xor_NONCE =
0d00000000000000650300203e788f7f
with MSBit cleared =
0d00000000000000650300203e788f7f
TAG =
a75aa62b704e826d984a72184e370598
AAD =
CT =
dcc8d2f2c0e30b565f5d3ef5bf6638f
f50e8909ced008e051b79f7c8c3d1f5
8ec1bb09177133b4cd1b375911d81579
Encryption_Key =
57d4b7ae59e30a6861b61e6ce4e

***************

APPENDIX

***************

KEY_SCHEDULE (Encryption_Key)

57d4b7ae59e30a6861b61e6ce4e
d85f98411081017f2027876411c1492a
a2647dc2b2e57c9d2c2fbd9d303b2f3
dd5370a46f60c19fd74f7c02e774533
203db3954f8bf8cb2ff484c9c880d7f
f4ea614bb61dec7899e96e95169bf4
93fede61289f00a62101962db4170dd9

CTRBLKS (with MSbit set to 1)

00000000704e826d984a72184e370598
01000000704e826d984a72184e370598
02000000704e826d984a72184e370598

--------------------- 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
00010203040506070809101112131415

--------------------- 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
00010203040506070809101112131415

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

PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000

LENBLK =
00000000000000000002000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

POLYVAL =
0f000000000000000000000000000000
POLYVAL_xor_NONCE =
0c000000000000000000000000000000
with MSBit cleared =
0c000000000000000000000000000000
TAG =
d7f4efe2f6c72e3b8df168cab6b790ab
AAD =

2329ebe4bb6eb4a2ab77d679ea070be
437845e748ceead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfd547a50a1f771e161633
CT = 472d6309563c74b6d5497145e929725a
    ab08979e64fc72c30c2e3e936e68b94
    92e1b0351167937ee2faae79d40af93e
    24ee405fda1b2040440632f1a34433
Encryption_Key= 57d4b7ae8e99e30a6861b61e6ce4e

****************************************************
APPENDIX
****************************************************

KEY_SCHEDULE (Encryption_Key) 57d4b7ae8e99e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57c8bd92c2fafd9d303b2f3
dd5370a46fb60c9fd74f7c0e774533
2039f354f88bf8cb2f484c9c88bd7f
f4ea614bfb61dec7099e968b95169bf4
93f6ed61289f00a62101962db4170dd9
2329ebc9b6e42a2b77d679e07b0e
437845e748ceead62793d3caac9a374
6d72d75725bc79a4c7c5aa30b1c094
7c73cc5ed2cfb547a501f77e161633

CTRBLKS (with MSbit set to 1)

00000000f6c72b3bf168cab6790ab
01000000f6c723bf168cab6790ab
02000000f6c723bf168cab6790ab
03000000f6c723bf168cab6790ab

----------------------------------------- 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
K1 = H = 03000000000000000000000000000000000000000000
K2 = K = 01000000000000000000000000000000000000000000
NONCE = 03000000000000000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 08000000000000004000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL = 130000000000008091000000f0501631
POLYVAL_xor_NONCE = 100000000000008091000000f0501631
with MSBit cleared = 100000000000008091000000f0501631
TAG = 633c11b2eef65be03f1e0c824c5e0
AAD = 01
CT = 5adcda74026afbb9
Encryption_Key= 57d4b7ae8de993e0a861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key) 57d4b7ae8de993e0a861b61e6ce4e
d85f9841101017f2027876441c1492a
a2647dc2b2e57c922f9d303b2f3
dd5370a46fb60c1f7d47f7c02e774533
203db95f8bfb8cb2f484c9c880d7ff4ea614bb61dec7099e968b95169bf4
93fed61289f00a62101962db4170dd9
2329ebe0bb6e4a2ab77d679e070b6437845e748ceae9d279d3caefcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbdde2cfb547a50af771e161633

CTRBLKS (with MSbit set to 1)

000000000ee1f65be03f1e0c824c5e0

--------------------- 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

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 08000000000000060000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = 1300000000000040d9000000f0501631
POLYVAL_xor_NONCE = 1000000000000040d9000000f0501631
with MSBit cleared = 1000000000000040d9000000f0501631
TAG = f229e75b2c4c3048fc70f163c9aefe0d
AAD = 01
CT = b4fabbadb27257bbe8b807d5
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

--------------------- 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
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
LENBLK = 08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = 1300000000000000000000000023010000f0501631
POLYVAL_xor_NONCE = 1000000000000000000000000023010000f0501631
with MSBit cleared = 1000000000000000000000000023010000f0501631
TAG = cfb5aa16cdd9d39acc5d99b6ee2c6fc
AAD = 01
CT = dce7c7cd4d1060f8dd63b9fe8de25385
Encryption_Key= 57d4b7ae8de993e30a6861b61e6ce4e

********************
APPENDIX
********************

KEY_SCHEDULE (Encryption_Key) 57d4b7ae8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46f6b0c19fd7f7c02e774533
203db3954f8b8f8c2f4849c880d7f
f4e6141b61d7099e968b95169bf4
93fede61289f00a62101962d4170dd9
2329ebec0bb6eb4a2ab77d679e070be
437845e748ceead6279d3cafd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbdbe2cfb547a50a771e161633

CTRBLKS (with MSbit set to 1)
00000000cdd9d39acc5d99b6ee2c6fc
--------------------- 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
00010203040506070809101112131415

K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
NONCE =                         03000000000000000000000000000000
AAD =                           01
MSG =                           02000000000000000000000000000000
PADDED_AAD_and_MSG =            01000000000000000000000000000000

LENBLK =

08000000000000000001000000000000

Computing POLYVAL on a buffer of 3 blocks + LENBLK.

POLYVAL =

1c0000000000000000000000000000000460200203e78ef5b

POLYVAL_xor_NONCE =

1f0000000000000000000000000000000460200203e78ef5b

with MSBit cleared =

8df5606f057468e4b38e89736255ad2d

AAD =

01

CT =

c6d3098e12ac653520764bcccdbd90655
b3d91bf034f7549d5f775fca5d6ad34f

Encryption_Key=

57d4b7a8a8d93e30a6861b61e6ce4e

******************************************************************************

APPENDIX
******************************************************************************

KEY_SCHEDULE (Encryption_Key) 57d4b7a8a8d93e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbb82fbd9d303b2f3
dd5370a46fb60c19fd747c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea61b861dec7099e968b95169bf4
93fede61289f00a62101962db4701d9
2329ebec0bb6eb4a2a77d679e070be
437845e748ceae6d279d3cafc9a374
CTRBLKS (with MSbit set to 1)

000000000057468e4b38e89736255adad
010000000057468e4b38e89736255adad

---------------------------- 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
00010203040506070809101112131415
--------------------------------
K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
NONCE =                         03000000000000000000000000000000
AAD =                           01
MSG =                           02000000000000000000000000000000
                      03000000000000000000000000000000
                      04000000000000000000000000000000
PADDED_AAD_and_MSG =            01000000000000000000000000000000
                      02000000000000000000000000000000
                      03000000000000000000000000000000
                      04000000000000000000000000000000
LENBLK =                        0800000000000000000800100000000000

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

POLYVAL =                      1d000000000000006503c04c63ad386b
POLYVAL_xor_NONCE =            1e000000000000006503c04c63ad386b
with MSBit cleared =            1e000000000000006503c04c63ad386b
TAG =                         b52274e14d6111c74edf5d95855256a2
AAD =                              01
CT =                          186abbbe486294281b1514c11c240e6a
                      4d959a1ac6da46e5b83bbe2d3d37de44
                      ab009bb885b5c0bf83db80b651c06e74
Encryption_Key=                  57d4b7ae8de993e30a6861b61e6ce4e
APPENDIX

KEY_SCHEDULE (Encryption_Key)

| 57d4b7aec8de993e30a6861b61e6ce4e |
| d85f98411081017f2027876441c492a |
| a2647dc2b2e57cbd92c2f5d9d303b2f3 |
| dd5370a46fb60c19fd74f7c02e774533 |
| 203db3954f8bbb8cb2f484c9c880d7f |
| f4ea614bb61dec7099e968b95169bf4 |
| 93fed61289f00a62101962db4170dd9 |
| 2329ebec0bb6eb4a2ab77d679ea070be |
| 437845e748ceead6279d3cafcd9a374 |
| 6d72d75725bc79fa47c5aa30bb1c0944 |
| c773c2bde2cfb5475a50af771e161633 |

CTRBLKS (with MSbit set to 1)

| 00000004d611c74edf5d95855256a2 |
| 01000004d611c74edf5d95855256a2 |
| 02000004d611c74edf5d95855256a2 |

--------------------- 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 |

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

| K1 = H = |
| K2 = K = |
| NONCE = |
| AAD = 01 |
| MSG = |
| PADDED_AAD_and_MSG = |

| 01000000000000000000000000000000 |
| 02000000000000000000000000000000 |
| 03000000000000000000000000000000 |
LENBLK =
04000000000000000000000000000000
05000000000000000000000000000000
08000000000000000000000000000000

Computing POLYVAL on a buffer of 5 blocks + LENBLK.

