

CFRG	S. Gueron
Internet-Draft	University of Haifa and Intel Corporation
Intended status: Informational	A. Langley
Expires: October 16, 2016	Google
	Y. Lindell
	Bar Ilan University
	April 14, 2016

AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption
draft-gueron-gcmsiv-03

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

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

Table of Contents

1.	Introduction	2
2.	Requirements Language	3
3.	POLYVAL	3
4.	Encryption	4
5.	Decryption	4
6.	AEADs	5
7.	Field operation examples	5
8.	Worked example	6
9.	Security Considerations	7
10.	IANA Considerations	7
11.	Acknowledgements	7
12.	References	7
12.1.	Normative References	7
12.2.	Informative References	8
Appendix A.	Test vectors	8
A.1.	AEAD_AES_128_GCM_SIV	8
A.2.	AEAD_AES_256_GCM_SIV	46
	Authors' Addresses	88

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: $\text{dot}(a, b)$, where $\text{dot}(a, b) = a * b * x^{-128}$. 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 be 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 $X_1, \dots, X_s$. 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 $\text{POLYVAL}(H, X_1, X_2, \dots)$ is equal to $\text{ByteSwap}(\text{GHASH}(x^*H, \text{ByteSwap}(X_1), \text{ByteSwap}(X_2), \dots))$, where ByteSwap is a function that converts a field element to a 128-bit string, reverses the order of the bytes, and interprets the result as a field element again.

4. Encryption

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

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

Alternatively, if the AES key is 32 bytes long then AES-256 is used throughout. 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 `len(additional_length)*8` and `len(plaintext)*8`. Pad the plaintext and additional data with zeros until they are each a multiple of 16 bytes, the AES block size. Then `X_1`, `X_2`, etc (the series of field elements that are inputs to POLYVAL) are the concatenation of the padded additional data, the padded plaintext and the length block.

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

The ciphertext is produced by using AES in counter mode on the unpadded plaintext. The initial counter 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 `length_block` and `X_1`, `X_2`, etc as above and compute `S_s = POLYVAL(authentication_key, X_1, X_2, ...)`. Compute the expected tag by XORing `S_s` and the nonce, setting the most-significant byte of the last byte to zero and encrypting with the record-encryption key. Compare the provided and expected tag values in constant time. If they do not match, fail. Otherwise return the plaintext.

6. AEADs

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

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

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

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

7. Field operation examples

Polynomials in this document will be written as 16-byte values. For example, the sixteen bytes `010000000000000000000000000000492` would represent the polynomial $x^{127} + x^{124} + x^{121} + x^{114} + 1$, which is also the value of x^{-128} in this field.

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

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 $752abad3e0afb5f434dc4310f71f3d21$.

The record encryption key will be $\text{AES}(\text{key} = fab3a110b8ae672eba07d91ba52d6cea, \text{data} = 752abad3e0afb5f434dc4310f71f3d21) = b55e60e9e8886006db16db23e1e0e103$.

The length block contains the encoding of the bit-lengths of the additional data and plaintext, respectively, which are 56 and 88. Thus `length_block` is $3800000000000000058000000000000000$.

The input to POLYVAL is the padded additional data, padded plaintext and then the length block. This is $6578616d706c65000000000000000000048656c6c6f20776f726c64000000000058000000000000000380000000000000$.

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

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

In order to form the initial counter block, the most-significant bit of the last byte of the tag is set to one and a 32-bit, little-endian counter is written to the first four bytes. This gives $0000000054c0997cae05d8b2be1d96be$. Encrypting this with the record key gives the first block of the keystream: $b30b19ed9ba05d29b6aecc0146b7fb19$.

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

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

12.2. Informative References

- [GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST SP-800-38D, November 2007, <<http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>>.
- [GCM-SIV] Gueron, S. and Y. Lindell, "GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle Per Byte", Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, <<http://doi.acm.org/10.1145/2810103.2813613>>.
- [RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", [RFC 5116](#), DOI 10.17487/RFC5116, January 2008, <<http://www.rfc-editor.org/info/rfc5116>>.

Appendix A. Test vectors

A.1. AEAD_AES_128_GCM_SIV

```

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

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

                                BYTES ORDER
                                LSB-----MSB
                                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 =                     fabfd7964630aa612ee6269f061f08b
AAD =
CT =
Encryption_Key=          57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

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

```

AAD_byte_len = 0
AAD_bit_len  = 0
MSG_byte_len = 8
MSG_bit_len  = 64
padded_AAD_byte_len = 0
padded_MSG_byte_len = 16
L1 blocks AAD(padded) = 0
L2 blocks MSG(padded) = 1

```

BYTES ORDER

```

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

```

```

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

```



```

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.
POLYVAL = 0400000000000000809100000000283b1c
POLYVAL_xor_NONCE = 0700000000000000809100000000283b1c
with MSBit cleared = 0700000000000000809100000000283b1c
TAG = 5537355b0a4f4cb05ce77d1b815d7299
AAD =
CT = 3b0f5baabe526e9f
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

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
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 = 040000000000000040d9000000000283b1c
POLYVAL_xor_NONCE = 070000000000000040d9000000000283b1c
with MSBit cleared = 070000000000000040d9000000000283b1c
TAG = dd55830c690eadd7fd2155b3615470bd
AAD =
CT = 9391b4122fccfecb60ec40ab
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (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 =
MSG =                          01000000000000000000000000000000
PADDED_AAD_and_MSG =          01000000000000000000000000000000
LENBLK =                       00000000000000000800000000000000

```

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.

```

POLYVAL =                      040000000000000002301000000283b1c
POLYVAL_xor_NONCE =            070000000000000002301000000283b1c
with MSBit cleared =           070000000000000002301000000283b1c
TAG =                          147650d36f064f6b5dbbe8f04077d903
AAD =
CT =                           565e4a931280ecdece8620abcf90b65e
Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (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 =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
LENBLK = 000000000000000000000000100000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL = 0100000000000000046020000f0507615
POLYVAL_xor_NONCE = 0200000000000000046020000f0507615
with MSBit cleared = 0200000000000000046020000f0507615
TAG = 78a50cb3f901ee38c588f6662d785a24
AAD =
CT = 9b1d2ba7d2d3a02efeccc18d03be2b56
      1753b147ae642183f2c4bbd72e4ed8e1
      57d4b7aec8de993e30a6861b61e6ce4e

Encryption_Key=

```

```
*****
```

APPENDIX

```
*****
```

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafc9d9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

