Network Working Group Request for Comments: 3394 Category: Informational J. Schaad Soaring Hawk Consulting R. Housley RSA Laboratories September 2002

Advanced Encryption Standard (AES) Key Wrap Algorithm

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

The purpose of this document is to make the Advanced Encryption Standard (AES) Key Wrap algorithm conveniently available to the Internet community. The United States of America has adopted AES as the new encryption standard. The AES Key Wrap algorithm will probably be adopted by the USA for encryption of AES keys. The authors took most of the text in this document from the draft AES Key Wrap posted by NIST.

Table of Contents

1. Introduction	2
2. Overview	2
2.1 Notation and Definitions	3
2.2 Algorithms	4
2.2.1 Key Wrap	4
2.2.2 Key Unwrap	5
2.2.3 Key Data Integrity the Initial Value	6
2.2.3.1 Default Initial Value	7
2.2.3.2 Alternative Initial Values	7
3. Object Identifiers	8
4. Test Vectors	8
4.1 Wrap 128 bits of Key Data with a 128-bit KEK	8
4.2 Wrap 128 bits of Key Data with a 192-bit KEK	11
4.3 Wrap 128 bits of Key Data with a 256-bit KEK	14
4.4 Wrap 192 bits of Key Data with a 192-bit KEK	
4.5 Wrap 192 bits of Key Data with a 256-bit KEK	
4.6 Wrap 256 bits of Key Data with a 256-bit KEK	
,	_

5.	Security Considerations	39
6.	References	39
	Acknowledgments	
8.	Authors' Äddresses	39
	Full Copyright Statement	

1. Introduction

NOTE: Most of the following text is taken from [AES-WRAP], and the assertions regarding the security of the AES Key Wrap algorithm are made by the US Government, not by the authors of this document.

This specification is intended to satisfy the National Institute of Standards and Technology (NIST) Key Wrap requirement to: Design a cryptographic algorithm called a Key Wrap that uses the Advanced Encryption Standard (AES) as a primitive to securely encrypt plaintext key(s) with any associated integrity information and data, such that the combination could be longer than the width of the AES block size (128-bits). Each ciphertext bit should be a highly non-linear function of each plaintext bit, and (when unwrapping) each plaintext bit should be a highly non-linear function of each ciphertext bit. It is sufficient to approximate an ideal pseudorandom permutation to the degree that explaints of pseudorandom permutation to the degree that exploitation of undesirable phenomena is as unlikely as quessing the AES engine key.

This key wrap algorithm needs to provide ample security to protect keys in the context of prudently designed key management architecture.

Throughout this document, any data being wrapped will be referred to as the key data. It makes no difference to the algorithm whether the as the key data. It makes no difference to the algorithm whether the data being wrapped is a key; in fact there is often good reason to include other data with the key, to wrap multiple keys together, or to wrap data that isn't strictly a key. So, the term "key data" is used broadly to mean any data being wrapped, but particularly keys, since this is primarily a key wrap algorithm. The key used to do the wrapping will be referred to as the key-encryption key (KEK).

In this document a KEK can be any valid key supported by the AES codebook. That is, a KEK can be a 128-bit key, a 192-bit key, or a 256-bit key.

2. Overview

The AES key wrap algorithm is designed to wrap or encrypt key data. The key wrap operates on blocks of 64 bits. Before being wrapped, the key data is parsed into n blocks of 64 bits.

Schaad & Housley Informational

The only restriction the key wrap algorithm places on n is that n be at least two. (For key data with length less than or equal to 64 bits, the constant field used in this specification and the key data form a single 128-bit codebook input making this key wrap unnecessary.) The key wrap algorithm accommodates all supported AES key sizes. However, other cryptographic values often need to be wrapped. One such value is the seed of the random number generator for DSS. This seed value requires n to be greater than four. Undoubtedly other values require this type of protection. Therefore, no upper bound is imposed on n.

The AES key wrap can be configured to use any of the three key sizes supported by the AES codebook. The choice of a key size affects the overall security provided by the key wrap, but it does not alter the description of the key wrap algorithm. Therefore, in the description that follows, the key wrap is described generically; no key size is specified for the KEK.

2.1 Notation and Definitions

The following notation is used in the description of the key wrapping algorithms:

```
Encrypt W using the AES codebook with key K Decrypt W using the AES codebook with key K Return the most significant j bits of W Return the least significant j bits of W The bitwise exclusive or (XOR) of B1 and B2 Conservants B1 and B2
AES(K, W)
AES-1(K, W)
MSB(j, W)
LSB(j, W)
B1 ^ B2
B1 | B2
                    Concatenate B1 and B2
K
                    The key-encryption key K
                    The number of 64-bit key data blocks
n
                    The number of steps in the wrapping process, s = 6n
P[i]
                    The ith plaintext key data block
                    The ith ciphertext data block
C[i]
                   The 64-bit integrity check register
R[i]
                    An array of 64-bit registers where
                        i = 0, 1, 2, ..., n
A[t], R[i][t] The contents of registers A and R[i] after encryption
                        step t.
IV
                    The 64-bit initial value used during the wrapping
                        process.
```

In the key wrap algorithm, the concatenation function will be used to concatenate 64-bit quantities to form the 128-bit input to the AES codebook. The extraction functions will be used to split the 128-bit output from the AES codebook into two 64-bit quantities.

2.2 Algorithms

The specification of the key wrap algorithm requires the use of the AES codebook [AES]. The next three sections will describe the key wrap algorithm, the key unwrap algorithm, and the inherent data integrity check.

2.2.1 Key Wrap

The inputs to the key wrapping process are the KEK and the plaintext to be wrapped. The plaintext consists of n 64-bit blocks, containing the key data being wrapped. The key wrapping process is described below.

Inputs: Plaintext, n 64-bit values {P1, P2, ..., Pn}, and Key, K (the KEK).
Outputs: Ciphertext, (n+1) 64-bit values {C0, C1, ..., Cn}.

1) Initialize variables.

```
Set A0 to an initial value (see 2.2.3)
For i = 1 to n
    R[0][i] = P[i]
```

2) Calculate intermediate values.

```
For t = 1 to s, where s = 6n
    A[t] = MSB(64, AES(K, A[t-1] | R[t-1][1])) ^ t
    For i = 1 to n-1
        R[t][i] = R[t-1][i+1]
    R[t][n] = LSB(64, AES(K, A[t-1] | R[t-1][1]))
```

3) Output the results.

```
Set C[0] = A[t]
For i = 1 to n
    C[i] = R[t][i]
```

An alternative description of the key wrap algorithm involves indexing rather than shifting. This approach allows one to calculate the wrapped key in place, avoiding the rotation in the previous description. This produces identical results and is more easily implemented in software.