POLYVAL =
1b0000000000000008c841a0172a376e
POLYVAL_xor_NONCE =
18000000000000008c841a01712a376e
with MSBit cleared =
18000000000000008c841a01712a376e
TAG =
668fc00b6b40b4bb0c8d6cdb9730358d
AAD =
01
CT =
499ec09c83c2b79cf6b219e6b79ec81c
7c7b572c8a04b322094ec011e7003ded
388627f831ee79bd3df5db27648125a
f6f277438c34b6652b866ca84bdcd8

Encryption_Key=
57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cd92c2fbf69d3d03b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bb61dec7099e968b95169bf4
93fed961289f00a62101962db4170dd9
2329e9e09b6eb4a2ab77d679ea070be
437845e748ceae66279d3cafcd9a374
6d72d75725bc79fa47c5aa3bb1c0944
c773cbbe2cbe547a50a1771e161633

CTRBLKS (with MSbit set to 1)
000000006b40b4bb0c8d6cdb9730358d
010000006b40b4bb0c8d6cdb9730358d
020000006b40b4bb0c8d6cdb9730358d
030000006b40b4bb0c8d6cdb9730358d

--------------------- 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
00010203040506070809101112131415
--------------------------------
K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
MSG =
02000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
60000000000000000000000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL =
d8000000000000000c048000000f050f665
POLYVAL_xor_NONCE =
db0000000000000000c048000000f050f665
with MSBit cleared =
db0000000000000000c048000000f050f665
TAG =
488346eaebe2d64ffa58e0fa82f8fcd43
AAD =
01000000000000000000000000000000
CT =
7d5240be
Encryption Key=
57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
da2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46f60c19fd7f47c02e774533
203db3954f8bbf8cb2f2f484c9880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f0a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845748ceae6d279d3cafcd9a374
6d72d75725bc79fa47c5aa30b1c0944
c773ccbdde2cfb547a50a7f771e16133

CTRBLKS (with MSbit set to 1)
00000000ebe2d64ffa58e0fa82f8fcd3

---------------------------- 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
00010203040506070809101112131415
--------------------------------
K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
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 =                        0801000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE  =            0b010000000000c06b01c04c63ad9807
with MSBit cleared =            0b010000000000c06b01c04c63ad9807
tag =                            d010794cf97252f1c06b01c04c63ad9807
AAD =                            01000000000000000000000000000000
0200
CT =                            6d98c309d4f472480c5b1389e83569e5
217dd9c
Encryption_Key=                 57d4b7ae8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key) 57d4b7ae8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bba61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
CTRBLKS (with MSbit set to 1)

00000000fdbbc65ef641b8ccb9c2dda3
01000000fdbbc65ef641b8ccb9c2dda3

--------------------- 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
00010203040506070809101112131415
--------------------------------
K1 = H =                        03000000000000000000000000000000
K2 = K =                        01000000000000000000000000000000
NONCE =                         03000000000000000000000000000000
AAD =                           01000000000000000000000000000000
02000000
MSG =                           03000000000000000000000000000000
0400
PADDED_AAD_and_MSG =            01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK =                        a000000000000900000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

POLYVAL = 64010000000000600701c04c63add8de
POLYVAL_xor_NONCE = 670100000000600701c04c63add8de
with MSBit cleared = 670100000000600701c04c63add85e
TAG = 98e16515942fb8ff9e108e7ce53a963
AAD = 01000000000000000000000000000000
02000000
CT = 4649087685b01b476bd3420f36ca67d3
b18b
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbb92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bf8cb2f4849c9880d7f
f4e614bb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab7778d799ea070be
437845e748ceaed6279d3cafcd9a374
6d72d5725b79fa47c5aaa30b1c0944
c773cbde2cfe57a50a771e761633

CTRBLKS (with MSbit set to 1)

000000000942ff9e108e7ce53a9e3
010000000942ff9e108e7ce53a9e3

--------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
MSG =
PADD rooted AAD_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
a2647dc2b2e57c92c2fbd9d303b2f3
d5370a46fb60c19fd74f7c02e774533
203db395f8bbf8cb2f484c9c880d7f
f4ea6141bb561dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab7d79e9a70be
437845e748c9e9ed6279d3cafc9a374
6d72d75725bc79fa47c5a30bb1c0944
c773ccbcde2cfb547a50a1f771e61633

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
0010203040506070809101112131415

------------------------
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
PADDDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000000000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.
POLYVAL = 04000000000000809100000000283b1c
POLYVAL_xor_NONCE = 07000000000000809100000000283b1c
with MSBit cleared = 07000000000000809100000000283b1c
TAG = 5537355b0a4fcb05ce77d1b815d7299
AAD = CT = 3b0f5babe526e9f
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key)
d85f98411081017f2027876441c1492a
a2647dc2b2e57c经商2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614b61dec7099e968b95169bf4
93fed61289f00a62101962db4170dd9
2329ebec8bb6e4a2ab77d6799e070be
437845e748ceaaed6279d3cafcde9a374
6d72d75725bc79fa47c5aa30bb2c944
c773ccbd62c547a50af771e61633

CTRBLKS (with MSbit set to 1)
000000000a4f4cb05ce77d1b815d7299

--------------------- 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
0010203040506070809101112131415

K1 = H =
0300000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000000000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.
POLYVAL = 04000000000000040d90000000283b1c
POLYVAL_xor_NONCE = 07000000000000040d90000000283b1c
with MSBit cleared = 07000000000000040d90000000283b1c
TAG = dd55830c690eadd7fd2155b3615470bd
AAD =
CT = 9391b4122fccfebc60ec40ab
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

************************************************
APPENDIX
************************************************
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f9841081017f2027876441c1492a
a2647dc2be57cb92c2fbfd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bb8cb2ff484c9c880d7f
f4ea614b61dec7099e96895169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3ca8cd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbdde2cfb547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

00000000690eadd7fd2155b3615470bd

--------------------- 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
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
MSG =
01000000000000000000000000000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
LENBLK =
00000000000000008000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL =
040000000000000000000000000000002301000000283b1c
POLYVAL_xor_NONCE =
070000000000000000000000000000002301000000283b1c
with MSBit cleared =
070000000000000000000000000000002301000000283b1c
TAG =
147650d36f064f6b5dbbe8f04077d903
AAD =
565e4a931280ecdece8620abcf90b65e
Encryption.Key= 57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption.Key)
57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbb92c2fbd9d303b2f3
dd5370a46fb60c19f74f7c02e774533
203db3954f88bf8cb2ff484c9c880d7f
f4ea614bb61dec7099e968b95169bf4
93fede61289f00a62101962db4170d9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceae6d6279d3cafcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbd2cfb547a50a1f771e161633

CTRBLKS (with MSbit set to 1)
000000006f064f6b5dbbe8f04077d983

--------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
MSG =
02000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
000000000000000000000100000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL =
01000000000000000000046020000f0507615
POLYVAL_xor_NONCE =
02000000000000000000046020000f0507615
with MSBit cleared =
02000000000000000000046020000f0507615
TAG =
78a50cb3f901ee38c588f6662d785a24
AAD =
9bd2ba7d2d3a0efeeec18d03be2b56
CT =
1753b147ae642183f2c4bbd72e4ed8e1
Encryption_Key=
57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key) 
57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbb92c2fb9d9303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8b3bf8cb2ff484fc9880d7f
f4ea614bb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0b6e842ab77d679ea070be
437845e748ceead6279d3ca76179f43
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbd2c8b547a50a1f771e61633

CTRBLKS (with MSbit set to 1)
000000000f901ee38c588f6662d785aa4
01000000f901ee38c588f6662d785aa4

---------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
LENBLK =
00000000000000008001000000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.