```
CTRBLKS (with MSbit set to 1)
```

```

00000000f901ee38c588f6662d785aa4
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 =
MSG =                           01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
PADDED_AAD_and_MSG =           01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
LENBLK =                        00000000000000000800100000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.
POLYVAL =                      0e000000000000000650300203e788f7f
POLYVAL_xor_NONCE =            0d000000000000000650300203e788f7f
with MSB bit cleared =         0d000000000000000650300203e788f7f
TAG =                          a75aa62b704e826d984a72184e370598
AAD =
CT =                            dcc8d2f2c0e30b565f5d3ef58bf6638f
                                f50e8909ced008e0515b79f7c8c3d1f5
                                8ec1bb09177133b4cd1b375911d81579
Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

```

* * * * *

APPENDIX

KEY_SCHEDULE (Encryption_Key)	57d4b7aec8de993e30a6861b61e6ce4e d85f98411081017f2027876441c1492a a2647dc2b2e57cbd92c2fbd9d303b2f3 dd5370a46fb60c19fd74f7c02e774533 203db3954f8bbf8cb2ff484c9c880d7f f4ea614bbb61dec7099e968b95169bf4 93fede61289f00a62101962db4170dd9
-------------------------------	--


```

2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```

000000000704e826d984a72184e370598
010000000704e826d984a72184e370598
020000000704e826d984a72184e370598

```

----- 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 =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
      03000000000000000000000000000000
      04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                     02000000000000000000000000000000
                     03000000000000000000000000000000
                     04000000000000000000000000000000
LENBLK = 00000000000000000000000020000000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```

POLYVAL = 0f0000000000000008c04c04c63ad584f
POLYVAL_xor_NONCE = 0c0000000000000008c04c04c63ad584f
with MSBit cleared = 0c0000000000000008c04c04c63ad584f
TAG = d7f4efe2f6c72e3b8df168cab6b790ab
AAD =

```



```

CT =
472d6309563c74b6d5497145e929725a
ab08979e6c4fc72c30c2e3a1ce568b94
92e1b0351167937ee2faae79d40af93e
24eee045fdab1b2040440632f1a34433
Encryption_Key=
57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceae6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

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 = 0200000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
LENBLK = 08000000000000004000000000000000
```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```
POLYVAL = 13000000000000008091000000f0501631
POLYVAL_xor_NONCE = 10000000000000008091000000f0501631
with MSBit cleared = 10000000000000008091000000f0501631
TAG = 633c11b2eee1f65be0e3f1e0c824c5e0
AAD = 01
CT = 5adcda74026afb99
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e
```

APPENDIX

```
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633
```

CTRBLS (with MSbit set to 1)

```
00000000eee1f65be0e3f1e0c824c5e0
```

----- 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 =                       08000000000000000600000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL =                      13000000000000040d9000000f0501631
POLYVAL_xor_NONCE =            10000000000000040d9000000f0501631
with MSBit cleared =          10000000000000040d9000000f0501631
TAG =                          f229e75b2c4c3048fc70f163c9aefe0d
AAD =                          01
CT =                           b4fabbadb27257bbe8b807d5
Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```

000000002c4c3048fc70f163c9aefe8d

```

----- 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 = 08000000000000000080000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL = 13000000000000000023010000f0501631
POLYVAL_xor_NONCE = 10000000000000000023010000f0501631
with MSBit cleared = 10000000000000000023010000f0501631
TAG = cfb5aa16cdd9d39acc5d99b6eee2c6fc
AAD = 01
CT = dce7c7cd4d1060fdc663b9fe8de25385
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

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

```

CTRBLKS (with MSbit set to 1)

```
00000000cdd9d39acc5d99b6eee2c6fc
```



```

----- 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
PADDED_AAD_and_MSG =            01000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
LENBLK =                        08000000000000000000000000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.
POLYVAL =                      1c00000000000000460200203e78ef5b
POLYVAL_xor_NONCE =            1f00000000000000460200203e78ef5b
with MSBBit cleared =          1f00000000000000460200203e78ef5b
TAG =                           8df5606f057468e4b38e89736255ad2d
AAD =                            01
CT =                            c6d3098e12ac653520764cbccdb90655
                                b3d91bf034f7549d5f775fca5d6ad34f
Encryption_Key=                 57d4b7aec8de993e30a6861b61e6ce4e

```

* * * * *

APPENDIX

* * * * *

```
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9d9a374
```


6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

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
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
	04000000000000000000000000000000
LENBLK =	08000000000000000800100000000000

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=	57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

```
KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633
```

CTRBLKS (with MSbit set to 1)

```
000000004d6111c74edf5d95855256a2
010000004d6111c74edf5d95855256a2
020000004d6111c74edf5d95855256a2
```

----- 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
      01000000000000000000000000000000
      02000000000000000000000000000000
      03000000000000000000000000000000
```

PADDED_AAD_and_MSG =


```

                                04000000000000000000000000000000
                                05000000000000000000000000000000
LENBLK =                        08000000000000000002000000000000

```

Computing POLYVAL on a
buffer of 5 blocks + LENBLK.

```

POLYVAL =                      1b0000000000000008c841a01712a376e
POLYVAL_xor_NONCE =            180000000000000008c841a01712a376e
with MSBit cleared =          180000000000000008c841a01712a376e
TAG =                          668fc00b6b40b4bb0c8d6cdb9730358d
AAD =                          01
CT =                           499ec09c83c2b79cf6b219e6b79ec81c
                                7c7b572c8a04b322094ec011e7003ded
                                388627f831ee79bd3df5db27f648125a
                                fbfe2774388c34bb652b866ca84bdc8d
                                57d4b7aec8de993e30a6861b61e6ce4e
Encryption_Key=

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```

                                0000000006b40b4bb0c8d6cdb9730358d
                                0100000006b40b4bb0c8d6cdb9730358d
                                0200000006b40b4bb0c8d6cdb9730358d
                                0300000006b40b4bb0c8d6cdb9730358d

```

----- 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 = 60000000000000000200000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL = d800000000000000c048000000f050f665
POLYVAL_xor_NONCE = db00000000000000c048000000f050f665
with MSBit cleared = db00000000000000c048000000f050f665
TAG = 488346eaebe2d64ffa58e0fa82f8cd43
AAD = 01000000000000000000000000000000
CT = 7d5240be
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

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

```

CTRBLS (with MSbit set to 1)

```
00000000e0be2d64ffa58e0fa82f8cdc3
```

----- 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 = 900000000000000000a0000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 0801000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b01000000000000c06b01c04c63ad9807
with MSBit cleared = 0b01000000000000c06b01c04c63ad9807
TAG = d010794cfdbbc65ef641b8ccb9c2dda3
AAD = 01000000000000000000000000000000
0200
CT = 6d98c309d4f472480c5b1389e83569e5
217ddb9c
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be

```



```

437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

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 = a0000000000000000000000000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```

POLYVAL = 6401000000000000600701c04c63add8de
POLYVAL_xor_NONCE = 6701000000000000600701c04c63add8de
with MSBit cleared = 6701000000000000600701c04c63add85e
TAG = 98e16515942fb8ff9ef108e7ce53a963
AAD = 01000000000000000000000000000000
02000000
CT = 4649087685b01b476bd3420f36ca67d3
b18b

```


Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

00000000942fb8ff9ef108e7ce53a9e3
01000000942fb8ff9ef108e7ce53a9e3

----- 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 =
PADDED_AAD_and_MSG =
LENBLK = 00000000000000000000000000000000

Computing POLYVAL on a
buffer of 0 blocks + LENBLK.


```

POLYVAL =                                00000000000000000000000000000000
POLYVAL_xor_NONCE =                      03000000000000000000000000000000
with MSBit cleared =                     03000000000000000000000000000000
TAG =                                     fabfd7964630aa6128ee6269f061f08b
AAD =
CT =
Encryption_Key=                           57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafcd9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (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 =                                0100000000000000
PADDED_AAD_and_MSG =                    01000000000000000000000000000000

```


LENBLK = 0000000000000000004000000000000000

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.