1) Initialize variables.

```
Set A = IV, an initial value (see 2.2.3)
For i = 1 to n
    R[i] = P[i]
```

2) Calculate intermediate values.

3) Output the results.

2.2.2 Key Unwrap

The inputs to the unwrap process are the KEK and (n+1) 64-bit blocks of ciphertext consisting of previously wrapped key. It returns n blocks of plaintext consisting of the n 64-bit blocks of the decrypted key data.

1) Initialize variables.

```
Set A[s] = C[0] where s = 6n
For i = 1 to n
   R[s][i] = C[i]
```

2) Calculate the intermediate values.

```
For t = s to 1
   A[t-1] = MSB(64, AES-1(K, ((A[t] ^ t) | R[t][n]))
   R[t-1][1] = LSB(64, AES-1(K, ((A[t]^t) | R[t][n]))
   For i = 2 to n
        R[t-1][i] = R[t][i-1]
```

Schaad & Housley

Informational

[Page 5]

3) Output the results.

```
If A[0] is an appropriate initial value (see 2.2.3),
Then
        For i = 1 to n
            P[i] = R[0][i]
Else
        Return an error
```

The unwrap algorithm can also be specified as an index based operation, allowing the calculations to be carried out in place. Again, this produces the same results as the register shifting approach.

1) Initialize variables.

2) Compute intermediate values.

```
For j = 5 to 0
    For i = n to 1
    B = AES-1(K, (A ^ t) | R[i]) where t = n*j+i
    A = MSB(64, B)
    R[i] = LSB(64, B)
```

3) Output results.

If A is an appropriate initial value (see 2.2.3),
Then
 For i = 1 to n

Else

Return an error

2.2.3 Key Data Integrity -- the Initial Value

The initial value (IV) refers to the value assigned to A[0] in the first step of the wrapping process. This value is used to obtain an integrity check on the key data. In the final step of the unwrapping process, the recovered value of A[0] is compared to the expected

Schaad & Housley

Informational

value of A[0]. If there is a match, the key is accepted as valid, and the unwrapping algorithm returns it. If there is not a match, then the key is rejected, and the unwrapping algorithm returns an error.

The exact properties achieved by this integrity check depend on the definition of the initial value. Different applications may call for somewhat different properties; for example, whether there is need to determine the integrity of key data throughout its lifecycle or just when it is unwrapped. This specification defines a default initial value that supports integrity of the key data during the period it is wrapped (2.2.3.1). Provision is also made to support alternative initial values (in 2.2.3.2).

2.2.3.1 Default Initial Value

The default initial value (IV) is defined to be the hexadecimal constant:

A[0] = IV = A6A6A6A6A6A6A6A6

The use of a constant as the IV supports a strong integrity check on the key data during the period that it is wrapped. If unwrapping produces A[0] = A6A6A6A6A6A6A6A6A6, then the chance that the key data is corrupt is 2^-64 . If unwrapping produces A[0] any other value, then the unwrap must return an error and not return any key data.

2.2.3.2 Alternative Initial Values

When the key wrap is used as part of a larger key management protocol or system, the desired scope for data integrity may be more than just the key data or the desired duration for more than just the period that it is wrapped. Also, if the key data is not just an AES key, it may not always be a multiple of 64 bits. Alternative definitions of the initial value can be used to address such problems. NIST will define alternative initial values in future key management publications as needed. In order to accommodate a set of alternatives that may evolve over time, key wrap implementations that are not application-specific will require some flexibility in the way that the initial value is set and tested.

3. Object Identifiers

NIST has assigned the following object identifiers to identify the key wrap algorithm with the default initial value specified in 2.2.3.1. One object identifier is assigned for use with each of the KEK AES key sizes.

```
aes OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
    us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 1 }
id-aes128-wrap OBJECT IDENTIFIER ::= { aes 5 }
id-aes192-wrap OBJECT IDENTIFIER ::= { aes 25 }
id-aes256-wrap OBJECT IDENTIFIER ::= { aes 45 }
```

4. Test Vectors

The examples in this section were generated using the index-based implementation of the key wrap algorithm. The use of this approach allows a straightforward software implementation of the key wrap algorithm.

4.1 Wrap 128 bits of Key Data with a 128-bit KEK

Input:

KEK: 000102030405060708090A0B0C0D0E0F Key Data: 00112233445566778899AABBCCDDEEFF

Wrap:

```
Step t A R1 R2
```

```
In A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
Enc F4740052E82A2251 74CE86FBD7B805E7 8899AABBCCDDEEFF
XorT F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF
```

```
2
In F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF
Enc 06BA4EBDE7768D0B 74CE86FBD7B805E7 D132EE38147E76F8
XorT 06BA4EBDE7768D09 74CE86FBD7B805E7 D132EE38147E76F8
```

```
3
In 06BA4EBDE7768D09 74CE86FBD7B805E7 D132EE38147E76F8
Enc FC967627BE937208 FE6E8D679C5D3460 D132EE38147E76F8
XorT FC967627BE93720B FE6E8D679C5D3460 D132EE38147E76F8
```

```
4
     FC967627BE93720B FE6E8D679C5D3460 D132EE38147E76F8
In
      5896EA9028EE203B FE6E8D679C5D3460 07B2BD973E36A6FC
Enc
XorT 5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC
In 5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC Enc 93AEA71B258D90C3 25F5A3ADC2195401 07B2BD973E36A6FC XorT 93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC
6
     93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC
In
     E3EE986344D878F7 25F5A3ADC2195401 F14863BB1E9CA90A
Enc
XorT E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
In
     E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
      2BFC21B2C20E4006 B556D35ED8CEF052 F14863BB1E9CA90A
XorT 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
8
     2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
In
     4BE8CE99C0A43A7D B556D35ED8CEF052 64BAE5818D0570BB
XorT 4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB
9
      4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB
In
     EBE1CE91067024F3 BE114B343EB00981 64BAE5818D0570BB
Enc
XorT EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB
10
      EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB
In
     5A9C7B1F5B1C3B46 BE114B343EB00981 4FD3D2B7D74FBB42
Enc
XorT 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42
11
      5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42
In
Enc 93B71967EED41FFC AEF34BD8FB5A7B82 4FD3D2B7D74FBB42 XorT 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
12
     93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
In
      1FA68B0A8112B44B AEF34BD8FB5A7B82 9D3E862371D2CFE5
XorT 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5
Output:
```

Ciphertext: 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5

Unwrap:

Step	t	A	R1	R2
12 In XorT Dec	1FA68B0/	A8112B447 A8112B44B 7EED41FF7	AEF34BD8FB5A7B82 AEF34BD8FB5A7B82 AEF34BD8FB5A7B82	9D3E862371D2CFE5 9D3E862371D2CFE5 4FD3D2B7D74FBB42
11 In XorT Dec	93B71967	7EED41FF7 7EED41FFC F5B1C3B4C	AEF34BD8FB5A7B82 AEF34BD8FB5A7B82 BE114B343EB00981	4FD3D2B7D74FBB42 4FD3D2B7D74FBB42 4FD3D2B7D74FBB42
10 In XorT Dec	5A9C7B1F	F5B1C3B4C F5B1C3B46 1067024FA	BE114B343EB00981 BE114B343EB00981 BE114B343EB00981	4FD3D2B7D74FBB42 4FD3D2B7D74FBB42 64BAE5818D0570BB
9 In XorT Dec	EBE1CE91	1067024FA 1067024F3 9C0A43A75	BE114B343EB00981 BE114B343EB00981 B556D35ED8CEF052	64BAE5818D0570BB 64BAE5818D0570BB 64BAE5818D0570BB
8 In XorT Dec	4BE8CE99	9C0A43A75 9C0A43A7D 2C20E4001	B556D35ED8CEF052 B556D35ED8CEF052 B556D35ED8CEF052	64BAE5818D0570BB 64BAE5818D0570BB F14863BB1E9CA90A
7 In XorT Dec	2BFC21B2	2C20E4001 2C20E4006 344D878F1	B556D35ED8CEF052 B556D35ED8CEF052 25F5A3ADC2195401	F14863BB1E9CA90A F14863BB1E9CA90A F14863BB1E9CA90A
6 In XorT Dec	E3EE9863	344D878F1 344D878F7 3258D90C6	25F5A3ADC2195401 25F5A3ADC2195401 25F5A3ADC2195401	F14863BB1E9CA90A F14863BB1E9CA90A 07B2BD973E36A6FC
5 In XorT Dec	93AEA71E	3258D90C3	25F5A3ADC2195401 25F5A3ADC2195401 FE6E8D679C5D3460	07B2BD973E36A6FC 07B2BD973E36A6FC 07B2BD973E36A6FC
4 In XorT Dec	5896EA90		FE6E8D679C5D3460 FE6E8D679C5D3460 FE6E8D679C5D3460	07B2BD973E36A6FC 07B2BD973E36A6FC D132EE38147E76F8

```
In
         FC967627BE93720B FE6E8D679C5D3460 D132EE38147E76F8
   XorT FC967627BE937208 FE6E8D679C5D3460 D132EE38147E76F8
         06BA4EBDE7768D09 74CE86FBD7B805E7 D132EE38147E76F8
   In 06BA4EBDE7768D09 74CE86FBD7B805E7 D132EE38147E76F8
XorT 06BA4EBDE7768D0B 74CE86FBD7B805E7 D132EE38147E76F8
   Dec F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF
   1
         F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF
   In
   XorT F4740052E82A2251 74CE86FBD7B805E7 8899AABBCCDDEEFF
   Dec A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Plaintext A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Output:
   Key Data: 00112233445566778899AABBCCDDEEFF
4.2 Wrap 128 bits of Key Data with a 192-bit KEK
   Input:
                 000102030405060708090A0B0C0D0E0F1011121314151617
   KEK:
   Key Data: 00112233445566778899AABBCCDDEEFF
   Wrap:
   Step t
                  Α
                                    R1
                                                        R21
         A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
         DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
   XorT DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
   2
   In DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
Enc 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
XorT 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
   3
         9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
   In
         7B8E343CA51CF8AB BC164F51E20CC983 51F22F3286758A2D
   Enc
   XorT 7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D
   4
   In
         7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D
         02A97C5897140595 BC164F51E20CC983 05FC2D8F8FF4B919
   Enc
   XorT 02A97C5897140591 BC164F51E20CC983 05FC2D8F8FF4B919
```

```
In
      02A97C5897140591 BC164F51E20CC983 05FC2D8F8FF4B919
      15D4B63F66583817 429487269D3A0016 05FC2D8F8FF4B919
Enc
XorT 15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919
6
In 15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919 Enc AE2D0B76A6951EEA 429487269D3A0016 05A2D8FB4DD5BD7A XorT AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A
7
      AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A
In
      79F849444F4B8AA8 D40B091CDBAC0340 05A2D8FB4DD5BD7A
Enc
XorT 79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A
      79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A
In
      5933A9195B5F5E21 D40B091CDBAC0340 89F0D6C06F8CA9B4
XorT 5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4
9
      5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4
In
      57ADA800299C2E85 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
XorT 57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
10
      57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4 BF17BD6A9BC80163 4D5B3DFE7C04ABBA EB24CCFA52EA9078
In
Enc
XorT BF17BD6A9BC80169 4D5B3DFE7C04ABBA EB24CCFA52EA9078
11
      BF17BD6A9BC80169 4D5B3DFE7C04ABBA EB24CCFA52EA9078
In
     B68BF270AE81544F F92B5B97C050AED2 EB24CCFA52EA9078
Enc
XorT B68BF270AE815444 F92B5B97C050AED2 EB24CCFA52EA9078
12
      B68BF270AE815444 F92B5B97C050AED2 EB24CCFA52EA9078
In
      96778B25AE6CA439 F92B5B97C050AED2 468AB8A17AD84E5D
XorT 96778B25AE6CA435 F92B5B97C050AED2 468AB8A17AD84E5D
```

Output:

Ciphertext: 96778B25AE6CA435 F92B5B97C050AED2 468AB8A17AD84E5D

Unwrap:

Step	t	A	R1	R2
12 In XorT Dec	96778B2	5AE6CA435 5AE6CA439 0AE815444	F92B5B97C050AED2 F92B5B97C050AED2 F92B5B97C050AED2	468AB8A17AD84E5D 468AB8A17AD84E5D EB24CCFA52EA9078
11 In XorT Dec	B68BF27	0AE815444 0AE81544F A9BC80169	F92B5B97C050AED2 F92B5B97C050AED2 4D5B3DFE7C04ABBA	EB24CCFA52EA9078 EB24CCFA52EA9078 EB24CCFA52EA9078
10 In XorT Dec	BF17BD6	A9BC80169 A9BC80163 0299C2E8C	4D5B3DFE7C04ABBA 4D5B3DFE7C04ABBA 4D5B3DFE7C04ABBA	EB24CCFA52EA9078 EB24CCFA52EA9078 89F0D6C06F8CA9B4
9 In XorT Dec	57ADA80	0299C2E8C 0299C2E85 95B5F5E29	4D5B3DFE7C04ABBA 4D5B3DFE7C04ABBA D40B091CDBAC0340	89F0D6C06F8CA9B4 89F0D6C06F8CA9B4 89F0D6C06F8CA9B4
8 In XorT Dec	5933A91	95B5F5E29 95B5F5E21 44F4B8AAF	D40B091CDBAC0340 D40B091CDBAC0340 D40B091CDBAC0340	89F0D6C06F8CA9B4 89F0D6C06F8CA9B4 05A2D8FB4DD5BD7A
7 In XorT Dec	79F8494	44F4B8AAF 44F4B8AA8 6A6951EEC	D40B091CDBAC0340 D40B091CDBAC0340 429487269D3A0016	05A2D8FB4DD5BD7A 05A2D8FB4DD5BD7A 05A2D8FB4DD5BD7A
6 In XorT Dec	AE2D0B7	6A6951EEC 6A6951EEA F66583812	429487269D3A0016 429487269D3A0016 429487269D3A0016	05A2D8FB4DD5BD7A 05A2D8FB4DD5BD7A 05FC2D8F8FF4B919
5 In XorT Dec	15D4B63	F66583812 F66583817 897140591	429487269D3A0016 429487269D3A0016 BC164F51E20CC983	05FC2D8F8FF4B919 05FC2D8F8FF4B919 05FC2D8F8FF4B919
4 In XorT Dec	02A97C5	897140591 897140595 CA51CF8A8	BC164F51E20CC983 BC164F51E20CC983 BC164F51E20CC983	

```
3
         7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D
   In
   XorT 7B8E343CA51CF8AB BC164F51E20CC983 51F22F3286758A2D
         9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
   In 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D XorT 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
         DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
   1
   In DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF XorT DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF Dec A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Plaintext A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Output:
   Key Data: 00112233445566778899AABBCCDDEEFF
4.3 Wrap 128 bits of Key Data with a 256-bit KEK
   KEK: 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
   Key Data: 00112233445566778899AABBCCDDEEFF
   Wrap:
   Step t
                                      R1
                                                          R2
         A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   In
         794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
   Enc
   XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   2
         794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   In
         D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
```

3

In

XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8

XorT 85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8

D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8 85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8

```
4
      85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8 738C291128B7226D 5602001BFA07AD8B 58924F777C3F678C
In
Enc
XorT 738C291128B72269 5602001BFA07AD8B 58924F777C3F678C
In 738C291128B72269 5602001BFA07AD8B 58924F777C3F678C Enc 2656A02DFFF054DC F4DF378183E3D5B2 58924F777C3F678C XorT 2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
6
      2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
In
      DDFD0C0E8B52A63A F4DF378183E3D5B2 91AC1D36A964F41B
Enc
XorT DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
In
      DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
      39AB00D4AE4399EA 5271D5CED80F34ED 91AC1D36A964F41B
XorT 39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B
8
      39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B 4CE414878463EAAC 5271D5CED80F34ED 67D8ED899E7929B8
In
XorT 4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8
9
      4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8
In
      FBB44DB106AA0789 0DF7E50829123648 67D8ED899E7929B8
XorT FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8
10
      FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8
In
Enc 877112A7308ADCC5 0DF7E50829123648 3472D5993D318FD2
XorT 877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2
11
      877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2
In
      78E40190807CC151 63E9777905818A2A 3472D5993D318FD2
XorT 78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2
12
      78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2
In
      64E8C3F9CE0F5BAE 63E9777905818A2A 93C8191E7D6E8AE7
XorT 64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
```

Output:

Ciphertext: 64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7

Unwrap:

Step 12	t	A	R1	R2
In XorT Dec	64E8C3F9	9CE0F5BA2 9CE0F5BAE 0807CC15A	63E9777905818A2A 63E9777905818A2A 63E9777905818A2A	93C8191E7D6E8AE7 93C8191E7D6E8AE7 3472D5993D318FD2
11 In XorT Dec	78E4019	0807CC15A 0807CC151 7308ADCCF	63E9777905818A2A 63E9777905818A2A 0DF7E50829123648	3472D5993D318FD2 3472D5993D318FD2 3472D5993D318FD2
10 In XorT Dec	877112A	7308ADCCF 7308ADCC5 106AA0780	0DF7E50829123648 0DF7E50829123648 0DF7E50829123648	3472D5993D318FD2 3472D5993D318FD2 67D8ED899E7929B8
9 In XorT Dec	FBB44DB	106AA0780 106AA0789 78463EAA4	0DF7E50829123648 0DF7E50829123648 5271D5CED80F34ED	67D8ED899E7929B8 67D8ED899E7929B8 67D8ED899E7929B8
8 In XorT Dec	4CE4148	78463EAA4 78463EAAC 4AE4399ED	5271D5CED80F34ED 5271D5CED80F34ED 5271D5CED80F34ED	67D8ED899E7929B8 67D8ED899E7929B8 91AC1D36A964F41B
7 In XorT Dec	39AB00D4	4AE4399ED 4AE4399EA E8B52A63C	5271D5CED80F34ED 5271D5CED80F34ED F4DF378183E3D5B2	91AC1D36A964F41B 91AC1D36A964F41B 91AC1D36A964F41B
6 In XorT Dec	DDFD0C0I	E8B52A63C E8B52A63A DFFF054D9	F4DF378183E3D5B2 F4DF378183E3D5B2 F4DF378183E3D5B2	91AC1D36A964F41B 91AC1D36A964F41B 58924F777C3F678C
5 In XorT Dec	2656A02I	DFFF054D9 DFFF054DC 128B72269	F4DF378183E3D5B2 F4DF378183E3D5B2 5602001BFA07AD8B	58924F777C3F678C 58924F777C3F678C 58924F777C3F678C
4 In XorT Dec	738C2913	128B72269 128B7226D 879D5C0A6		58924F777C3F678C 58924F777C3F678C F60E0CDB7F429FE8

```
In 85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8 XorT 85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8
        D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
   Dec
   In
        D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
   XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
        794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   1
        794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   In
   XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
       A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Plaintext A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Output:
   Key Data: 00112233445566778899AABBCCDDEEFF
4.4 Wrap 192 bits of Key Data with a 192-bit KEK
   Input:
              000102030405060708090A0B0C0D0E0F1011121314151617
   KEK:
   Key Data: 00112233445566778899AABBCCDDEEFF0001020304050607
   Wrap:
   Step t A/R3
                                R1
                                                  R2
        A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   In
        0001020304050607
        DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
   Enc
        0001020304050607
   XorT DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
   Tn
        DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
        9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
   XorT 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
```

```
In
     9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
     0001020304050607
     2C8E19A519025B7C 351D385096CCFB29 51F22F3286758A2D
     FF540E514DE120A3
XorT 2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
     FF540E514DE120A3
In
     2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
     FF540E514DE120A3
    E727C7BDF822602E A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
XorT E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
In
     E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
    15B61F7B25D51700 A08DAA041D17BBBA AE82BC1118A5DEA4
Enc
     FF540E514DE120A3
XorT 15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
     FF540E514DE120A3
6
Tn
     15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
     FF540E514DE120A3
     A187755AEA64719C A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787
XorT A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787
In
     A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787
     5A994895D81644B7 926ED65A9E853FD9 AE82BC1118A5DEA4
Enc
     D1E708FD13778787
XorT 5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
     D1E708FD13778787
In
     5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
     D1E708FD13778787
     864F408C8AB8CDCF 926ED65A9E853FD9 552A09E141D08AE3
Enc
     D1E708FD13778787
XorT 864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
     D1E708FD13778787
```