POLYVAL =
0e000000000000000000000000000000650300203e788f7f
POLYVAL_xor_NONCE =
0d000000000000000000000000000000650300203e788f7f
with MSBit cleared =
0d000000000000000000000000000000650300203e788f7f
TAG =
a75aa62b704e826d984a72184e370598
AAD =
CT =
dcc8d2f2c0e30b565f5d3ef58bf6638f
f50e8909ced008e0515b79f7c8c3d1f5
8ec1bb09177133b4cd1b375911d81579
Encryption_Key=
57d4b7ae8de993e30a6961b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
57d4b7ae8de993e30a6961b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
CTRBLKS (with MSbit set to 1)

0000000704e826d984a72184e370598
0100000704e826d984a72184e370598
0200000704e826d984a72184e370598

-------------- 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
00010203040506070809101112131415

K1 = H =
K2 = K =
NONCE =
AAD =
MSG =
PADDED_AAD_and_MSG =
LENBLK =

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

0f00000000000008c04c04c63ad584f
POLYVAL_xor_NONCE = 0c00000000000008c04c04c63ad584f
with MSBit cleared = 0c00000000000008c04c04c63ad584f
TAG = d7f4efe2f6c72e3b8df168cab6b790ab
AAD = 
CT = 472d6309563c74b6d5497145e929725a
ab08979e6c4fc72a30c23e1aece568b94
92e1b0351c167937ee2faae79d40af93e
24eed045f1ab12b0404040632fa3a4433
Encryption_Key = 57d4b7aec8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key)

57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cb9c22fd9d3033b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bfb8cb2ff484c9c880df7f
f4ea614bb61dec7099e968b95169bf4
93fede6128f00a62101962db4170dd9
3239ebec0b6eb4a2ab77d679ea070be
437845e748ceae6d279d3cafcfd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbd3c2b547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

00000000f6c72e3b8df168cab6b790ab
01000000f6c72e3b8df168cab6b790ab
02000000f6c72e3b8df168cab6b790ab
03000000f6c72e3b8df168cab6b790ab

--------------------- 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
00010203040506070809101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 08000000000000004000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = 130000000000008091000000f0501631
POLYVAL_xor_NONCE = 100000000000008091000000f0501631
with MSBit cleared = 633c11b2eee1f65be0e3f1e0c824c5e0
AAD = 01
CT = 5adcda74026afbb9
Encryption_Key= 57d4b7aeb8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
57d4b7aeb8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cb92c2fbd9d303b2f3
dd5370aa46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff48c9c880d7f
f4ea614b661dec7099e968b95169fb4
93fede61289f00a62101962db4170dd9
2329ebecc0b6eb4a2ab77d679ea070be
437845e748ce5ead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbdde2cfb547a50af77l61633

CTRBLKS (with MSbit set to 1)
on0000000eeef165be0e3f1e0c824c5e0

-------------------------------- 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
01000000000000000000000000000000

K1 = H =
K2 = K =
NONCE =
AAD =
MSG =
PADDED_AAD_and_MSG =
LENBLK =

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL =
POLYVAL_xor_NONCE =
with MSBit cleared =
TAG =
AAD =
CT =
Encryption_Key =

***************
APPENDIX
***************

KEY_SCHEDULE (Encryption_Key)
CTRBLKS (with MSbit set to 1)

--------------- 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
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
08000000000000008000000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL =
1300000000000000023010000f0501631
POLYVAL_xor_NONCE =
1000000000000000023010000f0501631
with MSBit cleared =
100000000000000023010000f0501631
TAG =
cfb5aa16cdd93acc5d99b6e26ea2c6fc
AAD =
01
CT =
dce7c7cd4d1060f663b9fe8de25385
Encryption_Key=
57d4b7aec8de993e30a6861b61e6ce4e

**********************
APPENDIX
**********************
KEY_SCHEDULE (Encryption_Key)
57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fb9d9303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbfb2ff8484c9e80dd7f
f4ea614bbb61dec7099e968b95169bf4
93fed61289f00a62101962db4170dd9
2329ebec0bb6e4a2ab77d679ea070be
437845e748ceae6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbdde2cfe547a50af771e161633

CTRBLKS (with MSbit set to 1)
--------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
03000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
LENBLK =
08000000000000000000000010000000000

Computing POLYVAL on a buffer of 3 blocks + LENBLK.

POLYVAL =
1c0000000000000000000460200203e78ef5b
POLYVAL_xor_NONCE =
1f00000000000000000460200203e78ef5b
with MSB cleared =
1f00000000000000000460200203e78ef5b
TAG =
8df5606f057468e4b38e973625ad2d
AAD =
01
CT =
c6d3098e12ac653520764cbccdb90655
b3d91bf034f7549d5f775fca5d6ad34f
Encryption_Key=
57d4b7ae8de993e30a6861b61e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
57d4b7ae8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f

CTRBLKS (with MSbit set to 1)

00000000057468e4b38e89736255adad
01000000057468e4b38e89736255adad

-------------- 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
00010203040506070809101112131415
--------------------------------

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK =
08000000000000800100000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

POLYVAL =
1d000000000000006503c04c63ad386b
POLYVAL_xor_NONCE =
1e000000000000006503c04c63ad386b
with MSBit cleared =
1e000000000000006503c04c63ad386b
TAG =
b52274e14d6111c74edf5d95855256a2
AAD =
01

CT = 186abbbe4862942f81b514c11c240e6a
   4d959a1ac6a46e5b83b2b2d3d37de44
   ab009bb85b5c0bf83db80b651c06e74

Encryption_Key=
   57d4b7aec8de993e30a86861b6e6ce4e

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
   57d4b7aec8de993e30a86861b6e6ce4e
d85f98411081017f2027876441c1492a
   a2647dc2b2e57c9d2c2fd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
   203d395f8bff8cb2ff4849c880d7f
   f4e6a14bb6d1ec7099e968b95169bf4
   93fede61289f00a62101962db4170d9
   2329ebec0b6e4a2ab77d799ea707be
   437845e748ceaead6279d3caaf9a374
   6d72d7525bc79fa47c5aa03bb1c944
c773ccbe2cfb547a50a7f771e161633

CTRBLKS (with MSbit set to 1)
   00000004d1111c74edf5d95855256a2
   01000004d1111c74edf5d95855256a2
   02000004d1111c74edf5d95855256a2

--------------------- 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
K1 = H =
   0300000000000000000000000000000000000000000000000000000000000000
K2 = K =
   0100000000000000000000000000000000000000000000000000000000000000
NONCE =
   0300000000000000000000000000000000000000000000000000000000000000
AAD =
   01
MSG =
   0200000000000000000000000000000000000000000000000000000000000000
   0300000000000000000000000000000000000000000000000000000000000000
Computing POLYVAL on a buffer of 5 blocks + LENBLK.

POLYVAL = 1b0000000000000008c841a01712a376e
POLYVAL_xor_NONCE = 18000000000000008c841a01712a376e
with MSBit cleared = 18000000000000008c841a01712a376e
TAG = 668fc00b6b40b4bb0c8d6cdb9730358d
AAD = 01
CT = 499ec09c83c2b79cf6b219e6b79ec81c
7c7b572c8a04b322094ec011e7003ded
388627f831ee79bd3df5db27f648125a
fbfe2774388c34bb652b866ca84bdc8
Encryption_key= 57d4b7aec8de993e30a6861b61e6ce4e

****************************************
APPENDIX
****************************************

KEY_SCHEDULE (Encryption_key)

57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cb59c2fbfd9d303b2f3
dd537a46fb60c19fd7f7c02e774533
203db3954f8bf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93feded1289f00a62101962db170dd9
2329ebeec0b6eb42ab77d879e4070be
4378457e748ceaead6279d3cafed9a374
6d72d57525bc79fa47c5aa30bb1c0944
4773ccbdde2cbb547a50a1f771e16133

CTRBLKS (with MSbit set to 1)

000000006b40b4bb0c8d6cdb9730358d
010000006b40b4bb0c8d6cdb9730358d
020000006b40b4bb0c8d6cdb9730358d
030000006b40b4bb0c8d6cdb9730358d

--------------------- 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

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = d800d00c00f0f665
POLYVAL_xor_NONCE = db0000000000c0f0f665
with MSBit cleared = db0000000000c0f0f665
TAG = 488346eaebe2d64ffa58e0fa82f8cd43
AAD = 01000000000000000000000000000000
CT = 7d5240be
Encryption_Key= 57d4b7ae8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key)
57d4b7ae8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d330b2f3
dd5370a46fb60c19fd74f7c02e774533
203db39e0e88ff8cb2ff48e9c880d7f
f4ea614b6b61dec7099e968b95169bf4
93f3e6e61289f00a62101962db4170cd9
2329ebec0bb6eb42ab77d679ea07b0e
437845e748ceead6279d3cafcd9a374
6d72d75725bc79fa47c5a30bb1c0944
c773ccbcde2c5b547a50af771e161633

CTRBLKS (with MSbit set to 1)
00000000ebe2d64ff58e0fa82f8cdc3

----------------------- 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
00010203040506070809101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
0200
MSG = 03000000000000000000000000000000
04000000
PADDDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 90000000000000000000000000000000

Computing POLYVAL on a buffer of 4 blocks + LENBLK.
POLYVAL = 080100000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b010000000000c06b01c04c63ad9807
with MSBit cleared = 0b010000000000c06b01c04c63ad9807
TAG = d010794cfdbbc65ef641b8cccb9c2dda3
AAD = 01000000000000000000000000000000
0200
CT = 6d98c309d4f472480c5b1389e83569e5
217db9c
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

**********************************************************************
APPENDIX
**********************************************************************
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
CTRBLKS (with MSbit set to 1)

00000000fdbbc65ef641b8cc9c2dda3
01000000fdbbc65ef641b8cc9c2dda3

--------------------- 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
00010203040506070809101112131415
--------------------------------
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
02000000
MSG = 03000000000000000000000000000000
0400
PADDDED_AAD_and_MSG = 01000000000000000000000000000000
02000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = a00000000000000000000000000000000000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

