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



## 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

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 exploitation of undesirable phenomena is as unlikely as guessing 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 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.

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:

| | |
|---|---|
| AES(K, W) | Encrypt W using the AES codebook with key K |
| AES-1(K, W) | Decrypt W using the AES codebook with key K |
| MSB(j, W) | Return the most significant j bits of W |
| LSB(j, W) | Return the least significant j bits of W |
| B1 ^ B2 | The bitwise exclusive or (XOR) of B1 and B2 |
| B1 \| B2 | Concatenate B1 and B2 |
| K | The key-encryption key K |
| n | The number of 64-bit key data blocks |
| s | The number of steps in the wrapping process, s = 6n |
| P[i] | The ith plaintext key data block |
| C[i] | The ith ciphertext data block |
| A | 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.

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

2) Calculate intermediate values.

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

3) Output the results.

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

### 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.

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

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]
```

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.

```
Inputs:  Ciphertext, (n+1) 64-bit values {C0, C1, ..., Cn}, and
         Key, K (the KEK).
Outputs: Plaintext, n 64-bit values {P0, P1, K, Pn}.
```

1) Initialize variables.

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

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
        P[i] = R[i]
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

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] = A6A6A6A6A6A6A6A6, 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

1
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
In   FC967627BE93720B FE6E8D679C5D3460 D132EE38147E76F8
Enc  5896EA9028EE203B FE6E8D679C5D3460 07B2BD973E36A6FC
XorT 5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC

5
In   5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC
Enc  93AEA71B258D90C3 25F5A3ADC2195401 07B2BD973E36A6FC
XorT 93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC

6
In   93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC
Enc  E3EE986344D878F7 25F5A3ADC2195401 F14863BB1E9CA90A
XorT E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A

7
In   E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
Enc  2BFC21B2C20E4006 B556D35ED8CEF052 F14863BB1E9CA90A
XorT 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A

8
In   2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
Enc  4BE8CE99C0A43A7D B556D35ED8CEF052 64BAE5818D0570BB
XorT 4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB

9
In   4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB
Enc  EBE1CE91067024F3 BE114B343EB00981 64BAE5818D0570BB
XorT EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB

10
In   EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB
Enc  5A9C7B1F5B1C3B46 BE114B343EB00981 4FD3D2B7D74FBB42
XorT 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42

11
In   5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42
Enc  93B71967EED41FFC AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
XorT 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42

12
In   93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
Enc  1FA68B0A8112B44B AEF34BD8FB5A7B82 9D3E862371D2CFE5
XorT 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5

Output:
Ciphertext:  1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5
```

Unwrap:

| Step | t | A | R1 | R2 |
|---|---|---|---|---|
| 12 | | | | |
| In | | 1FA68B0A8112B447 | AEF34BD8FB5A7B82 | 9D3E862371D2CFE5 |
| XorT | | 1FA68B0A8112B44B | AEF34BD8FB5A7B82 | 9D3E862371D2CFE5 |
| Dec | | 93B71967EED41FF7 | AEF34BD8FB5A7B82 | 4FD3D2B7D74FBB42 |
| 11 | | | | |
| In | | 93B71967EED41FF7 | AEF34BD8FB5A7B82 | 4FD3D2B7D74FBB42 |
| XorT | | 93B71967EED41FFC | AEF34BD8FB5A7B82 | 4FD3D2B7D74FBB42 |
| Dec | | 5A9C7B1F5B1C3B4C | BE114B343EB00981 | 4FD3D2B7D74FBB42 |
| 10 | | | | |
| In | | 5A9C7B1F5B1C3B4C | BE114B343EB00981 | 4FD3D2B7D74FBB42 |
| XorT | | 5A9C7B1F5B1C3B46 | BE114B343EB00981 | 4FD3D2B7D74FBB42 |
| Dec | | EBE1CE91067024FA | BE114B343EB00981 | 64BAE5818D0570BB |
| 9 | | | | |
| In | | EBE1CE91067024FA | BE114B343EB00981 | 64BAE5818D0570BB |
| XorT | | EBE1CE91067024F3 | BE114B343EB00981 | 64BAE5818D0570BB |
| Dec | | 4BE8CE99C0A43A75 | B556D35ED8CEF052 | 64BAE5818D0570BB |
| 8 | | | | |
| In | | 4BE8CE99C0A43A75 | B556D35ED8CEF052 | 64BAE5818D0570BB |
| XorT | | 4BE8CE99C0A43A7D | B556D35ED8CEF052 | 64BAE5818D0570BB |
| Dec | | 2BFC21B2C20E4001 | B556D35ED8CEF052 | F14863BB1E9CA90A |
| 7 | | | | |
| In | | 2BFC21B2C20E4001 | B556D35ED8CEF052 | F14863BB1E9CA90A |
| XorT | | 2BFC21B2C20E4006 | B556D35ED8CEF052 | F14863BB1E9CA90A |
| Dec | | E3EE986344D878F1 | 25F5A3ADC2195401 | F14863BB1E9CA90A |
| 6 | | | | |
| In | | E3EE986344D878F1 | 25F5A3ADC2195401 | F14863BB1E9CA90A |
| XorT | | E3EE986344D878F7 | 25F5A3ADC2195401 | F14863BB1E9CA90A |
| Dec | | 93AEA71B258D90C6 | 25F5A3ADC2195401 | 07B2BD973E36A6FC |
| 5 | | | | |
| In | | 93AEA71B258D90C6 | 25F5A3ADC2195401 | 07B2BD973E36A6FC |
| XorT | | 93AEA71B258D90C3 | 25F5A3ADC2195401 | 07B2BD973E36A6FC |
| Dec | | 5896EA9028EE203F | FE6E8D679C5D3460 | 07B2BD973E36A6FC |
| 4 | | | | |
| In | | 5896EA9028EE203F | FE6E8D679C5D3460 | 07B2BD973E36A6FC |
| XorT | | 5896EA9028EE203B | FE6E8D679C5D3460 | 07B2BD973E36A6FC |
| Dec | | FC967627BE93720B | FE6E8D679C5D3460 | D132EE38147E76F8 |