9 In	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3
Enc	D1E708FD13778787 53F4373F575EB7A4 ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
XorT		926ED65A9E853FD9	552A09E141D08AE3
10			
In	53F4373F575EB7AD ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
Enc	9EAA4CDA0B1BA5FF ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
XorT		98883EDC6B080FB5	552A09E141D08AE3
11			
In	9EAA4CDA0B1BA5F5 ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
Enc	B1B9902C68E0EB52 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
XorT		98883EDC6B080FB5	63F6D88A0663FEF9
12			
In	B1B9902C68E0EB59 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
Enc	FCE591D77709A6E0 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
XorT		98883EDC6B080FB5	63F6D88A0663FEF9
13			
In	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9
Enc	463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5	C46965F34EFB2261	63F6D88A0663FEF9
XorT		C46965F34EFB2261	63F6D88A0663FEF9
14			
In	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9
Enc	463437433A93EFE5 6AC861AB961DA578 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4
XorT	6AC861AB961DA576 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4

15 In		LAB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4
Enc	E80DB4	7433A93EFE5 49CC9A1EA61	C46965F34EFB2261	56E3CEE892BBEFC4
XorT	E80DB4	C8C67FCFD53 49CC9A1EA6E C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
16 In		49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4
Enc	ABEE35		68F24EC260743EDC	56E3CEE892BBEFC4
XorT	ABEE35	C8C67FCFD53 534AC465C3C C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
<u>1</u> 7				
In		534AC465C3C C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
Enc		08CEDE62BF7 08C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	E7CC8	08CEDE62BE6 C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
18				
In		08CEDE62BE6 08C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
Enc	031D33	3264E15D320 4915C6762D2	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	031D33	3264E15D332 4915C6762D2	68F24EC260743EDC	E1C6C7DDEE725A93
0utpi	ut:			
Ciphe	ertext	031D33264E 6BA814915C		0743EDC E1C6C7DDEE725A93
Unwrap:				
Step	t	A/R3	R1	R2
18	00400			-4.666-DD
In	6BA814	4915C6762D2	68F24EC260743EDC	
XorT		3264E15D320 4915C6762D2	68F24EC260743EDC	E1C6C7DDEE725A93
Dec	E7CC8		68F24EC260743EDC	E1C6C7DDEE725A93

17 In	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	84943C8C67FCFD53 E7CC8D8CEDE62BF7 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
Dec	ABEE3534AC465C3C 84943C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
16			
In	ABEE3534AC465C3C 84943C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
XorT	ABEE3534AC465C2C 84943C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
Dec	E80DB49CC9A1EA6E 84943C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
15			
In	E80DB49CC9A1EA6E 84943C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
XorT	E80DB49CC9A1EA61 84943C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
Dec	6AC861AB961DA576 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4
14			
In	6AC861AB961DA576 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4
XorT	6AC861AB961DA578 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4
Dec	428428D2BD88CF55 463437433A93EFE5	C46965F34EFB2261	63F6D88A0663FEF9
13			
In	428428D2BD88CF55 463437433A93EFE5	C46965F34EFB2261	63F6D88A0663FEF9
XorT	428428D2BD88CF58 463437433A93EFE5	C46965F34EFB2261	63F6D88A0663FEF9
Dec		98883EDC6B080FB5	63F6D88A0663FEF9
12			
In	FCE591D77709A6EC 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
XorT	FCE591D77709A6E0 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
Dec	B1B9902C68E0EB59 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9

11			
In	B1B9902C68E0EB59 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
XorT	B1B9902C68E0EB52 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
Dec	9EAA4CDA0B1BA5F5 ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
10			
In	9EAA4CDA0B1BA5F5 ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
XorT	9EAA4CDA0B1BA5FF ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
Dec	53F4373F575EB7AD ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
9			
Ĭn	53F4373F575EB7AD ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
XorT	53F4373F575EB7A4	926ED65A9E853FD9	552A09E141D08AE3
Dec	ED5E8456E61BD295 864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3
	D1E708FD13778787		
8			
In	864F408C8AB8CDC7 D1E708FD13778787	926ED65A9E853FD9	552A09E141D08AE3
XorT	864F408C8AB8CDCF	926ED65A9E853FD9	552A09E141D08AE3
Dec	D1E708FD13778787 5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4
	D1E708FD13778787		
7			
In	5A994895D81644B0 D1E708FD13778787	926ED65A9E853FD9	AE82BC1118A5DEA4
XorT	5A994895D81644B7 D1E708FD13778787	926ED65A9E853FD9	AE82BC1118A5DEA4
Dec	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4
	D1E708FD13778787		
6			
In	A187755AEA64719A D1E708FD13778787	A08DAA041D17BBBA	AE82BC1118A5DEA4
XorT	A187755AEA64719C	A08DAA041D17BBBA	AE82BC1118A5DEA4
Dec	D1E708FD13778787 15B61F7B25D51705 FF540E514DE120A3	A08DAA041D17BBBA	AE82BC1118A5DEA4

```
In
     15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
     FF540E514DE120A3
XorT 15B61F7B25D51700 A08DAA041D17BBBA AE82BC1118A5DEA4
     FF540E514DE120A3
Dec
    E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
In
     E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
XorT E727C7BDF822602E A08DAA041D17BBBA 51F22F3286758A2D
     FF540E514DE120A3
     2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
Dec
     FF540E514DE120A3
In
     2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
     FF540E514DE120A3
XorT 2C8E19A519025B7C 351D385096CCFB29 51F22F3286758A2D
     FF540E514DE120A3
     9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
Dec
     0001020304050607
2
Τn
     9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
     0001020304050607
XorT 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
     0001020304050607
     DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
Dec
     0001020304050607
     DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
In
     0001020304050607
XorT DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
     0001020304050607
     A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
Dec
     0001020304050607
Plaintext A6A6A6A6A6A6A6A6 0011223344556677
           8899AABBCCDDEEFF 0001020304050607
Output:
Key Data:
           00112233445566778899AABBCCDDEEFF0001020304050607
```