POLYVAL = 6401000000000000600701c04c63add8de
POLYVAL_xor_NONCE = 6701000000000000600701c04c63add8de
with MSBit cleared = 67010000000000600701c04c63add85e
TAG = 98e16515942fb8ff9e108e7ce53a963
AAD = 100000000000000000000000000000000
CT = 4649087685b01b476bd3420f36ca67d3
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

******************************************************************************
APPENDIX
******************************************************************************

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f202787641c1492a
a2647dc2b2e57c2bbf9e108e7ce53a963
d5370046fb60c19fd7f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bb61dec7099e968b95169bf4
93fedc61289f00a62101962db4170fd9
2329ebec0bb6eb4a2ab77d799ea07be
437845e748ceead6279d3cafc9a374
6d72d5725bc79fa47c5aa30b1c0944
c773ccbd2c3f547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

00000000942fb8ff9e108e7ce53a9e3
00100000942fb8ff9e108e7ce53a9e3

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
00010203040506070809101112131415
----------------------
K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000

AAD =
MSG =
PADDDED_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 = delafcd85a5217d91d8b349ab9cd224
AAD =
CT =
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cfeb99fd5cd4c805dcf487f5ae

******************************************************************************
APPENDIX
******************************************************************************

KEY_SCHEDULE (Encryption_Key) 
d77cdb05a40231d52ec7ef3b115a4259
c88735cfeb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32b2cd05149cf94579e22c514e995a48
c323b99ea29b7e19a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0ab5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247df87014e639dbf7e594bba
47cc0f3e979284c1b3e8d7bbaef4

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
00010203040506070809101112131415

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

Computing POLYVAL on a buffer of 1 blocks + LENBLK.
POLYVAL = 0400000000000000809100000000283b1c
POLYVAL_xor_NONCE = 0700000000000000000000000000283b1c
with MSBit cleared = 90d1e4ad87f53f63eb26c066193f3df
AAD =
CT = 4b0619edd74c6a09
Encryption_Key = d77c05a40231d52ec7ef3b115a4259
c88735c6fbb99f5cd4c805dcf487f5ae

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key) d77c05a40231d52ec7ef3b115a4259
c88735c6fbb99f5cd4c805dcf487f5ae
c19af6a5980e6f45fe15450a5a30d
76ec3f188d75c24459bd798ad3a3236
43b932e2f6213406d7ed514377b7619
c61c0c7e61b8c58838050210953f3026
32bd1d5149cf94579e22c514e995a48
c323e9a29b7c169a9e7e060fa1e20
48927a1730c833665ecaf672b75f52f
32be5f8b9025239d0abb59b3051a13bb
baef901c9e8112ec30d4c49e784966
a90264b839274725339c1abe36860905
d3eeefb1d780fe833bb2547a537a1d1c
44d8c0247df87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

CTRBLKS (with MSbit set to 1) 00000000087f53f63eb26c066193f3df
-------------- TWO_KEYS (AAD = 0, MSG = 12)--------------

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAD_byte_len</td>
<td>0</td>
</tr>
<tr>
<td>AAD_bit_len</td>
<td>0</td>
</tr>
<tr>
<td>MSG_byte_len</td>
<td>12</td>
</tr>
<tr>
<td>MSG_bit_len</td>
<td>96</td>
</tr>
<tr>
<td>padded_AAD_byte_len</td>
<td>0</td>
</tr>
<tr>
<td>padded_MSG_byte_len</td>
<td>16</td>
</tr>
<tr>
<td>L1 blocks AAD(padded)</td>
<td>0</td>
</tr>
<tr>
<td>L2 blocks MSG(padded)</td>
<td>1</td>
</tr>
</tbody>
</table>

BYTES ORDER
LSB--------------------------MSB
00010203040506070809101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000006000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL = 04000000000000000000040d9000000000283b1c
POLYVAL_xor_NONCE = 0700000000000000000000040d9000000000283b1c
with MSBit cleared = a42c36bcd7dd95273c5ded5a5ab0a8fc
TAG = ea410b6727fe50357dc2c9f9
Encryption_Key = d77cdeb05a0231d52ec7ef3b115a4259
c88735c0fbb99fd5cd4805dcf487f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
d77cdeb05a0231d52ec7ef3b115a4259
c88735c0fbb99fd5cd4805dcf487f5ae
c193fba65980e6f4b5fe154a05a30d
76ec3f188d75c24459bdc798ad3a236
43b93a2f2621344067ed514377b7619
eccd07cc61b8c5883805021095f3026
32bdc05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa1e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b51a3bb
baef9018a6e1132ec30dbc49e8784966
CTRBLKS (with MSbit set to 1)

00000000d7dd95273c5ded5a5ab0a8fc

--------------------- 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 =
K2 = K =
NONCE =
AAD =
MSG =
PADDED_AAD_and_MSG =
LENBLK =

Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL =
P强制YVAL_xor_NONCE =
with MSbit cleared =
TAG =
AAD =
CT =
Encryption_Key =

********************************
APPENDIX
********************************
KEY_SCHEDULE (Encryption_Key) d77c0b5a40231d52ec7ef3b115a4259
c88735cc1f89f5dcd4c805dcff487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76e3f1f88d75c24459bcd798ad3a3236
43b93a2f262134406d7ed5143777b7619
ecc07cc61b8c58838050210953f3026
32bdc05149cf94579e22c514e995a48
c31b3b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb59b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247df87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbae4f

CTRBLKS (with MSbit set to 1)

000000005dea30d23ec045223ef5859e

------------------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
00000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
00000000000000000000000000000000
MSG =
00000000000000000000000000000000
PADDED_AAD_and_MSG =
00000000000000000000000000000000
LENBLK =
0000000000000001000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

POLYVAL = 01000000000000046020000f0507615
POLYVAL_xor_NONCE = 02000000000000046020000f0507615
with MSBit cleared = 02000000000000046020000f0507615
TAG = ac78c482d3499b26ae97bf353c2c1bdb
AAD =
CT = cac82890d7f5a8330fa2f0f03701901a
ed8a9866b42f74cc1887b18964cf37
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735c9fb9fd5cd4805dcf487f5a

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key) 
d77cdb05a40231d52ec7ef3b115a4259
c88735c9fb9fd5cd4805dcf487f5a
c19a3fba65980e6f4b5e1545a5a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f2621344067ed514377b7619
ec6d07cc618c58838050201953f026
32bdc05149cf94579e22c51e995a48
323b99ea29b7c169a9e7e060fa14e20
08927a73c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d29b051a13bb
baef9018a6e1132ec3d0b49e8784966
a90264b392742725339c1abe3680905
deefebd780fe833bb02547a537a4d1c
44d8c0247ff87014e639dbf78e594aba
47cc0fa13fc379284c1b3e8d7baefb4

CTRBLKS (with MSbit set to 1)
00000000d3499b26ae97bf353c2c1bdb
01000000d3499b26ae97bf353c2c1bdb

--------------------- 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
Computing POLYVAL on a buffer of 3 blocks + LENBLK.
POLYVAL = 0e000000000000000650300203e788f7f
POLYVAL_xor_NONCE = 0d000000000000000650300203e788f7f
with MSBit cleared = 0d000000000000000650300203e788f7f
TAG = d47a04762c2dea133c87ae50fbeb1c1b3
AAD = bd562c8f8bbde467149c17a3f316fd2c8859c74876032d3296a5b233c4059e370a42d2b1812f4884801a184b23ae
CT = d77cfd05a40231d52ec7ef3b115a4259c88735c0b99f50c4805dfc487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)
d77cfd05a40231d52ec7ef3b115a4259
c88735c0b99f50c4805dfc487f5ae
c19a3f6ba65980e6f4b5f6e545a05a30d76ec3f188d75c24459bdc798ad3a323643b93a2f262134067d5d14377b7619
ec0d7cc61b8c58838050210953f302632bdc05149c94579e22c514e995a48c323b99e29b7c169a9e7e060fa14e208927a731c0e833665ecaf672b75f52f32be58b9025239d0abb59b051a13bbbaef9018a6e1132ec30dcb49e8784966a90264b839274725339c1abe366d0905aeeefb1d780fe83bb02547a537a1d1c44d8c0247dfe87014e639dfb78e594ba47cc0fa13fc3e79284c13e8d7bbafef4
CTRBLKS (with MSbit set to 1)

0000000002c2deal33c87aea50fb1c1b3
0100000002c2deal33c87aea50fb1c1b3
0200000002c2deal33c87aea50fb1c1b3

--------------------- 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
00010203040506070809101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 00000000000000000002000000000000

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

POLYVAL = 0f000000000000000000000000000000
POLYVAL_xor_NONCE = 0c000000000000000000000000000000
with MSBit cleared = 0c000000000000000000000000000000
TAG = 15e4bd316b19caa3a3493a81a3e4153c
AAD =
CT = d53e727defb0fe560c87f405ab19b1a2
6fd85249324b974564c477b2eb4d4162
943fa821946537d507e0713dccc556075
220130acb5f3daa8dd46ee9af3b36642
Encryption_Key = d77c065a40021d5e3f3b115a4259
c88735c6f99ff5d4c805dfc487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)

CTRBLKS (with MSbit set to 1)