POLYVAL = 0400000000000000809100000000283b1c
 POLYVAL_xor_NONCE = 0700000000000000809100000000283b1c
 with MSBit cleared = 0700000000000000809100000000283b1c
 TAG = 5537355b0a4f4cb05ce77d1b815d7299
 AAD =
 CT = 3b0f5baabe526e9f
 Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
 d85f98411081017f2027876441c1492a
 a2647dc2b2e57cbd92c2fbd9d303b2f3
 dd5370a46fb60c19fd74f7c02e774533
 203db3954f8bbf8cb2ff484c9c880d7f
 f4ea614bbb61dec7099e968b95169bf4
 93fede61289f00a62101962db4170dd9
 2329ebec0bb6eb4a2ab77d679ea070be
 437845e748ceaead6279d3cafc9a374
 6d72d75725bc79fa47c5aa30bb1c0944
 c773ccbde2cfb547a50a1f771e161633

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

00010203040506070809101112131415

K1 = H = 03000000000000000000000000000000


```

K2 = K =          01000000000000000000000000000000
NONCE =          03000000000000000000000000000000
AAD =
MSG =          01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK =        00000000000000000060000000000000

```

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.

```

POLYVAL =          040000000000000040d9000000000283b1c
POLYVAL_xor_NONCE = 070000000000000040d9000000000283b1c
with MSBit cleared = 070000000000000040d9000000000283b1c
TAG =          dd55830c690eadd7fd2155b3615470bd
AAD =
CT =          9391b4122fccfecb60ec40ab
Encryption_Key=    57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

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 =
MSG =                          01000000000000000000000000000000
PADDED_AAD_and_MSG =          01000000000000000000000000000000
LENBLK =                       00000000000000000800000000000000

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.
POLYVAL =                     040000000000000002301000000283b1c
POLYVAL_xor_NONCE =           070000000000000002301000000283b1c
with MSBit cleared =          070000000000000002301000000283b1c
TAG =                          147650d36f064f6b5dbbe8f04077d903
AAD =
CT =                           565e4a931280ecdece8620abcf90b65e
Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```
0000000006f064f6b5dbbe8f04077d983
```

----- 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 =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
LENBLK = 00000000000000000000000000000000
      00000000000000000000000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL = 01000000000000000046020000f0507615
POLYVAL_xor_NONCE = 02000000000000000046020000f0507615
with MSBit cleared = 02000000000000000046020000f0507615
TAG = 78a50cb3f901ee38c588f6662d785a24
AAD =
CT = 9b1d2ba7d2d3a02efeec18d03be2b56
      1753b147ae642183f2c4bbd72e4ed8e1
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e
```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceae6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633
```

CTRBLKS (with MSbit set to 1)

```
00000000f901ee38c588f6662d785aa4
```


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 =	
MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
LENBLK =	00000000000000000800100000000000

Computing POLYVAL on a
 buffer of 3 blocks + LENBLK.

POLYVAL =	0e000000000000000650300203e788f7f
POLYVAL_xor_NONCE =	0d000000000000000650300203e788f7f
with MSBit cleared =	0d000000000000000650300203e788f7f
TAG =	a75aa62b704e826d984a72184e370598
AAD =	
CT =	dcc8d2f2c0e30b565f5d3ef58bf6638f
	f50e8909ced008e0515b79f7c8c3d1f5
	8ec1bb09177133b4cd1b375911d81579
Encryption_Key=	57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key)	57d4b7aec8de993e30a6861b61e6ce4e
	d85f98411081017f2027876441c1492a
	a2647dc2b2e57cbd92c2fbd9d303b2f3


```

dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```

000000000704e826d984a72184e370598
010000000704e826d984a72184e370598
020000000704e826d984a72184e370598

```

----- 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 =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
      03000000000000000000000000000000
      04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
                    04000000000000000000000000000000
LENBLK = 00000000000000000000000020000000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```
POLYVAL = 0f00000000000000008c04c04c63ad584f
```



```

POLYVAL_xor_NONCE = 0c0000000000000008c04c04c63ad584f
with MSBit cleared = 0c0000000000000008c04c04c63ad584f
TAG = d7f4efe2f6c72e3b8df168cab6b790ab
AAD =
CT = 472d6309563c74b6d5497145e929725a
      ab08979e6c4fc72c30c2e3a1ce568b94
      92e1b0351167937ee2faae79d40af93e
      24eee045fdab1b2040440632f1a34433
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

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

```

CTRBLKS (with MSbit set to 1)

```

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 = 0200000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
LENBLK = 08000000000000000400000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL = 13000000000000008091000000f0501631
POLYVAL_xor_NONCE = 10000000000000008091000000f0501631
with MSBit cleared = 10000000000000008091000000f0501631
TAG = 633c11b2eee1f65be0e3f1e0c824c5e0
AAD = 01
CT = 5adcda74026afb99
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceae6279d3cafcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (with MSbit set to 1)

```
00000000eee1f65be0e3f1e0c824c5e0
```

----- 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 =	130000000000000040d9000000f0501631
POLYVAL_xor_NONCE =	100000000000000040d9000000f0501631
with MSBit cleared =	100000000000000040d9000000f0501631
TAG =	f229e75b2c4c3048fc70f163c9ae0d
AAD =	01
CT =	b4fabbbadb27257bbe8b807d5
Encryption_Key=	57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key)	57d4b7aec8de993e30a6861b61e6ce4e
	d85f98411081017f2027876441c1492a
	a2647dc2b2e57cbd92c2fbd9d303b2f3
	dd5370a46fb60c19fd74f7c02e774533
	203db3954f8bbf8cb2ff484c9c880d7f
	f4ea614bbb61dec7099e968b95169bf4
	93fede61289f00a62101962db4170dd9
	2329ebec0bb6eb4a2ab77d679ea070be
	437845e748ceae6279d3cafc9a374
	6d72d75725bc79fa47c5aa30bb1c0944
	c773ccbde2cfb547a50a1f771e161633

CTRBLKS (with MSbit set to 1)

000000002c4c3048fc70f163c9ae0d

----- 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 = 130000000000000000023010000f0501631
POLYVAL_xor_NONCE = 100000000000000000023010000f0501631
with MSBit cleared = 100000000000000000023010000f0501631
TAG = cfb5aa16cdd9d39acc5d99b6eee2c6fc
AAD = 01
CT = dce7c7cd4d1060fdc663b9fe8de25385
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (with MSbit set to 1)

00000000cdd9d39acc5d99b6eee2c6fc

----- 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
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
LENBLK =	08000000000000000000000000000000

Computing POLYVAL on a
 buffer of 3 blocks + LENBLK.