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

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

   1
   In   F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF
   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:
   KEK:        000102030405060708090A0B0C0D0E0F1011121314151617
   Key Data:   00112233445566778899AABBCCDDEEFF

   Wrap:

   Step t       A                R1               R21
   In   A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Enc  DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
   XorT DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF

   2
   In   DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
   Enc  9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
   XorT 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D

   3
   In   9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
   Enc  7B8E343CA51CF8AB BC164F51E20CC983 51F22F3286758A2D
   XorT 7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D

   4
   In   7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D
   Enc  02A97C5897140595 BC164F51E20CC983 05FC2D8F8FF4B919
   XorT 02A97C5897140591 BC164F51E20CC983 05FC2D8F8FF4B919
```

```
5
In   02A97C5897140591 BC164F51E20CC983 05FC2D8F8FF4B919
Enc  15D4B63F66583817 429487269D3A0016 05FC2D8F8FF4B919
XorT 15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919

6
In   15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919
Enc  AE2D0B76A6951EEA 429487269D3A0016 05A2D8FB4DD5BD7A
XorT AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A

7
In   AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A
Enc  79F849444F4B8AA8 D40B091CDBAC0340 05A2D8FB4DD5BD7A
XorT 79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A

8
In   79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A
Enc  5933A9195B5F5E21 D40B091CDBAC0340 89F0D6C06F8CA9B4
XorT 5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4

9
In   5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4
Enc  57ADA800299C2E85 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
XorT 57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4

10
In   57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
Enc  BF17BD6A9BC80163 4D5B3DFE7C04ABBA EB24CCFA52EA9078
XorT BF17BD6A9BC80169 4D5B3DFE7C04ABBA EB24CCFA52EA9078

11
In   BF17BD6A9BC80169 4D5B3DFE7C04ABBA EB24CCFA52EA9078
Enc  B68BF270AE81544F F92B5B97C050AED2 EB24CCFA52EA9078
XorT B68BF270AE815444 F92B5B97C050AED2 EB24CCFA52EA9078

12
In   B68BF270AE815444 F92B5B97C050AED2 EB24CCFA52EA9078
Enc  96778B25AE6CA439 F92B5B97C050AED2 468AB8A17AD84E5D
XorT 96778B25AE6CA435 F92B5B97C050AED2 468AB8A17AD84E5D