--------------------- 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

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000080000000

000000006b19caaa3a3493a81a3e415bc
010000006b19caaa3a3493a81a3e415bc
020000006b19caaa3a3493a81a3e415bc
030000006b19caaa3a3493a81a3e415bc

Bytes ORDER

LSB--------------------------MSB
00010203040506070809101112131415

03000000000000000000000000000000
01000000000000000000800000000000
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 0200000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 08000000000000004000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = 130000000000008091000000f0501631
POLYVAL_xor_NONCE = 100000000000008091000000f0501631
with MSBit cleared = 100000000000008091000000f0501631
TAG = 4cac1deb89734986b5f0546c661932e9
AAD = 01
CT = 8e5a22875d5d692e
Encryption_Key = d77c05a40231d52ec7ef3b115a4259
c88735c9f9bd5c805d8f487f5ae

**APPENDIX**

**APPENDIX**

KEY_SCHEDULE (Encryption_Key)
d77c05a40231d52ec7ef3b115a4259
c88735c9f9bd5c805d8f487f5ae
c19a3fb6a5980e6f4bfe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f26213440676d51377b7619
eccd07cc61b8c58838505210953f3026
32bdc05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa4e20
08927a731c0e833665eac672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30d4e98748966
a90264b839274725333c1abe36860f05
deeebf1bd780fe833bb02547a537a11d
44d8c0247ff87014e639dbf78e594ba
47cc0fa13fc3e792841c3e8d7bbaef4

CTRBLKS (with MSbit set to 1)

0000000089734986b5f0546c661932e9

--------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
00000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL =
130000000000000000000000040d9000000f0501631
POLYVAL_xor_NONCE =
1000000000000000000000000040d9000000f0501631
with MSBit cleared =
1000000000000000000000000040d9000000f0501631
TAG =
42794bd56cd0b78ebdad8dc2c2c11720
AAD =
01
CT =
ed921994f8d27aad941bfb6f
Encryption_Key =
d77cddb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805d5f487f5ae

********************
APPENDIX
********************

KEY_SCHEDULE (Encryption_Key)
d77cddb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805d5f487f5ae
c193fba65980e64b5fe154a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665eca6727b75f52f
32be5ff89b9025239d0abb5d9b05a13bb
baef9018a6e1132ec30bdc49e8784966
a90264b839274725339c1ab8e6b08905
deeefbd780fe833bb02547a537a1d1c
44d8c0247d0f87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4
CTRBLKS (with MSbit set to 1)

00000006cd0b78ebdad8dc2c2c117a0

------------------------------- 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
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL =
13000000000000000000000000000000f0501631
POLYVAL_xor_NONCE =
10000000000000000000000000000000f0501631
with MSBit cleared =
10000000000000000000000000000000f0501631
TAG =
1e1fb157ee961567ee5a686a3ac66e74
AAD =
01
CT =
295cb156a7ccc66c9026829a26b08a92
Encryption_Key =
d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805dcf487f5ae

***************************************************************
APPENDIX
***************************************************************
KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc79ad3a3236
CTRBLKS (with MSbit set to 1)

00000000ee961567ee5a686a3ac66ef4

---------------------- 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

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
03000000000000000000000000000000
PADED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
LENBLK =
0800000000000000000000100000000000

Computing POLYVAL on a buffer of 3 blocks + LENBLK.
PPLYVAL =
1c00000000000000000000460200203e78ef5b
POLYVAL_xor_NONCE =
1f00000000000000000000460200203e78ef5b
with MSBit cleared = 1f0000000000000460200203e78ef5b
TAG = c5558db375fc7fb253b477d990435e79
AAD = 01
CT = b1403a920a945105017054c07d78ef5b
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735ccfb99fd5cd4c805dcf487f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735ccfb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3226
43b93a2f26213406d7ed5143777b7619
eccd07cc61b8c58838058210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb59b051a3bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247dfff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

CTRBLKS (with MSbit set to 1)
0000000075fc7fb253b477d990435ef9
0100000075fc7fb253b477d990435ef9

--------------------- 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
00010203040506070809101112131415

----------------------------
K1 = H = 0300000000000000000000000000000000000000000000000000000000000000
K2 = K = 0100000000000000000000000000000000000000000000000000000000000000

NONCE = 0300000000000000000000000000000000000000000000000000000000000000
AAD = 01
MSG = 0200000000000000000000000000000000000000000000000000000000000000

PADDED_AAD_and_MSG = 0100000000000000000000000000000000000000000000000000000000000000

LENBLK = 0800000000000000800100000000000000000000000000000000000000000000

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

POLYVAL = 1d000000000000006503c04c63ad386b
POLYVAL_xor_NONCE = 1e000000000000006503c04c63ad386b
with MSBit cleared = 54538b4b90c4877f29632ec9441d9809
AAD = 01
CT = 687c9c5846e8fde28bc1bde37dd15b80

Encryption_Key = d77c9c5846e8fde28bc1bde37dd15b80

****************************
APPENDIX
****************************

KEY_SCHEDULE (Encryption_Key) d77c9c5846e8fde28bc1bde37dd15b80
c88735cffe99f5dcd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a5a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b5c888305210953f3026
32bd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e883665eacf67275f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b8392747253391cabe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247df87014e639df78e594ba
47cc0fa13fc3e79284c1b3e8d7bbafaef4

CTRBLKS (with MSbit set to 1)
--------------------- TWO_KEYS     (AAD = 1, MSG = 64)---------

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAD_byte_len</td>
<td>1</td>
</tr>
<tr>
<td>AAD_bit_len</td>
<td>8</td>
</tr>
<tr>
<td>MSG_byte_len</td>
<td>64</td>
</tr>
<tr>
<td>MSG_bit_len</td>
<td>512</td>
</tr>
<tr>
<td>padded_AAD_byte_len</td>
<td>16</td>
</tr>
<tr>
<td>padded_MSG_byte_len</td>
<td>64</td>
</tr>
<tr>
<td>L1 blocks AAD(padded)</td>
<td>1</td>
</tr>
<tr>
<td>L2 blocks MSG(padded)</td>
<td>4</td>
</tr>
</tbody>
</table>

BYTES ORDER

<table>
<thead>
<tr>
<th>LSBS--------------------------</th>
<th>MSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000000000000000000000000000</td>
<td>03000000000000000000000000000000</td>
</tr>
<tr>
<td>01000000000000000000000000000000</td>
<td>01000000000000000000000000000000</td>
</tr>
<tr>
<td>00000000000000000000000000000000</td>
<td>02000000000000000000000000000000</td>
</tr>
<tr>
<td>03000000000000000000000000000000</td>
<td>03000000000000000000000000000000</td>
</tr>
<tr>
<td>04000000000000000000000000000000</td>
<td>04000000000000000000000000000000</td>
</tr>
<tr>
<td>05000000000000000000000000000000</td>
<td>05000000000000000000000000000000</td>
</tr>
<tr>
<td>01000000000000000000000000000000</td>
<td>01000000000000000000000000000000</td>
</tr>
<tr>
<td>02000000000000000000000000000000</td>
<td>02000000000000000000000000000000</td>
</tr>
<tr>
<td>03000000000000000000000000000000</td>
<td>03000000000000000000000000000000</td>
</tr>
<tr>
<td>04000000000000000000000000000000</td>
<td>04000000000000000000000000000000</td>
</tr>
<tr>
<td>05000000000000000000000000000000</td>
<td>05000000000000000000000000000000</td>
</tr>
<tr>
<td>08000000000000000000000000000000</td>
<td>08000000000000000000000000000000</td>
</tr>
</tbody>
</table>

Computing POLYVAL on a buffer of 5 blocks + LENBLK.

POLYVAL = 1b00000000000000000008c841a01712a376e
POLYVAL_xor_NONCE = 18000000000000000008c841a01712a376e
with MSBit cleared = 18000000000000000008c841a01712a376e
TAG = 49650717f842d3d193e3cc498e80f2c7
AAD = 01
CT = c17abb9e321814304f3844af4c90cb8e
Encryption_Key = a89be09bd7a43a05021266c59a31609a

APPENDIX

KEY_SCHEDULE (Encryption_Key)

c88735c9fb99fd54d4c805dcf487f5ae

c88735c9fb99fd54d4c805dcf487f5ae

c19a3fba65980e6f4b5fe1545a05a30d

76ec3f188d75c24459bdc798ad3a3236

43b93a2f26213406d7ed514377b7619

ecc07cc61b8c588380520210953f3026

32bdcd05149cf94579e22514e995a48

c323b99eaf27c169a9e7e060fa1e420

08927a731c0e833665ecaf672b75f52f

32be5f8b9025239d0abb59b501a13bb

baef9018a6e1132e30dbc49e8784966

a90264b839274725339c1abe36860905

deeef1d780e83bb02547a5381a1dc

44d8c0247df87014e639def78e594ba

47cc0fa13fc3e79284c1b3e8d7bbaf4

CTRBLKS (with MSbit set to 1)