POLYVAL =	1c0000000000000000460200203e78ef5b
POLYVAL_xor_NONCE =	1f0000000000000000460200203e78ef5b
with MSB cleared =	1f0000000000000000460200203e78ef5b
TAG =	8df5606f057468e4b38e89736255ad2d
AAD =	01
CT =	c6d3098e12ac653520764cbccdb90655
	b3d91bf034f7549d5f775fca5d6ad34f
Encryption_Key=	57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key)	57d4b7aec8de993e30a6861b61e6ce4e
	d85f98411081017f2027876441c1492a
	a2647dc2b2e57cbd92c2fbd9d303b2f3
	dd5370a46fb60c19fd74f7c02e774533
	203db3954f8bbf8cb2ff484c9c880d7f


```
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceae6279d3cafcd9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633
```

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
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 08000000000000000800100000000000
```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```
POLYVAL = 1d0000000000000006503c04c63ad386b
POLYVAL_xor_NONCE = 1e0000000000000006503c04c63ad386b
with MSBit cleared = 1e0000000000000006503c04c63ad386b
TAG = b52274e14d6111c74edf5d95855256a2
AAD = 01
```



```

CT = 186abbbe486294281b1514c11c240e6a
      4d959a1ac6da46e5b83bbe2d3d37de44
      ab009bb885b5c0bf83db80b651c06e74
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

```
*****
```

APPENDIX

```
*****
```

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

```
CTRBLKS (with MSbit set to 1)
```

```

000000004d6111c74edf5d95855256a2
010000004d6111c74edf5d95855256a2
020000004d6111c74edf5d95855256a2

```

```
----- 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
PADDED_AAD_and_MSG =          0100000000000000000000000000000000
                                02000000000000000000000000000000
                                03000000000000000000000000000000
                                04000000000000000000000000000000
                                05000000000000000000000000000000
LENBLK =                       0800000000000000000020000000000000

```

Computing POLYVAL on a
buffer of 5 blocks + LENBLK.

```

POLYVAL =                      1b0000000000000008c841a01712a376e
POLYVAL_xor_NONCE =           180000000000000008c841a01712a376e
with MSBit cleared =          180000000000000008c841a01712a376e
TAG =                          668fc00b6b40b4bb0c8d6cdb9730358d
AAD =                          01
CT =                           499ec09c83c2b79cf6b219e6b79ec81c
                                7c7b572c8a04b322094ec011e7003ded
                                388627f831ee79bd3df5db27f648125a
                                fbfe2774388c34bb652b866ca84bdcd8
Encryption_Key=                57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
                                d85f98411081017f2027876441c1492a
                                a2647dc2b2e57cbd92c2fbd9d303b2f3
                                dd5370a46fb60c19fd74f7c02e774533
                                203db3954f8bbf8cb2ff484c9c880d7f
                                f4ea614bbb61dec7099e968b95169bf4
                                93fede61289f00a62101962db4170dd9
                                2329ebec0bb6eb4a2ab77d679ea070be
                                437845e748ceaead6279d3cafc9a374
                                6d72d75725bc79fa47c5aa30bb1c0944
                                c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

```

                                0000000006b40b4bb0c8d6cdb9730358d
                                0100000006b40b4bb0c8d6cdb9730358d
                                0200000006b40b4bb0c8d6cdb9730358d
                                0300000006b40b4bb0c8d6cdb9730358d

```

----- 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 = 60000000000000000020000000000000

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.
POLYVAL = d800000000000000c048000000f050f665
POLYVAL_xor_NONCE = db00000000000000c048000000f050f665
with MSBit cleared = db00000000000000c048000000f050f665
TAG = 488346eaebe2d64ffa58e0fa82f8cd43
AAD = 01000000000000000000000000000000
CT = 7d5240be
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) 57d4b7aec8de993e30a6861b61e6ce4e
d85f98411081017f2027876441c1492a
a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceaead6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLKS (with MSbit set to 1)

00000000e0e2d64ffa58e0fa82f8cdc3

----- 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 =	900000000000000000a0000000000000

Computing POLYVAL on a
 buffer of 4 blocks + LENBLK.

POLYVAL =	0801000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE =	0b01000000000000c06b01c04c63ad9807
with MSBit cleared =	0b01000000000000c06b01c04c63ad9807
TAG =	d010794cfdbbc65ef641b8ccb9c2dda3
AAD =	01000000000000000000000000000000
	0200
CT =	6d98c309d4f472480c5b1389e83569e5
	217ddb9c
Encryption_Key=	57d4b7aec8de993e30a6861b61e6ce4e

APPENDIX

KEY_SCHEDULE (Encryption_Key)	57d4b7aec8de993e30a6861b61e6ce4e
	d85f98411081017f2027876441c1492a


```

a2647dc2b2e57cbd92c2fbd9d303b2f3
dd5370a46fb60c19fd74f7c02e774533
203db3954f8bbf8cb2ff484c9c880d7f
f4ea614bbb61dec7099e968b95169bf4
93fede61289f00a62101962db4170dd9
2329ebec0bb6eb4a2ab77d679ea070be
437845e748ceae6279d3cafc9a374
6d72d75725bc79fa47c5aa30bb1c0944
c773ccbde2cfb547a50a1f771e161633

```

CTRBLS (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 = a0000000000000000900000000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```

POLYVAL = 6401000000000000600701c04c63add8de
POLYVAL_xor_NONCE = 6701000000000000600701c04c63add8de

```



```

with MSBit cleared = 6701000000000000600701c04c63add85e
TAG = 98e16515942fb8ff9ef108e7ce53a963
AAD = 01000000000000000000000000000000
02000000
CT = 4649087685b01b476bd3420f36ca67d3
b18b
Encryption_Key= 57d4b7aec8de993e30a6861b61e6ce4e

```

APPENDIX

```

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

```

CTRBLS (with MSbit set to 1)

```

00000000942fb8ff9ef108e7ce53a9e3
01000000942fb8ff9ef108e7ce53a9e3

```

[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
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000