4.5 Wrap 192 bits of Key Data with a 256-bit KEK

Input: KEK:

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

Key Data: 00112233445566778899AABBCCDDEEFF0001020304050607

Wrap:

Step t A/R3 R1 R2

1 In A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF 0001020304050607

Enc 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF 0001020304050607

XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF 0001020304050607

In 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF 0001020304050607

Enc D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8 0001020304050607

XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8 0001020304050607

In D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8 0001020304050607

Enc 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154

XorT 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154

4 In 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154

Enc F1D28EA6295891EC 0CC86A4D9B9C6A31 F60E0CDB7F429FE8 6CA405593A3B5154

XorT F1D28EA6295891E8 0CC86A4D9B9C6A31 F60E0CDB7F429FE8 6CA405593A3B5154

5 In	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8
Enc	6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT	BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
6			
Ĭn	BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
Enc	6F85BFBDB7E880E3 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT	6F85BFBDB7E880E5 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
7			
In	6F85BFBDB7E880E5 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
Enc	D532789E4E79D819 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
XorT	D532789E4E79D81E 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
8			
In	D532789E4E79D81E 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
Enc	2A5FFCEF1F1916D8 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
XorT	2A5FFCEF1F1916D0 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
9			
In	2A5FFCEF1F1916D0 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
Enc	01271BA91D9804F6 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
XorT		444F92BF78E77BB1	C6874607903270CD
10			
In	01271BA91D9804FF 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
Enc	A3223BD7237F7033 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
XorT		FB1611A83BEB567F	C6874607903270CD

11			
Ī'n	A3223BD7237F7039 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
Enc	B50C330616E7B1C7 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
XorT		FB1611A83BEB567F	73EDC8CB9322C34E
12			
In	B50C330616E7B1CC 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
Enc	FB8AFF3F083E12CE 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
XorT		FB1611A83BEB567F	73EDC8CB9322C34E
13			
In	FB8AFF3F083E12C2 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
Enc	82F597607784A33C 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
XorT		FB1F2965FCE1E783	73EDC8CB9322C34E
14 In	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E
Enc	0B08CFDF48020F0D D48E5E83B7C906DB	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	0B08CFDF48020F0D D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
	0D00C1 D1 400201 0D		
15 Tn	D40EEE02D7C006DE	FB1F2965FCE1E783	D26E4EEDA2C02ED0
In	D48E5E83B7C906D5 0B08CFDF48020F0D	LDTL5A00LCETE102	D36F4FFBA2C82ED9
Enc	1BF2B1CD947311B6	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	C490C33642717146 1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9
	C490C33642717146		
16			
In	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Enc		F6E6F4FBE30E71E4	D36F4FFBA2C82ED9
XorT	C490C33642717146	F6E6F4FBE30E71E4	D36F4FFRA2C82FDQ
AUI I	C490C33642717146	I OLOI TI DESUL/ILT	DOUTH I DAZCOZEDO

In C9F5F26A378011CE F6E6F4FBE30E71E4 D3 C490C33642717146	36F4FFBA2C82ED9
Enc 39128CE5E435F3A0 F6E6F4FBE30E71E4 76 C490C33642717146	69C8B80A32CB895
XorT 39128CE5E4325F3B1 F6E6F4FBE30E71E4 7 C490C33642717146	769C8B80A32CB895
18 In 39128CE5E435F3B1 F6E6F4FBE30E71E4 70	69C8B80A32CB895
C490C33642717146 Enc A8F9BC1612C68B2D F6E6F4FBE30E71E4 76	69C8B80A32CB895
8CD5D17D6B254DA1 XorT A8F9BC1612C68B3F F6E6F4FBE30E71E4 70 8CD5D17D6B254DA1	69C8B80A32CB895
Ciphertext A8F9BC1612C68B3F F6E6F4FBE30 769C8B80A32CB895 8CD5D17D6B2	
Unwrap:	
Step t A/R3 R1	R2
18 In A8F9BC1612C68B3F F6E6F4FBE30E71E4 76 8CD5D17D6B254DA1	69C8B80A32CB895
XorT A8F9BC1612C68B2D F6E6F4FBE30E71E4 76 8CD5D17D6B254DA1	69C8B80A32CB895
Dec 39128CE5E435F3B1 F6E6F4FBE30E71E4 70 C490C33642717146	69C8B80A32CB895
17	
In 39128CE5E435F3B1 F6E6F4FBE30E71E4 76 C490C33642717146	69C8B80A32CB895
XorT 39128CE5E435F3A0 F6E6F4FBE30E71E4 70 C490C33642717146	69C8B80A32CB895
Dec C9F5F26A378011CE F6E6F4FBE30E71E4 D3 C490C33642717146	36F4FFBA2C82ED9
16 In C9F5F26A378011CE F6E6F4FBE30E71E4 D3	36F4FFBA2C82ED9
C490C33642717146 XorT C9F5F26A378011DE F6E6F4FBE30E71E4 D3	36F4FFBA2C82ED9
C490C33642717146 Dec 1BF2B1CD947311B9 FB1F2965FCE1E783 D3 C490C33642717146	36F4FFBA2C82ED9

15 In	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	C490C33642717146 1BF2B1CD947311B6 C490C33642717146	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Dec	D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
14			
In	D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	D48E5E83B7C906DB 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Dec	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
13			
In	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
XorT		FB1F2965FCE1E783	73EDC8CB9322C34E
Dec	FB8AFF3F083E12C2 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
12			
In	FB8AFF3F083E12C2 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
XorT	FB8AFF3F083E12CE 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
Dec	B50C330616E7B1CC 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
11			
In	B50C330616E7B1CC 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
XorT	B50C330616E7B1C7 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
Dec		FB1611A83BEB567F	C6874607903270CD
10			
In	A3223BD7237F7039 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
XorT	A3223BD7237F7033 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
Dec		444F92BF78E77BB1	C6874607903270CD