00000000f842d3d193e3cc498e80f2c7

01000000f842d3d193e3cc498e80f2c7

02000000f842d3d193e3cc498e80f2c7

03000000f842d3d193e3cc498e80f2c7

--------------------- 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

00010203040506070809101112131415

---------------------

K1 = H =

03000000000000000000000000000000

K2 = K =

01000000000000000000000000000000

NONCE =

03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 02000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL = d8000000000000c048000000f050f665
POLYVAL_xor_NONCE = db000000000000c048000000f050f665
with MSBit cleared = db000000000000c048000000f050f665
TAG = 0ee2162b829d1b8087a61dec79c2b4dd
AAD = 01000000000000000000000000000000
CT = 7f25e1eb
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735c9f9d5cd4805dcf487f5ae

KEY_SCHEDULE (Encryption_Key)

APPENDIX

CTRBLKS (with MSbit set to 1)

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
00010203040506070809101112131415
--------------------------------

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
0200
MSG =
03000000000000000000000000000000
04000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK =
900000000000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL =
080100000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE =
0b0100000000000c06b01c04c63ad9807
with MSBit cleared =
0b0100000000000c06b01c04c63ad9807
TAG =
07e3ed3f0c192bb05b8de76bba7901aa
AAD =
01000000000000000000000000000000
0200
CT =
4f39b03cf9f45d747e576ff1a382004
54b94c28
Encryption_Key =
d77cdb05a40231d52ec7ef3b115a4259
c88735cffbf99f5cd4c805dcf487f5ae

********************************************************************************
APPENDIX
********************************************************************************

KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735cffbf99f5cd4c805dcf487f5ae
c19af6ba65980e6f4b5fe1545a05a30d76ec3f188d75c244590dc798ad3a323643b73a2f262134067ed514377b761eccd07cc61b8c58838050210953f032632bdc05149cf94579e22c514e995a48c323b99ea29b7c169a9e7e060fa14e2008927a731c0e833665ecaf672b75f52f32be5f89b025239d0abb59b501a13bb
CTRBLKS (with MSbit set to 1)

0000000000c192bb05b8de76bba7901aa
0100000000c192bb05b8de76bba7901aa

--------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
00000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
02000000
MSG =
03000000000000000000000000000000
0400
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK =
a00000000000000000000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL =
6401000000000000600701c04c63add8de
POLYVAL_xor_NONCE =
6701000000000000600701c04c63add8de
with MSBit cleared =
6701000000000000600701c04c63add85e
TAG =
33f0e38bd6fb197ed4f7eaaea861d60b
AAD =
01000000000000000000000000000000

CT = 625534f47020a12f11754fbc86ed46cf41d0
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5c4805dcf487f5ae

************
APPENDIX
************

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5c4805dcf487f5ae
c19a3fba65980e64b5e154a5a5a30d 
76ec3f188d75c24459bcd798ada3a3236 
43b93a2f26213406d7ed514377b7619 
ecc07cc61b8c58838050210953f3026 
32bdcd05149cf94579e22514e995a48 
c323b99ea92b7c169a9e7e060fa4e20 
08927a732c2e33665ecaf6727f5f2f 
32be5f8b9025239d0abb59b051a13bb 
baef9018a6e1132e330d4e98784966 
a90264b889274725339c1abe36860905 
deefb1d780fe83bb02547a537a1dccc 
44d8c247df87014e639dbf78e594ba 
077c0fa13fc3e79284c1b3e8d7baef4

CTRBLKS (with MSbit set to 1)

00000000d6fb197ed4f7eaaea861d68b 
01000000d6fb197ed4f7eaaea861d68b

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

AAD_bytes_len = 0
AAD_bit_len = 0
MSG_bytes_len = 0
MSG_bit_len = 0
padded_AAD_bytes_len = 0
padded_MSG_bytes_len = 0
L1 blocks AAD(padded) = 0
L2 blocks MSG(padded) = 0

BYTES ORDER
LSB--------------------------MSB
00010203040506070809101112131415 

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 00000000000000000000000000000000
AAD = 03000000000000000000000000000000
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 = de1a5fcd85a5217d91d8b349ab9cd224
AAD =
CT =
Encryption_Key =

APPENDIX

KEY_SCHEDULE (Encryption_Key)

-------------- 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
00010203040506070809101112131415

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

Computing POLYVAL on a buffer of 1 blocks + LENBLK.
POLYVAL =
04000000000000000000000000000000080910000000000283b1c
POLYVAL_xor_NONCE =
07000000000000000000000000000000080910000000000283b1c
with MSBit cleared =
07000000000000000000000000000000080910000000000283b1c
TAG =
90d1e4ad87f53bf3eb26c066193fd3f
AAD =
4b0619edd74c6a09
CT =
c88735ccfbb99fd5cd4c805df487f5ae
Encryption_Key =
d77cdb05a40231d52ec7ef3b115a4259

APPENDIX
**************

KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735ccfbb99fd5cd4c805df487f5ae
c19a3fba65980e6f4b5fe154a5a30d
c19a3fba65980e6f4b5fe154a5a30d
76ec3f188d75c24459bdc79ad3a3236
43b93a2f2621344067ed514377b7619
eecc07cc61b8c58838050210953f3026
32b6d9c05149cf49579e22c514e995a48
c323b99ea29b7c169a9e7e060fa1e20
08927a731c0e833665eacaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dcb49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc5e79284c1b3e8d7baef4

CTRBLKS (with MSbit set to 1)
0000000087f53fbf3eb26c066193fd3

------------------------ 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 = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000006000000000000000

Computing POLYVAL on a buffer of 1 blocks + LENBLK.

POLYVAL = 040000000000000400d90000000283b1c
POLYVAL_xor_NONCE = 070000000000040d90000000283b1c
with MSBit cleared = a42c36bcd7dd95273c5ded5a5ab0a8fc
AAD = ea410b6727fe50357dc2c9f9
CT = d77cdb05a40231d52ec7ef3b115a4259
c88735c9fb9fd5cd4805d487f5ae

Encryption_key = d77cdbc05a40231d52ec7ef3b115a4259
c88735c9fb9fd5cd4805d487f5ae
c19a3fba65980e6f4b5e1545a0a5a307
76ec3f188d75c24459c0798ad3a3236
43b93a2f26213406d7ed514377b7619
eccd07cc61b8c58838052010953f3026
32bdc05149cf94579e22c514e995a48

CTRBLKS (with MSbit set to 1)

00000000d7dd95273c5ded5a5ab0a8fc

--------------------- 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
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
MSG =
01000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
LENBLK =
00000000000000000000000000000000

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.
POLYVAL =
040000000000000000000000000000000000000000000000000000000023010000000000283b1c
POLYVAL_xor_NONCE =
0700000000000000000000000000000000000000000000000000000000230100000000000283b1c
with MSBit cleared =
07000000000000000000000000000000000000000000000000000000002301000000000000283b1c
TAG =
a86f26245dea30d23ec045223ef5851e
AAD =
CT =
d5d6c0782d45de97a027156334229387
Encryption Key =
d77cbeb05a40231d52ec7ef3b115a4259
c88735ccfb99fd5cd4c805dcf487f5ae
APPENDIX

KEY_SCHEDULE (Encryption_Key)

\[
d77cdb05a40231d52ec7ef3b115a4259
c88735cfff99f5c40855cf487f5ace
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c42459bd798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29bc169a9e7e060fa14e20
08927a731c0e83665eceaf672b75f52f
32be5f8b9025239d0abb59b51a13bb
badf90186e1132ec30db49e8788966
a90264b839274725339c1abe36860905
deefb1d780fe833bb0254765371a1dc
44d8c0247df87014e639dbf78e594ba
47cc0fa13fc3e79284c13e8d7bbaf4
\]

CTRBLKS (with MSbit set to 1)

\[
000000005dea30d23ec045223ef5859e
\]

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

<table>
<thead>
<tr>
<th>AAD_byte_len</th>
<th>AAD_bit_len</th>
<th>MSG_byte_len</th>
<th>MSG_bit_len</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>32</td>
<td>256</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>32</td>
<td>2</td>
</tr>
</tbody>
</table>

BYTES ORDER

<table>
<thead>
<tr>
<th>LSB</th>
<th>MSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>00010203040506070809101112131415</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K1 = H</th>
</tr>
</thead>
<tbody>
<tr>
<td>03000000000000000000000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K2 = K</th>
</tr>
</thead>
<tbody>
<tr>
<td>01000000000000000000000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NONCE =</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000000000000000000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAD =</th>
</tr>
</thead>
<tbody>
<tr>
<td>03000000000000000000000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MSG =</th>
</tr>
</thead>
<tbody>
<tr>
<td>01000000000000000000000000000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PADDED_AAD_and_MSG =</th>
</tr>
</thead>
<tbody>
<tr>
<td>02000000000000000000000000000000</td>
</tr>
</tbody>
</table>