```



```

AAD =
MSG =
PADDED_AAD_and_MSG =
LENBLK = 00000000000000000000000000000000

```

Computing POLYVAL on a
buffer of 0 blocks + LENBLK.

```

POLYVAL = 00000000000000000000000000000000
POLYVAL_xor_NONCE = 03000000000000000000000000000000
with MSBit cleared = 03000000000000000000000000000000
TAG = de1a5fcd85a5217d91d8b349ab9cd224
AAD =
CT =
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deeeffb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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
	00000000000000000000000000000000
NONCE =	03000000000000000000000000000000
AAD =	
MSG =	010000000000000000
PADDED_AAD_and_MSG =	01000000000000000000000000000000
LENBLK =	00000000000000000040000000000000
Computing POLYVAL on a buffer of 1 blocks + LENBLK.	
POLYVAL =	04000000000000000809100000000283b1c
POLYVAL_xor_NONCE =	07000000000000000809100000000283b1c
with MSBit cleared =	07000000000000000809100000000283b1c
TAG =	90d1e4ad87f53fbf3eb26c066193fdf3
AAD =	
CT =	4b0619edd74c6a09
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae c19a3fba65980e6f4b5fe1545a05a30d 76ec3f188d75c24459bdc798ad3a3236 43b93a2f262134406d7ed514377b7619 eccd07cc61b8c58838050210953f3026 32bdcd05149cf94579e22c514e995a48 c323b99ea29b7c169a9e7e060fa14e20 08927a731c0e833665ecaf672b75f52f 32be5f8b9025239d0abb5d9b051a13bb baef9018a6e1132ec30dbc49e8784966 a90264b839274725339c1abe36860905 deefb1d780fe833bb02547a537a1d1c 44d8c0247dff87014e639dbf78e594ba 47cc0fa13fc3e79284c1b3e8d7bbaef4
-------------------------------	---

CTRBLKS (with MSbit set to 1)

0000000087f53fbf3eb26c066193fdf3

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

Computing POLYVAL on a
 buffer of 1 blocks + LENBLK.

POLYVAL =	040000000000000040d9000000000283b1c
POLYVAL_xor_NONCE =	070000000000000040d9000000000283b1c
with MSBit cleared =	070000000000000040d9000000000283b1c
TAG =	a42c36bcd7dd95273c5ded5a5ab0a8fc
AAD =	
CT =	ea410b6727fe50357dc2c9f9
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae
	c19a3fba65980e6f4b5fe1545a05a30d
	76ec3f188d75c24459bdc798ad3a3236
	43b93a2f262134406d7ed514377b7619
	eccd07cc61b8c58838050210953f3026
	32bdcd05149cf94579e22c514e995a48
	c323b99ea29b7c169a9e7e060fa14e20
	08927a731c0e833665ecaf672b75f52f
	32be5f8b9025239d0abb5d9b051a13bb
	baef9018a6e1132ec30dbc49e8784966


```
a90264b839274725339c1abe36860905
deeeffb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4
```

CTRBKLS (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
00000000000000000000000000000000
03000000000000000000000000000000

NONCE = 01000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 01000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 0000000000000000000800000000000000
```

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.

```
POLYVAL = 0400000000000000002301000000283b1c
POLYVAL_xor_NONCE = 0700000000000000002301000000283b1c
with MSBit cleared = 0700000000000000002301000000283b1c
TAG = a86f26245dea30d23ec045223ef5851e
AAD =
CT = d5d6c0782d45de97a027156334229387
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLKS (with MSbit set to 1)

```
0000000005dea30d23ec045223ef5859e
```

----- 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
          00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                     02000000000000000000000000000000
LENBLK = 00000000000000000000000010000000000000

```

Computing POLYVAL on a


```

buffer of 2 blocks + LENBLK.
POLYVAL = 01000000000000000046020000f0507615
POLYVAL_xor_NONCE = 02000000000000000046020000f0507615
with MSBit cleared = 02000000000000000046020000f0507615
TAG = ac78c482d3499b26ae97bf353c2c1bdb
AAD =
CT = cac82890d7f5a8330fa2f0f03701901a
      ed8a98666b42f74cc1887bd18964cf37
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deee fb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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

```

BYTES ORDER

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae c19a3fba65980e6f4b5fe1545a05a30d 76ec3f188d75c24459bdc798ad3a3236 43b93a2f262134406d7ed514377b7619 eccd07cc61b8c58838050210953f3026 32bdcd05149cf94579e22c514e995a48 c323b99ea29b7c169a9e7e060fa14e20 08927a731c0e833665ecaf672b75f52f 32be5f8b9025239d0abb5d9b051a13bb baef9018a6e1132ec30dbc49e8784966 a90264b839274725339c1abe36860905 deefb1d780fe833bb02547a537a1d1c 44d8c0247dff87014e639dbf78e594ba 47cc0fa13fc3e79284c1b3e8d7bbaef4
-------------------------------	---

CTRBLKS (with MSbit set to 1)

```
000000002c2dea133c87aea50fb1c1b3
010000002c2dea133c87aea50fb1c1b3
020000002c2dea133c87aea50fb1c1b3
```

----- 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
        00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
      03000000000000000000000000000000
      04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
                    04000000000000000000000000000000
LENBLK = 00000000000000000000000020000000000000
```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```
POLYVAL = 0f0000000000000008c04c04c63ad584f
POLYVAL_xor_NONCE = 0c0000000000000008c04c04c63ad584f
with MSBit cleared = 0c0000000000000008c04c04c63ad584f
TAG = 15e4bd316b19caa3a3493a81a3e4153c
AAD =
CT = d53e727defb0fe560c87f405ab19b1a2
      6fd85249324b974564c477b2eb4d4162
      943fa821946537d507e0713dcc556075
      220130acb5f3daa8dd46ee9af3b36642
```



```
Encryption_Key =          d77cdb05a40231d52ec7ef3b115a4259
                           c88735cffb99fd5cd4c805dcf487f5ae
```

```
*****
```

APPENDIX

```
*****
```

```
KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4
```

```
CTRBLKS (with MSbit set to 1)
```

```
0000000006b19caa3a3493a81a3e415bc
0100000006b19caa3a3493a81a3e415bc
0200000006b19caa3a3493a81a3e415bc
0300000006b19caa3a3493a81a3e415bc
```

```
----- 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
                   00000000000000000000000000000000
```



```

NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 0200000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
LENBLK = 08000000000000000400000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL = 13000000000000008091000000f0501631
POLYVAL_xor_NONCE = 10000000000000008091000000f0501631
with MSBit cleared = 10000000000000008091000000f0501631
TAG = 4cac1deb89734986b5f0546c661932e9
AAD = 01
CT = 8e5a22875d5d692e
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deefb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
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

```


d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeffb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

CTRBLKS (with MSbit set to 1)

000000006cd0b78ebdad8dc2c2c117a0

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

AAD_byte_len = 1
 AAD_bit_len = 8
 MSG_byte_len = 16
 MSG_bit_len = 128
 padded_AAD_byte_len = 16
 padded_MSG_byte_len = 16
 L1 blocks AAD(padded) = 1
 L2 blocks MSG(padded) = 1

BYTES ORDER

LSB-----MSB
 00010203040506070809101112131415

K1 = H =	03000000000000000000000000000000
K2 = K =	01000000000000000000000000000000
	00000000000000000000000000000000
NONCE =	03000000000000000000000000000000
AAD =	01
MSG =	02000000000000000000000000000000
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
LENBLK =	08000000000000000800000000000000

Computing POLYVAL on a
 buffer of 2 blocks + LENBLK.