9 In	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD
XorT	740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
_	740A273461ED82C6		
Dec	2A5FFCEF1F1916D0 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
8			
In	2A5FFCEF1F1916D0 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
XorT	2A5FFCEF1F1916D8 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
Dec	D532789E4E79D81E 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
7			
In	D532789E4E79D81E 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
XorT	D532789E4E79D819 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
Dec	6F85BFBDB7E880E5 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
<u>6</u>			
In	6F85BFBDB7E880E5 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT	6F85BFBDB7E880E3 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
Dec	BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
5			
In	BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT	BF213BFD04E8A24F 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
Dec		0CC86A4D9B9C6A31	F60E0CDB7F429FE8
4			
In	F1D28EA6295891E8 6CA405593A3B5154	0CC86A4D9B9C6A31	F60E0CDB7F429FE8
XorT	F1D28EA6295891EC 6CA405593A3B5154	0CC86A4D9B9C6A31	F60E0CDB7F429FE8
Dec		F661BD9F31FBFA31	F60E0CDB7F429FE8

```
In
     9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154
XorT 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154
Dec
     D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607
In
     D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607
XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607
     794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
Dec
     0001020304050607
In
     794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
     0001020304050607
XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
     0001020304050607
Dec
     A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
     0001020304050607
Plaintext A6A6A6A6A6A6A6A6 0011223344556677
           8899AABBCCDDEEFF 0001020304050607
Output:
```

Key Data: 00112233445566778899AABBCCDDEEFF0001020304050607

4.6 Wrap 256 bits of Key Data with a 256-bit KEK

Input:

KEK:

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F **Key Data:**

OO112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

Wrap:

Step t A/R3 R1/R4 R2 A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF In 0001020304050607 08090A0B0C0D0E0F 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF Enc 0001020304050607 08090A0B0C0D0E0F XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF 0001020304050607 08090A0B0C0D0E0F 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF 0001020304050607 08090A0B0C0D0E0F D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8 Ιn Enc 0001020304050607 08090A0B0C0D0E0F XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8 0001020304050607 08090A0B0C0D0E0F In D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8 0001020304050607 08090A0B0C0D0E0F 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8 Enc 6CA405593A3B5154 08090A0B0C0D0E0F XorT 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154 08090A0B0C0D0E0F In 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154 08090A0B0C0D0E0F 564408FDD0DD2EA4 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154 E5923CB9FDB56FBC XorT 564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154 E5923CB9FDB56FBC In 564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8 6CA405593A3B5154 E5923CB9FDB56FBC 4EF02EDD3146AFBB E7D1194D853E53F8 F60E0CDB7F429FE8 6CA405593A3B5154 E5923CB9FDB56FBC XorT 4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8 6CA405593A3B5154 E5923CB9FDB56FBC

6 In	4EF02EDD3146AFBE 6CA405593A3B5154	E5923CB9FDB56FBC	F60E0CDB7F429FE8
Enc	963AAFFD96B223EC 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
XorT	963AAFFD96B223EA 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
7 In	963AAFFD96B223EA 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Enc	66D7A8ADD086B9DD	E7D1194D853E53F8	EFD48BA304945576
XorT	C365B66943E2D760 66D7A8ADD086B9DA C365B66943E2D760	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
8 In	66D7A8ADD086B9DA C365B66943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Enc	C58B9D3AC6D5B94E C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
XorT	C58B9D3AC6D5B946 C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
9 In	C58B9D3AC6D5B946 C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
Enc	1A681354E84C41F8 C365B66943E2D760	D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
XorT	1A681354E84C41F1 C365B66943E2D760	73E3B6CBE3D03D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
10 In	1A681354E84C41F1 C365B66943E2D760	D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
Enc	DBA417FB51F9E3CB C365B66943E2D760	D6AE29ECE7192D43 73E3B6CBE5D05D74	FBEC169FA5C0F6BA
XorT	DBA417FB51F9E3C1	D6AE29ECE7192D43 73E3B6CBE5D05D74	FBEC169FA5C0F6BA
11 In	DBA417FB51F9E3C1 C365B66943E2D760		FBEC169FA5C0F6BA
Enc	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA
XorT	0629EB29A42E4FD2	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	FBEC169FA5C0F6BA

12 In Enc XorT	0629EB29A42E4FD2 F56701DAF0388216 F9ED8A1429515665 F56701DAF0388216 F9ED8A1429515669 F56701DAF0388216	D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 3CF149E90E8C04D9 D6AE29ECE7192D43 3CF149E90E8C04D9	FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA
13 In Enc XorT	F9ED8A1429515669 F56701DAF0388216 2E8E2B6BB2016696 F56701DAF0388216 2E8E2B6BB201669B F56701DAF0388216	D6AE29ECE7192D43 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA
14 In Enc XorT	2E8E2B6BB201669B F56701DAF0388216 15342443CB95ADB1 F56701DAF0388216 15342443CB95ADBF F56701DAF0388216	4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA BCA418BBF7DCE60B BCA418BBF7DCE60B
15 In Enc XorT	15342443CB95ADBF F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9	4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
16 In Enc XorT		4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
17 In Enc XorT	5075496800978B5A C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 A5382A26B47551E0 C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B

```
18
     A5382A26B47551E0 1BB8C765A84195E7 BCA418BBF7DCE60B
In
     C272E9466AAE98F9 40F68C91DB49702C
     F19D80D437EFE8F9 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C
XorT F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C
19
In
     F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C
     B422B444B87A190B 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 40F68C91DB49702C
XorT B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
1CFBF6B4C24CB982 40F68C91DB49702C
20
In
     B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 40F68C91DB49702C
     D058823360F88A37 1BB8C765A84195E7 F7EDAD518C960D36
Enc
1CFBF6B4C24CB982 07DFE775B9687E73
XorT D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
21
     D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
Tn
     1CFBF6B4C24CB982 07DFE775B9687E73
     C89A96CA7B163ECC CBCCB35CFB87F826 F7EDAD518C960D36
1CFBF6B4C24CB982 07DFE775B9687E73
XorT C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
22
In
     C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
     39D02FE7435870ED CBCCB35CFB87F826 3F5786E2D80ED326
Enc
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT 39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73
23
In
     39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73
     0AEB82AE3146A91B CBCCB35CFB87F826 3F5786E2D80ED326
Enc
     CBC7F0E71A99F43B 07DFE775B9687E73
XorT 0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B 07DFE775B9687E73
```