LENBLK = 00000000000000000001000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL = 01000000000000000004602000F0507615
POLYVAL_xor_NONCE = 02000000000000000004602000F0507615
with MSBit cleared = ac78c482d3499b26ae97bf353c21bdb
AAD = cac82890d7f5a8330fa2f0f03701901a
CT = ed8a98666b42f74cc1887bd91864cf37
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cfff99fd5cd4c805dfcf487f5ae
c19afba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f26213406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdc05dcdcf94579e22c514e995a48
c323b99ea29b7c169a9e0e6f0fa4e20
08927a731c0e833665eacaf72b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132e3d0b49e8784966
a90264b839274725339c1abe36860905
deeef1d780fe833bbb02547a53ald1c
44d8c0247df87014e639dbf78e594ba
47cc0fa3fc3e79284c1b3e8d7bbaef4

CTRBLKS (with MSbit set to 1)

00000000d3499b26ae97bf353c21bd0
01000000d3499b26ae97bf353c21bd0

--------------------- 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
0010203040506070809101112131415

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000000000000000000000

Computing POLYVAL on a buffer of 3 blocks + LENBLK.
POLYVAL = 0e00000000000000650300203e788f7f
POLYVAL_xor_NONCE = 0d00000000000000650300203e788f7f
with MSBit cleared = 0d00000000000000650300203e788f7f
TAG = d47a0762c2de1a33c87a450f8c1b3
AAD = bd562c8f8bbde467149c17a3f316fd2c
CT = 8859c748760332d3296a5b233c4059e3
e70a042fc2b1812f484801a184b23ae
Encryption_Key = d77c0b5a04231d52ec7ef3b115a4259
c88735c0ff9fd5c4805dcf487f5ae

************************************************
APPENDIX
************************************************

KEY_SCHEDULE (Encryption_Key)
d77c0b5a04231d52ec7ef3b115a4259
c88735c0ff9fd5c4805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd076cc1b8c58838050210953f3026
32bcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa1e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a3bb
baef9018a6e1132ec30dcb49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c

Gueron, et al. Expires October 16, 2016 [Page 74]
CTRBLKS (with MSbit set to 1)

<table>
<thead>
<tr>
<th>Block</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000000002c2dea133c87aaea50fb1c1b3</td>
</tr>
<tr>
<td>1</td>
<td>0100000002c2dea133c87aaea50fb1c1b3</td>
</tr>
<tr>
<td>2</td>
<td>0200000002c2dea133c87aaea50fb1c1b3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAD_byte_len</td>
<td>0</td>
</tr>
<tr>
<td>AAD_bit_len</td>
<td>0</td>
</tr>
<tr>
<td>MSG_byte_len</td>
<td>64</td>
</tr>
<tr>
<td>MSG_bit_len</td>
<td>512</td>
</tr>
<tr>
<td>padded_AAD_byte_len</td>
<td>0</td>
</tr>
<tr>
<td>padded_MSG_byte_len</td>
<td>64</td>
</tr>
<tr>
<td>L1 blocks AAD(padded)</td>
<td>0</td>
</tr>
<tr>
<td>L2 blocks MSG(padded)</td>
<td>4</td>
</tr>
</tbody>
</table>

BYTES ORDER

<table>
<thead>
<tr>
<th>Byte</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00010203040506070809101112131415</td>
</tr>
</tbody>
</table>

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 00000000000000000002000000000000

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

<table>
<thead>
<tr>
<th>POLYVAL</th>
<th>0f0000000000000000000008c04c04c63ad584f</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLYVAL_xor_NONCE</td>
<td>0c0000000000000000000008c04c04c63ad584f</td>
</tr>
<tr>
<td>with MSBit cleared =</td>
<td>0c0000000000000000000008c04c04c63ad584f</td>
</tr>
<tr>
<td>TAG</td>
<td>15e4bd316b19caaa3a3493381a3e4153c</td>
</tr>
<tr>
<td>AAD</td>
<td>d53e727defb0fe560c87f405ab19b1a2</td>
</tr>
</tbody>
</table>

Encryption_Key =
6fd85249324b974564c477b2eb4d4162
943fa821946537d507e0713dcc556075
220130acb5f3daa8dd4ee9af3b36642
d77cdb05a40231d52e7ebf3b115a4259
c88735cfff99fd4c805dce487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)
6fd85249324b974564c477b2eb4d4162
d77cdb05a40231d52e7ebf3b115a4259
c88735cfff99fd4c805dce487f5ae
c19a3fba65980e64f5e1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c5883805021093f3026
32bdc05149cf94579e22c514e99a48
c323b99ea29b7c169a9e7e060fa1e20
08927a731c0e33665ecaf672b75f52f
32be5f89b025239d0abb59b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264ba8392747253391cabe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247dfe87014e639dbf7e594ba
47cc0fa13fc3e79284c1b3e8d7bbbaef4

CTRBLKS (with MSbit set to 1)
000000006b19caaa3a3493a81a3e415bc
010000006b19caaa3a3493a81a3e415bc
020000006b19caaa3a3493a81a3e415bc
030000006b19caaa3a3493a81a3e415bc

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
00010203040506070809101112131415

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

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL = 130000000000008091000000f0501631
POLYVAL_xor_NONCE = 100000000000008091000000f0501631
with MSBit cleared = 100000000000008091000000f0501631
TAG = 4cac1deb89734986b5f0546c661932e9
AAD = 01
CT = 8e5a22875d5d692e
Encryption_Key = d77cddb05a40231d52ec7ef3b115a4259
                c88735cffb99fd5cd4805dcf487f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key) d77cddb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a3bb
baef9018a6e1132ec30d4e9e8784966
a90264bb39274725339c1abe36860905
deeefbd780fe833bb02547a537a1d1c
44d8c0247df87014e639dbf7e8594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

CTRBLKS (with MSbit set to 1)

0000000089734986b5f0546c661932e9

--------------------- 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
00010203040506070809101112131415

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
PADDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
LENBLK =
08000000000000000000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.

POLYVAL =
13000000000000040d9000000f051631
POLYVAL_xor_NONCE =
10000000000000040d9000000f051631
with MSBit cleared =
10000000000000040d9000000f051631
TAG =
42794bd56cd0b78ebdad8dc2c2c11720
AAD =
01
CT =
ed921994f8d27a9d941bfb6f
Encryption_Key =
d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805dcf487f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459dcd798ad3a11236
43b93a2f26213406d7ed514377b7619
ecc07d619cc8588590210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99a929b7c169a9e7e06fa14e20
08927a731c0e833665e9caf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec3d0b49e8784966
a90264b839274725339c1abe36860905
CTRBLKS (with MSbit set to 1)

0000000006cd0b78ebdad8dc2c2c117a0

------------------------ 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
00000000000000006cd0b78ebdad8dc2c2c117a0

K1 = H =
K2 = K =
NONCE =
AAD =
MSG =
PADDDED_AAD_and_MSG =
LENBLK =

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
PONGYAL =
POLYVAL_xor_NONCE =
with MSBit cleared =
TAG =
AAD =
CT =
Encryption Key =

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key)  
d77cdb05a40231d52ec7ef3b115a4259  
c88735cfff9f5cd4c805dcf487f5ae  
c19a3fba65980e6f4b5fe1545a05a30d  
76ec3f188d75c24459bdc798ad3a3236  
43b93a2f262134406d7ed514377b7619  
eccd07cc61b8c58838050210953f3026  
32bdc05149cf94579e22c514e995a48  
c323b99ea29b7c169a9e7e060fa14e20  
0892a731c0e833665ecaf67275f52f  
32be5f8b9025239d0abb5d9b051a13bb  
baff918a6e1132ec30d49e8784966  
a90264b39274725339c1abe3e860905  
deefb1d780fe831bb02547a537a1d1c  
44d8c02474f87014639dbf78e594ba  
47cc0f13fc3e79284c13eb387bbaef4  

CTRBLKS (with MSbit set to 1)  
00000000ee961567ee5a686a3ac66ef4  

--------------------- 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  
00010203040506070809101112131415  

K1 = H =  
03000000000000000000000000000000  
K2 = K =  
01000000000000000000000000000000  
00000000000000000000000000000000  
NONCE =  
03000000000000000000000000000000  
AAD =  
01  
MSG =  
02000000000000000000000000000000  
03000000000000000000000000000000  
PADDDED_AAD_and_MSG =  
01000000000000000000000000000000  
02000000000000000000000000000000  
03000000000000000000000000000000  
LENBLK =  
08000000000000000000000000000000
Computing POLYVAL on a buffer of 3 blocks + LENBLK.