POLYVAL =	1300000000000000023010000f0501631
POLYVAL_xor_NONCE =	1000000000000000023010000f0501631
with MSBit cleared =	1000000000000000023010000f0501631
TAG =	1e1fb157ee961567ee5a686a3ac66e74
AAD =	01
CT =	295cb156a7ccc66c9026829a26b08a92
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae
	c19a3fba65980e6f4b5fe1545a05a30d
	76ec3f188d75c24459bdc798ad3a3236


```

43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
LENBLK = 08000000000000000000000000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.
POLYVAL = 1c0000000000000000460200203e78ef5b
POLYVAL_xor_NONCE = 1f0000000000000000460200203e78ef5b

```



```

with MSBit cleared = 1f00000000000000460200203e78ef5b
TAG = c5558db375fc7fb253b477d990435e79
AAD = 01
CT = b1403a920a945105017054ccd7754e54
      7f471b9e42bd847f9ff2a6d5e1f72b92
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                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 = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
          00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
        03000000000000000000000000000000
        04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
                    04000000000000000000000000000000
LENBLK = 08000000000000000800100000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```

POLYVAL = 1d0000000000000006503c04c63ad386b
POLYVAL_xor_NONCE = 1e0000000000000006503c04c63ad386b
with MSBit cleared = 1e0000000000000006503c04c63ad386b
TAG = 54538b4b90c4877f29632ec9441d9809
AAD = 01
CT = 687c9c5846e8fde28bc1bde37dd15b80
      7ab731537d765e93f0d74bcac390ffbd
      b71ddb1af7505791ca74e87c697120b8
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLKS (with MSbit set to 1)


```

00000000090c4877f29632ec9441d9889
01000000090c4877f29632ec9441d9889
02000000090c4877f29632ec9441d9889

```

```

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

```

```

AAD_byte_len = 1
AAD_bit_len  = 8
MSG_byte_len = 64
MSG_bit_len  = 512
padded_AAD_byte_len = 16
padded_MSG_byte_len = 64
L1 blocks AAD(padded) = 1
L2 blocks MSG(padded) = 4

```

BYTES ORDER

```

LSB-----MSB
00010203040506070809101112131415
-----
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
        00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
      03000000000000000000000000000000
      04000000000000000000000000000000
      05000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
                    04000000000000000000000000000000
                    05000000000000000000000000000000
LENBLK = 08000000000000000000000000000000

```

Computing POLYVAL on a
buffer of 5 blocks + LENBLK.

```

POLYVAL = 1b0000000000000008c841a01712a376e
POLYVAL_xor_NONCE = 180000000000000008c841a01712a376e
with MSBit cleared = 180000000000000008c841a01712a376e
TAG = 49650717f842d3d193e3cc498e80f2c7
AAD = 01
CT = c17abb9e321814304f3844af4c90cb8e
      a89be09bd7a43a05021266c59a31609a
      3a2e7edf107c4c83d8370b36e52caca9
      de04c10dfd7eac3008852914cd9e900d
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259

```


c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
 c88735cffb99fd5cd4c805dcf487f5ae
 c19a3fba65980e6f4b5fe1545a05a30d
 76ec3f188d75c24459bdc798ad3a3236
 43b93a2f262134406d7ed514377b7619
 eccd07cc61b8c58838050210953f3026
 32bdcd05149cf94579e22c514e995a48
 c323b99ea29b7c169a9e7e060fa14e20
 08927a731c0e833665ecaf672b75f52f
 32be5f8b9025239d0abb5d9b051a13bb
 baef9018a6e1132ec30dbc49e8784966
 a90264b839274725339c1abe36860905
 deefb1d780fe833bb02547a537a1d1c
 44d8c0247dff87014e639dbf78e594ba
 47cc0fa13fc3e79284c1b3e8d7bbaef4

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
 00000000000000000000000000000000
 NONCE = 03000000000000000000000000000000


```

AAD =                01000000000000000000000000000000
MSG =                02000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
LENBLK =             60000000000000000020000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL =            d800000000000000c048000000f050f665
POLYVAL_xor_NONCE =  db00000000000000c048000000f050f665
with MSBit cleared = db00000000000000c048000000f050f665
TAG =                0ee2162b829d1b8087a61dec79c2b4dd
AAD =                01000000000000000000000000000000
CT =                 7f25e1eb
Encryption_Key =     d77cdb05a40231d52ec7ef3b115a4259
                    c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLKS (with MSbit set to 1)

```
00000000829d1b8087a61dec79c2b4dd
```

----- 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
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
0200
MSG = 03000000000000000000000000000000
04000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 9000000000000000a000000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 0801000000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b01000000000000c06b01c04c63ad9807
with MSBit cleared = 0b01000000000000c06b01c04c63ad9807
TAG = 07e3ed3f0c192bb05b8de76bba7901aa
AAD = 01000000000000000000000000000000
0200
CT = 4f39b03d1cf9f45d74e756ff1a382004
54b94c28
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb

```



```

baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBKLS (with MSbit set to 1)

```

000000000c192bb05b8de76bba7901aa
010000000c192bb05b8de76bba7901aa

```

----- 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
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = a0000000000000000900000000000000

```

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.

```

POLYVAL = 6401000000000000600701c04c63add8de
POLYVAL_xor_NONCE = 6701000000000000600701c04c63add8de
with MSBit cleared = 6701000000000000600701c04c63add85e
TAG = 33f0e38bd6fb197ed4f7eaaea861d60b
AAD = 01000000000000000000000000000000

```



```

CT      =      02000000
            625534f47020a12f11754fbc86ed46cf
            41d0
Encryption_Key =  d77cdb05a40231d52ec7ef3b115a4259
                   c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deeeffb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLKS (with MSbit set to 1)

```

00000000d6fb197ed4f7eaaea861d68b
01000000d6fb197ed4f7eaaea861d68b

```

----- 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

```



```

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

Computing POLYVAL on a
buffer of 0 blocks + LENBLK.
POLYVAL =                    00000000000000000000000000000000
POLYVAL_xor_NONCE =          03000000000000000000000000000000
with MSBit cleared =         03000000000000000000000000000000
TAG =                        de1a5fcd85a5217d91d8b349ab9cd224
AAD =
CT =
Encryption_Key =              d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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
        00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 0100000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
LENBLK = 00000000000000004000000000000000

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.
POLYVAL = 04000000000000000809100000000283b1c
POLYVAL_xor_NONCE = 07000000000000000809100000000283b1c
with MSBit cleared = 07000000000000000809100000000283b1c
TAG = 90d1e4ad87f53fbf3eb26c066193fdf3
AAD =
CT = 4b0619edd74c6a09
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRLKS (with MSbit set to 1)

0000000087f53fbf3eb26c066193fdf3

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

Computing POLYVAL on a
 buffer of 1 blocks + LENBLK.