24

```
In
     OAEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B 07DFE775B9687E73
     28C9F404C4B810EC CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B FB988B9B7A02DD21
XorT 28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B FB988B9B7A02DD21
Output:
Ciphertext 28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
            CBC7F0E71A99F43B FB988B9B7A02DD21
Unwrap:
Step t A/R3
                             R1/R4
                                              R2
24
     28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
In
     CBC7F0E71A99F43B FB988B9B7A02DD21
XorT 28C9F404C4B810EC CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B FB988B9B7A02DD21
0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
Dec
     CBC7F0E71A99F43B 07DFE775B9687E73
23
     OAEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
Tn
     CBC7F0E71A99F43B 07DFE775B9687E73
XorT 0AEB82AE3146A91B CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B 07DFE775B9687E73
     39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
Dec
     1CFBF6B4C24CB982 07DFE775B9687E73
22
     39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
Ιŋ
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT 39D02FE7435870ED CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73
     C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
Dec
     1CFBF6B4C24CB982 07DFE775B9687E73
21
In
     C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT C89A96CA7B163ECC CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
Dec
     D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
```

20 In XorT Dec	D058823360F88A23 1CFBF6B4C24CB982 D058823360F88A37 1CFBF6B4C24CB982 B422B444B87A1918 1CFBF6B4C24CB982	1BB8C765A84195E7 07DFE775B9687E73 1BB8C765A84195E7 07DFE775B9687E73 1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36 F7EDAD518C960D36 F7EDAD518C960D36
19 In XorT Dec	B422B444B87A1918 1CFBF6B4C24CB982 B422B444B87A190B 1CFBF6B4C24CB982 F19D80D437EFE8EB	1BB8C765A84195E7 40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 1BB8C765A84195E7	F7EDAD518C960D36 F7EDAD518C960D36 F7EDAD518C960D36
18 In XorT Dec	C272E9466AAE98F9 F19D80D437EFE8EB C272E9466AAE98F9 F19D80D437EFE8F9 C272E9466AAE98F9 A5382A26B47551E0	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 1BB8C765A84195E7	F7EDAD518C960D36 F7EDAD518C960D36 BCA418BBF7DCE60B
17 In XorT	C272E9466AAE98F9 A5382A26B47551E0 C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B
Dec 16 In XorT	5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B4A	4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
Dec 15 In XorT	C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9 33FE29365885C4B7	3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
Dec		3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B

14 In	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
XorT	F56701DAF0388216 15342443CB95ADB1 F56701DAF0388216	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B
Dec	2E8E2B6BB201669B F56701DAF0388216	4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA
13 In	2E8E2B6BB201669B F56701DAF0388216	4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA
XorT	2E8E2B6BB2016696 F56701DAF0388216	4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA
Dec	F9ED8A1429515669 F56701DAF0388216	D6AE29ECE7192D43 3CF149E90E8C04D9	FBEC169FA5C0F6BA
12 In	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
XorT	F56701DAF0388216 F9ED8A1429515665	3CF149E90E8C04D9 D6AE29ECE7192D43	FBEC169FA5C0F6BA
Dec	F56701DAF0388216 0629EB29A42E4FD2	3CF149E90E8C04D9 D6AE29ECE7192D43	FBEC169FA5C0F6BA
БСС	F56701DAF0388216	73E3B6CBE5D05D74	I BECTOSI ASCOI OBA
11 In	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74 D6AE29ECE7192D43	
XorT	0629EB29A42E4FD9		FBEC169FA5C0F6BA
Dec	F56701DAF0388216 DBA417FB51F9E3C1	73E3B6CBE5D05D74 D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
10 In	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
XorT	C365B66943E2D760 DBA417FB51F9E3CB	73E3B6CBE5D05D74 D6AE29ECE7192D43	FBEC169FA5C0F6BA
Dec	C365B66943E2D760 1A681354E84C41F1	73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576
		73E3B6CBE5D05D74	
9 In	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
XorT	1A681354E84C41F8 C365B66943E2D760	D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
Dec	C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576

8 In		3AC6D5B946 6943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
XorT	C58B9D3	3AC6D5B94E 6943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
Dec	66D7A8/	ADD086B9DA 6943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
7 In		ADD086B9DA 6943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
XorT	66D7A8/	ADD086B9DD 6943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Dec	963AAFI	FD96B223EA 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
6 In		FD96B223EA 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
XorT	963AAFI	FD96B223EC 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Dec	4EF02EI	DD3146AFBE 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
5 In		DD3146AFBE 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
XorT	4EF02EI	DD3146AFBB 593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
Dec	5644081	FDD0DD2EA0 593A3B5154	F661BD9F31FBFA31 E5923CB9FDB56FBC	F60E0CDB7F429FE8
4 In		FDD0DD2EA0 593A3B5154	F661BD9F31FBFA31 E5923CB9FDB56FBC	F60E0CDB7F429FE8
XorT	5644081	FDD0DD2EA4 593A3B5154	F661BD9F31FBFA31 E5923CB9FDB56FBC	F60E0CDB7F429FE8
Dec	9DF8F5	405FBC00C2	F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8
3 In		405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8
XorT	9DF8F54	593A3B5154 405FBC00C1 593A3B5154	08090A0B0C0D0E0F F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8
Dec	D450EA	5C5BBCB563 0304050607	F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8

2

In	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
	0001020304050607	08090A0B0C0D0E0F	
XorT		F661BD9F31FBFA31	F60E0CDB7F429FE8
	0001020304050607	08090A0B0C0D0E0F	
Dec	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
1			
Īn	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
XorT	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
Dec	A6A6A6A6A6A6A6A	0011223344556677	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	

Plaintext A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF 0001020304050607 08090A0B0C0D0E0F

Output: Key Data:

00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

5. Security Considerations

The key wrap algorithm includes a strong integrity check on the key data. If unwrapping produces the expected check value in A[0], then the chance that the key data is corrupt is 2^-64. If unwrapping produces an unexpected value, then the algorithm implementation MUST return an error, and it MUST NOT return any key data.

Implementations must protect the KEK from disclosure. Compromise of the KEK may result in the disclosure of all key data protected with that KEK.

6. References

AES National Institute of Standards and Technology. FIPS Pub 197: Advanced Encryption Standard (AES). 26 November 2001.

AES-WRAP National Institute of Standards and Technology. AES Key Wrap Specification. 17 November 2001.
[http://csrc.nist.gov/encryption/kms/key-wrap.pdf]

7. Acknowledgments

Most of the text in this document is taken from [AES-WRAP]. The authors of that document are responsible for the development of the AES key wrap algorithm.

8. Authors' Addresses

Jim Schaad Soaring Hawk Consulting

EMail: jimsch@exmsft.com

Russell Housley RSA Laboratories 918 Spring Knoll Drive Herndon, VA 20170 USA

EMail: rhousley@rsasecurity.com

9. Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others provided that the above copyright notice and this paragraph are included on all such copies. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.