POLYVAL = 1c00000000000000460200203e78ef5b
POLYVAL_xor_NONCE = 1f00000000000000460200203e78ef5b
with MSBit cleared = 1f00000000000000460200203e78ef5b
TAG = c558db375fc7fb253b477d990435e79
AAD = 01
CT = b1403a920a945105017054cc7754e54
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cfbb99fd4c805dcf487f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)

d77cdb05a40231d52ec7ef3b115a4259
c88735cfbb99fd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a2336
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bcdc05149cf94579e22c514e995a48
323b99ea297c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b05a13bb
baef9018a6e1132ec30d9b5e874966
a90264b83927425339c1abe36860905
deee1d780f833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e687f594ba
47cc0fa13fc3e79284c1b3e8d7bb9fa4

CTRBLKS (with MSbit set to 1)

0000000075fc7fb253b477d990435ef9
0100000075fc7fb253b477d990435ef9

--------------------- 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

<table>
<thead>
<tr>
<th>MSB</th>
<th>00010203040506070809101112131415</th>
</tr>
</thead>
</table>

\[
\begin{align*}
K_1 &= H = 03000000000000000000000000000000 \\
K_2 &= K = 01000000000000000000000000000000 \\
\text{NONCE} &= 03000000000000000000000000000000 \\
\text{AAD} &= 01 \\
\text{MSG} &= 02000000000000000000000000000000 \\
\text{PADDED_AAD_and_MSG} &= 01000000000000000000000000000000 \\
\text{LENBLK} &= 08000000000000008001000000000000 \\
\end{align*}
\]

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

\[
\begin{align*}
\text{POLYVAL} &= 1d000000000000006503c04c63ad386b \\
\text{POLYVAL_xor_NONCE} &= 1e000000000000006503c04c63ad386b \\
\text{with MSBit cleared} &= 1e000000000000006503c04c63ad386b \\
\text{TAG} &= 54538b4b90c4877f29632ec9441d9809 \\
\text{AAD} &= 01 \\
\text{CT} &= 687c9c5846e8fde28bc1bde37dd15b80 \\
& \quad 7ab731537d765e93f0d74bcac390ffbd \\
& \quad b71ddb1af7505791ca74e87c697120b8 \\
\text{Encryption_Key} &= d77cdb05a40231d52ec7ef3b115a4259 \\
& \quad c88735cfff99f5d4c805dfc487f5ae \\
\end{align*}
\]

\*\*\*\*\*\*

APPENDIX

\*\*\*\*\*\*

KEY_SCHEDULE (Encryption_Key)

\[
\begin{align*}
\text{d77cdb05a40231d52ec7ef3b115a4259} \\
\text{c88735cfff99f5d4c805dfc487f5ae} \\
\text{c19a3fba65980e6f4b5fe1545a05a30d} \\
& \quad 76ec3f188d75c24459bdc798ad3a3236 \\
& \quad 43b93a2f262134406d7ed514377b7619 \\
& \quad eccd07cc61b8c58838050210953f3026 \\
& \quad 32bdc05149cf94579e22c514e995a48 \\
& \quad c323b99ea29b7c169a9e7e60fa14e20 \\
& \quad 08927a731c0e833665ecaf672b75f52f \\
& \quad 32b5f8b9025239d0abb5d9b051a13bb \\
& \quad baef9018a6e1132ec30dbc49e8784966 \\
& \quad a90264b839274725339c1abe36860905 \\
& \quad deeeb1d780fe833bb02547a537a1d1c \\
& \quad 44d8c0247dff87014e639dbf7e594ba \\
\end{align*}
\]
CTRBLKS (with MSbit set to 1)

0000000090c4877f29632ec9441d9889
0100000090c4877f29632ec9441d9889
0200000090c4877f29632ec9441d9889

--------------------- 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
NONCE =
03000000000000000000000000000000
AAD =
01
MSG =
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
05000000000000000000000000000000
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
05000000000000000000000000000000
LENBLK =
08000000000000000002000000000000

Computing POLYVAL on a buffer of 5 blocks + LENBLK.

POLYVAL =
1b0000000000000000000000000000008c841a01712a376e

POLYVAL_xor_NONCE =
180000000000000000000000000000008c841a01712a376e

with MSBit cleared =
180000000000000000000000000000008c841a01712a376e

TAG =
49650717f842d3d193e3cc498e80f2c7

AAD =
01

CT =
c17abb9e321814304f3844af4c90cb8e
Encryption_Key =

d77c6b05a40231d52e976f3b115a4259

APPENDIX

KEY_SCHEDULE (Encryption_Key)  

d77c6b05a40231d52e976f3b115a4259

c88735c9f99fd5c4a85df8759f5ae

c19a3fba65980e6f4b5fe1545a05a30d

CTRBLKS (with MSbit set to 1)

00000000f842d3d193e3cc498e80f2c7
01000000f842d3d193e3cc498e80f2c7
02000000f842d3d193e3cc498e80f2c7
03000000f842d3d193e3cc498e80f2c7

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
00010203040506070809101112131415

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

K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 60000000000000002000000000000000

Computing POLYVAL on a buffer of 2 blocks + LENBLK.
POLYVAL = d8000000000000c048000000f050f665
POLYVAL_xor_NONCE = db000000000000c048000000f050f665
with MSBit cleared = db000000000000c048000000f050f665
TAG = 0ee2162b829d1b8087a61dec79c2b4dd
AAD = 01000000000000000000000000000000
CT = 7f25e1eb
Encryption_Key = d77c9b05a40231d52ec7ef3b115a4259
                     c88735c9fb99fd5cd4805dcf487f5ae

***************************
APPENDIX
***************************
KEY_SCHEDULE (Encryption_Key) d77c9b05a40231d52ec7ef3b115a4259
c88735c9fb99fd5cd4805dcf487f5ae
                          c19a3fba65980e6f4b5fe1545a05a30d
                          76ec3f18ed75c24459bd798ad3a236
                          43b93af267234406d7ed514377b7619
                          eccd07c61b8c5883805021095f3026
                          32bdc0d55149cf9579e225149e99a48
                          c323b829af2b7c1e9a9f7e089412f20
                          8929a731c0e533665ecaf67275ef52f
                          32b8f8b0925239d0abb5d9b595113bb
                          baef9018ae1123e3d049e878496
                          a90264b839274725339c1abe36860905
                          deee81d780fe833bb02547a537a1d1c
                          44d8c0247dfe87014e639d7f78e59ba
                          47c0fa13fc3e79284c8d8d7bbaef4

CTRBLKS (with MSbit set to 1)
00000000829d18087a61dec79c2b4dd

-------------- 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

Computing POLYVAL on a buffer of 4 blocks + LENBLK.

POLYVAL = 0801000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b0100000000000000c06b01c04c63ad9807
with MSBit cleared = 0b3ed3f0c192bb05b8de76bba7901aa
TAG = 07e3ed3f0c192bb05b8de76bba7901aa
AAD = 010000000000000000000000000000000200
MSG = 0300000000000000000000000000000004000000
PADDDED_AAD_and_MSG = 010000000000000000000000000000000200000003000000000000000000000000000000040000000000000000000000000000000
LENBLK = 90000000000000000000000000000000

Encryption_Key = d77c0db05a40231d52ec7ef3b115a4259
                  c88735c7b99fd5ce805dc087f5a

APPENDIX

KEY_SCHEDULE (Encryption_Key)

d77c0db05a40231d52ec7ef3b115a4259
c88735c7b99fd5ce805dc087f5a
c19a3fba65980e6f4b5fe1545a030d
c176ec3f188d75c2a4b9bdc798ad3a3236
c43b93a2f2b6213440676514377b7619
c88735c7b99fd5ce805dc087f5a

CTRBLKS (with MSbit set to 1)

0000000000c192bb05b8de76bba7901aa
0100000000c192bb05b8de76bba7901aa

--------------------- 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
00010203040506070809101112131415

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

K1 = H =
03000000000000000000000000000000
K2 = K =
01000000000000000000000000000000
NONCE =
03000000000000000000000000000000
AAD =
01000000000000000000000000000000
02000000
MSG =
03000000000000000000000000000000
0400
PADDDED_AAD_and_MSG =
01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK =
a000000000000009000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL =
64010000000000600701c04c63add8de
POLYVAL_xor_NONCE = 67010000000000600701c04c63add8de
with MSBit cleared = 67010000000000600701c04c63add85e
TAG = 33f0e38bd6fb197ed4f7eaaea861d60b
AAD = 010000000000000000000000000000000000000000
CT = 625534f47020a12f11754fbc86ed46cf41d0
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805d4f87f5ae

***************************
APPENDIX
***************************

KEY_SCHEDULE (Encryption_Key)
d77cdb05a40231d52ec7ef3b115a4259
c88735cffe99fd5cd4c805d4f87f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc799ad3a3236
43b93a2f26213406d7ed514377b7619
eccd07cc61bc8588380520193f34026
32bdc05149cf94579e22c514e995a48
c323b99e297c169a9e7e060fae14e20
08927a731c0e833665ecaf672b75f52f
32bea5f8b902529d0abb5d9b051a3bb
baef9018a6e1132ec30db49e8784966
a0264b83927425339c1abe36860905
deefbf1d780fe83b02547a537a1d1c
44d8c0247ff87014e639d5b7e594ba
47cc0fa13fc3e79284c1b3e8d7bae6f4

CTRBLKS (with MSbit set to 1)
00000000d6fb197ed4f7eaaea861d68b
01000000d6fb197ed4f7eaaea861d68b

Authors’ Addresses

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

Email: shay@math.haifa.ac.il