POLYVAL =	040000000000000040d900000000283b1c
POLYVAL_xor_NONCE =	070000000000000040d900000000283b1c
with MSBit cleared =	070000000000000040d900000000283b1c
TAG =	a42c36bcd7dd95273c5ded5a5ab0a8fc
AAD =	
CT =	ea410b6727fe50357dc2c9f9
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae
	c19a3fba65980e6f4b5fe1545a05a30d
	76ec3f188d75c24459bdc798ad3a3236
	43b93a2f262134406d7ed514377b7619
	eccd07cc61b8c58838050210953f3026
	32bdcd05149cf94579e22c514e995a48

c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeefb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

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

```

[illegible]

Computing POLYVAL on a
buffer of 1 blocks + LENBLK.

POLYVAL =	04000000000000002301000000283b1c
POLYVAL_xor_NONCE =	07000000000000002301000000283b1c
with MSBit cleared =	07000000000000002301000000283b1c
TAG =	a86f26245dea30d23ec045223ef5851e
AAD =	
CT =	d5d6c0782d45de97a027156334229387
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae

APPENDIX

```
KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4
```

CTRBLKS (with MSbit set to 1)

```
0000000005dea30d23ec045223ef5859e
```

----- 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
        00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
      02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
```



```
L1 blocks AAD(padded) = 0
L2 blocks MSG(padded) = 3
```

BYTES ORDER

```

LSB-----MSB
00010203040506070809101112131415
-----
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
LENBLK = 000000000000000000080010000000000000

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.
POLYVAL = 0e000000000000000650300203e788f7f
POLYVAL_xor_NONCE = 0d000000000000000650300203e788f7f
with MSBit cleared = 0d000000000000000650300203e788f7f
TAG = d47a0a762c2dea133c87aea50fb1c1b3
AAD =
CT = bd562c8f8bbde467149c17a3f316fd2c
8859c748760332d3296a5b233c4059e3
e70a042dfc2b1812f484801a184b23ae
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae

```

* * * * *

APPENDIX

* * * * *

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae c19a3fba65980e6f4b5fe1545a05a30d 76ec3f188d75c24459bdc798ad3a3236 43b93a2f262134406d7ed514377b7619 eccd07cc61b8c58838050210953f3026 32bdcd05149cf94579e22c514e995a48 c323b99ea29b7c169a9e7e060fa14e20 08927a731c0e833665ecaf672b75f52f 32be5f8b9025239d0abb5d9b051a13bb baef9018a6e1132ec30dbc49e8784966 a90264b839274725339c1abe36860905 deeeffb1d780fe833bb02547a537a1d1c
-------------------------------	---


```
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4
```

CTRBLKS (with MSbit set to 1)

```
000000002c2dea133c87aea50fb1c1b3
010000002c2dea133c87aea50fb1c1b3
020000002c2dea133c87aea50fb1c1b3
```

----- 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
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD =
MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 000000000000000000000000200000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 0f0000000000000008c04c04c63ad584f
POLYVAL_xor_NONCE = 0c0000000000000008c04c04c63ad584f
with MSBit cleared = 0c0000000000000008c04c04c63ad584f
TAG = 15e4bd316b19caa3a3493a81a3e4153c
AAD =
CT = d53e727defb0fe560c87f405ab19b1a2
```



```

Encryption_Key = 6fd85249324b974564c477b2eb4d4162
                  943fa821946537d507e0713dcc556075
                  220130acb5f3daa8dd46ee9af3b36642
                  d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deeeffb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBKLS (with MSbit set to 1)

```

0000000006b19caa3a3493a81a3e415bc
0100000006b19caa3a3493a81a3e415bc
0200000006b19caa3a3493a81a3e415bc
0300000006b19caa3a3493a81a3e415bc

```

----- 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
          00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 0200000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
LENBLK = 08000000000000000400000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL = 13000000000000008091000000f0501631
POLYVAL_xor_NONCE = 10000000000000008091000000f0501631
with MSBit cleared = 10000000000000008091000000f0501631
TAG = 4cac1deb89734986b5f0546c661932e9
AAD = 01
CT = 8e5a22875d5d692e
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                               c88735cffb99fd5cd4c805dcf487f5ae
                               c19a3fba65980e6f4b5fe1545a05a30d
                               76ec3f188d75c24459bdc798ad3a3236
                               43b93a2f262134406d7ed514377b7619
                               eccd07cc61b8c58838050210953f3026
                               32bdcd05149cf94579e22c514e995a48
                               c323b99ea29b7c169a9e7e060fa14e20
                               08927a731c0e833665ecaf672b75f52f
                               32be5f8b9025239d0abb5d9b051a13bb
                               baef9018a6e1132ec30dbc49e8784966
                               a90264b839274725339c1abe36860905
                               deeeffb1d780fe833bb02547a537a1d1c
                               44d8c0247dff87014e639dbf78e594ba
                               47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLS (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

[illegible]

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```
POLYVAL = 130000000000000040d9000000f0501631
POLYVAL_xor_NONCE = 100000000000000040d9000000f0501631
with MSBit cleared = 100000000000000040d9000000f0501631
TAG = 42794bd56cd0b78ebdad8dc2c2c11720
AAD = 01
CT = ed921994f8d27aad941bfb6f
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
```

APPENDIX

* * * * *

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae c19a3fba65980e6f4b5fe1545a05a30d 76ec3f188d75c24459bdc798ad3a3236 43b93a2f262134406d7ed514377b7619 eccd07cc61b8c58838050210953f3026 32bdcd05149cf94579e22c514e995a48 c323b99ea29b7c169a9e7e060fa14e20 08927a731c0e833665ecaf672b75f52f 32be5f8b9025239d0abb5d9b051a13bb baef9018a6e1132ec30dbc49e8784966 a90264b839274725339c1abe36860905
-------------------------------	--


```

deeefb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBKLS (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
00010203040506070809101112131415
-----
K1 = H = 03000000000000000000000000000000
K2 = K = 01000000000000000000000000000000
          00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01
MSG = 02000000000000000000000000000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
LENBLK = 0800000000000000000800000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL = 130000000000000000023010000f0501631
POLYVAL_xor_NONCE = 100000000000000000023010000f0501631
with MSBit cleared = 100000000000000000023010000f0501631
TAG = 1e1fb157ee961567ee5a686a3ac66e74
AAD = 01
CT = 295cb156a7ccc66c9026829a26b08a92
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key)  d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLS (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
PADDED_AAD_and_MSG = 01000000000000000000000000000000
                    02000000000000000000000000000000
                    03000000000000000000000000000000
LENBLK = 08000000000000000000000000000000

```



```

Computing POLYVAL on a
buffer of 3 blocks + LENBLK.
POLYVAL = 1c0000000000000000460200203e78ef5b
POLYVAL_xor_NONCE = 1f0000000000000000460200203e78ef5b
with MSBit cleared = 1f0000000000000000460200203e78ef5b
TAG = c5558db375fc7fb253b477d990435e79
AAD = 01
CT = b1403a920a945105017054ccd7754e54
      7f471b9e42bd847f9ff2a6d5e1f72b92
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deefb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLS (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 =	03000000000000000000000000000000
K2 = K =	01000000000000000000000000000000
	00000000000000000000000000000000
NONCE =	03000000000000000000000000000000
AAD =	01
MSG =	02000000000000000000000000000000
	03000000000000000000000000000000
	04000000000000000000000000000000
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
	04000000000000000000000000000000
LENBLK =	08000000000000000800100000000000
Computing POLYVAL on a buffer of 4 blocks + LENBLK.	
POLYVAL =	1d000000000000006503c04c63ad386b
POLYVAL_xor_NONCE =	1e000000000000006503c04c63ad386b
with MSBit cleared =	1e000000000000006503c04c63ad386b
TAG =	54538b4b90c4877f29632ec9441d9809
AAD =	01
CT =	687c9c5846e8fde28bc1bde37dd15b80
	7ab731537d765e93f0d74bcac390ffbd
	b71ddb1af7505791ca74e87c697120b8
Encryption_Key =	d77cdb05a40231d52ec7ef3b115a4259
	c88735cffb99fd5cd4c805dcf487f5ae

* * * * *

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259c88735cffb99fd5cd4c805dcf487f5aec19a3fba65980e6f4b5fe1545a05a30d76ec3f188d75c24459bdc798ad3a323643b93a2f262134406d7ed514377b7619eccd07cc61b8c58838050210953f302632bdcd05149cf94579e22c514e995a48c323b99ea29b7c169a9e7e060fa14e2008927a731c0e833665ecaf672b75f52f32be5f8b9025239d0abb5d9b051a13bbbaef9018a6e1132ec30dbc49e8784966a90264b839274725339c1abe36860905deeefb1d780fe833bb02547a537a1d1c44d8c0247dff87014e639dbf78e594ba
-------------------------------	--

47cc0fa13fc3e79284c1b3e8d7bbaef4

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
	00000000000000000000000000000000
NONCE =	03000000000000000000000000000000
AAD =	01
MSG =	02000000000000000000000000000000
	03000000000000000000000000000000
	04000000000000000000000000000000
	05000000000000000000000000000000
PADDED_AAD_and_MSG =	01000000000000000000000000000000
	02000000000000000000000000000000
	03000000000000000000000000000000
	04000000000000000000000000000000
	05000000000000000000000000000000
LENBLK =	080000000000000000000000200000000000

Computing POLYVAL on a
 buffer of 5 blocks + LENBLK.

POLYVAL =	1b000000000000000008c841a01712a376e
POLYVAL_xor_NONCE =	18000000000000000008c841a01712a376e
with MSBit cleared =	18000000000000000008c841a01712a376e
TAG =	49650717f842d3d193e3cc498e80f2c7
AAD =	01
CT =	c17abb9e321814304f3844af4c90cb8e


```

Encryption_Key = a89be09bd7a43a05021266c59a31609a
                  3a2e7edf107c4c83d8370b36e52caca9
                  de04c10dfd7eac3008852914cd9e900d
                  d77cdb05a40231d52ec7ef3b115a4259
                  c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
                                c88735cffb99fd5cd4c805dcf487f5ae
                                c19a3fba65980e6f4b5fe1545a05a30d
                                76ec3f188d75c24459bdc798ad3a3236
                                43b93a2f262134406d7ed514377b7619
                                eccd07cc61b8c58838050210953f3026
                                32bdcd05149cf94579e22c514e995a48
                                c323b99ea29b7c169a9e7e060fa14e20
                                08927a731c0e833665ecaf672b75f52f
                                32be5f8b9025239d0abb5d9b051a13bb
                                baef9018a6e1132ec30dbc49e8784966
                                a90264b839274725339c1abe36860905
                                deeeffb1d780fe833bb02547a537a1d1c
                                44d8c0247dff87014e639dbf78e594ba
                                47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
MSG = 02000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
LENBLK = 60000000000000000020000000000000

```

Computing POLYVAL on a
buffer of 2 blocks + LENBLK.

```

POLYVAL = d800000000000000c048000000f050f665
POLYVAL_xor_NONCE = db00000000000000c048000000f050f665
with MSBit cleared = db00000000000000c048000000f050f665
TAG = 0ee2162b829d1b8087a61dec79c2b4dd
AAD = 01000000000000000000000000000000
CT = 7f25e1eb
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

```

KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeffb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

```

CTRBLKS (with MSbit set to 1)

```
00000000829d1b8087a61dec79c2b4dd
```

----- 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
00000000000000000000000000000000
NONCE = 03000000000000000000000000000000
AAD = 01000000000000000000000000000000
0200
MSG = 03000000000000000000000000000000
04000000
PADDED_AAD_and_MSG = 01000000000000000000000000000000
02000000000000000000000000000000
03000000000000000000000000000000
04000000000000000000000000000000
LENBLK = 900000000000000000a0000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 08010000000000c06b01c04c63ad9807
POLYVAL_xor_NONCE = 0b010000000000c06b01c04c63ad9807
with MSBit cleared = 0b010000000000c06b01c04c63ad9807
TAG = 07e3ed3f0c192bb05b8de76bba7901aa
AAD = 01000000000000000000000000000000
0200
CT = 4f39b03d1cf9f45d74e756ff1a382004
54b94c28
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae

```

APPENDIX

KEY_SCHEDULE (Encryption_Key)	d77cdb05a40231d52ec7ef3b115a4259 c88735cffb99fd5cd4c805dcf487f5ae c19a3fba65980e6f4b5fe1545a05a30d 76ec3f188d75c24459bdc798ad3a3236 43b93a2f262134406d7ed514377b7619 eccd07cc61b8c58838050210953f3026
-------------------------------	--


```

32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeffb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4

```

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
                    02000000000000000000000000000000
                    03000000000000000000000000000000
                    04000000000000000000000000000000
LENBLK = a000000000000000000900000000000000

Computing POLYVAL on a
buffer of 4 blocks + LENBLK.
POLYVAL = 6401000000000000600701c04c63add8de

```



```
POLYVAL_xor_NONCE = 6701000000000000600701c04c63add8de
with MSBit cleared = 6701000000000000600701c04c63add85e
TAG = 33f0e38bd6fb197ed4f7eaaea861d60b
AAD = 01000000000000000000000000000000
02000000
CT = 625534f47020a12f11754fbc86ed46cf
41d0
Encryption_Key = d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
```

APPENDIX

```
KEY_SCHEDULE (Encryption_Key) d77cdb05a40231d52ec7ef3b115a4259
c88735cffb99fd5cd4c805dcf487f5ae
c19a3fba65980e6f4b5fe1545a05a30d
76ec3f188d75c24459bdc798ad3a3236
43b93a2f262134406d7ed514377b7619
eccd07cc61b8c58838050210953f3026
32bdcd05149cf94579e22c514e995a48
c323b99ea29b7c169a9e7e060fa14e20
08927a731c0e833665ecaf672b75f52f
32be5f8b9025239d0abb5d9b051a13bb
baef9018a6e1132ec30dbc49e8784966
a90264b839274725339c1abe36860905
deeeffb1d780fe833bb02547a537a1d1c
44d8c0247dff87014e639dbf78e594ba
47cc0fa13fc3e79284c1b3e8d7bbaef4
```

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

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

Email: agl@google.com

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

Email: Yehuda.Lindell@biu.ac.il