Output:
Ciphertext:  96778B25AE6CA435 F92B5B97C050AED2 468AB8A17AD84E5D
```

Unwrap:

| Step | t | A | R1 | R2 |
|---|---|---|---|---|
| 12 | | | | |
| In | | 96778B25AE6CA435 | F92B5B97C050AED2 | 468AB8A17AD84E5D |
| XorT | | 96778B25AE6CA439 | F92B5B97C050AED2 | 468AB8A17AD84E5D |
| Dec | | B68BF270AE815444 | F92B5B97C050AED2 | EB24CCFA52EA9078 |
| 11 | | | | |
| In | | B68BF270AE815444 | F92B5B97C050AED2 | EB24CCFA52EA9078 |
| XorT | | B68BF270AE81544F | F92B5B97C050AED2 | EB24CCFA52EA9078 |
| Dec | | BF17BD6A9BC80169 | 4D5B3DFE7C04ABBA | EB24CCFA52EA9078 |
| 10 | | | | |
| In | | BF17BD6A9BC80169 | 4D5B3DFE7C04ABBA | EB24CCFA52EA9078 |
| XorT | | BF17BD6A9BC80163 | 4D5B3DFE7C04ABBA | EB24CCFA52EA9078 |
| Dec | | 57ADA800299C2E8C | 4D5B3DFE7C04ABBA | 89F0D6C06F8CA9B4 |
| 9 | | | | |
| In | | 57ADA800299C2E8C | 4D5B3DFE7C04ABBA | 89F0D6C06F8CA9B4 |
| XorT | | 57ADA800299C2E85 | 4D5B3DFE7C04ABBA | 89F0D6C06F8CA9B4 |
| Dec | | 5933A9195B5F5E29 | D40B091CDBAC0340 | 89F0D6C06F8CA9B4 |
| 8 | | | | |
| In | | 5933A9195B5F5E29 | D40B091CDBAC0340 | 89F0D6C06F8CA9B4 |
| XorT | | 5933A9195B5F5E21 | D40B091CDBAC0340 | 89F0D6C06F8CA9B4 |
| Dec | | 79F849444F4B8AAF | D40B091CDBAC0340 | 05A2D8FB4DD5BD7A |
| 7 | | | | |
| In | | 79F849444F4B8AAF | D40B091CDBAC0340 | 05A2D8FB4DD5BD7A |
| XorT | | 79F849444F4B8AA8 | D40B091CDBAC0340 | 05A2D8FB4DD5BD7A |
| Dec | | AE2D0B76A6951EEC | 429487269D3A0016 | 05A2D8FB4DD5BD7A |
| 6 | | | | |
| In | | AE2D0B76A6951EEC | 429487269D3A0016 | 05A2D8FB4DD5BD7A |
| XorT | | AE2D0B76A6951EEA | 429487269D3A0016 | 05A2D8FB4DD5BD7A |
| Dec | | 15D4B63F66583812 | 429487269D3A0016 | 05FC2D8F8FF4B919 |
| 5 | | | | |
| In | | 15D4B63F66583812 | 429487269D3A0016 | 05FC2D8F8FF4B919 |
| XorT | | 15D4B63F66583817 | 429487269D3A0016 | 05FC2D8F8FF4B919 |
| Dec | | 02A97C5897140591 | BC164F51E20CC983 | 05FC2D8F8FF4B919 |
| 4 | | | | |
| In | | 02A97C5897140591 | BC164F51E20CC983 | 05FC2D8F8FF4B919 |
| XorT | | 02A97C5897140595 | BC164F51E20CC983 | 05FC2D8F8FF4B919 |
| Dec | | 7B8E343CA51CF8A8 | BC164F51E20CC983 | 51F22F3286758A2D |

```
   3
   In   7B8E343CA51CF8A8 BC164F51E20CC983 51F22F3286758A2D
   XorT 7B8E343CA51CF8AB BC164F51E20CC983 51F22F3286758A2D
   Dec  9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D

   2
   In   9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
   XorT 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
   Dec  DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF

   1
   In   DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
   XorT DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
   Dec  A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF

   Plaintext A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF

   Output:
   Key Data:  00112233445566778899AABBCCDDEEFF
```

### 4.3 Wrap 128 bits of Key Data with a 256-bit KEK

```
   Input:
   KEK:000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
   Key Data:    00112233445566778899AABBCCDDEEFF

   Wrap:

   Step t       A                R1                R2
   1
   In   A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
   Enc  794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
   XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF

   2
   In   794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   Enc  D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
   XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8

   3
   In   D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
   Enc  85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8
   XorT 85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
```

```
4
In   85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
Enc  738C291128B7226D 5602001BFA07AD8B 58924F777C3F678C
XorT 738C291128B72269 5602001BFA07AD8B 58924F777C3F678C

5
In   738C291128B72269 5602001BFA07AD8B 58924F777C3F678C
Enc  2656A02DFFF054DC F4DF378183E3D5B2 58924F777C3F678C
XorT 2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C

6
In   2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
Enc  DDFD0C0E8B52A63A F4DF378183E3D5B2 91AC1D36A964F41B
XorT DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B

7
In   DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
Enc  39AB00D4AE4399EA 5271D5CED80F34ED 91AC1D36A964F41B
XorT 39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B

8
In   39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B
Enc  4CE414878463EAAC 5271D5CED80F34ED 67D8ED899E7929B8
XorT 4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8

9
In   4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8
Enc  FBB44DB106AA0789 0DF7E50829123648 67D8ED899E7929B8
XorT FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8

10
In   FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8
Enc  877112A7308ADCC5 0DF7E50829123648 3472D5993D318FD2
XorT 877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2

11
In   877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2
Enc  78E40190807CC151 63E9777905818A2A 3472D5993D318FD2
XorT 78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2

12
In   78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2
Enc  64E8C3F9CE0F5BAE 63E9777905818A2A 93C8191E7D6E8AE7
XorT 64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7

Output:
Ciphertext:  64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
```

Unwrap:

```
Step t       A                R1                R2
12
In   64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
XorT 64E8C3F9CE0F5BAE 63E9777905818A2A 93C8191E7D6E8AE7
Dec  78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2

11
In   78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2
XorT 78E40190807CC151 63E9777905818A2A 3472D5993D318FD2
Dec  877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2

10
In   877112A7308ADCCF 0DF7E50829123648 3472D5993D318FD2
XorT 877112A7308ADCC5 0DF7E50829123648 3472D5993D318FD2
Dec  FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8

9
In   FBB44DB106AA0780 0DF7E50829123648 67D8ED899E7929B8
XorT FBB44DB106AA0789 0DF7E50829123648 67D8ED899E7929B8
Dec  4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8

8
In   4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8
XorT 4CE414878463EAAC 5271D5CED80F34ED 67D8ED899E7929B8
Dec  39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B

7
In   39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B
XorT 39AB00D4AE4399EA 5271D5CED80F34ED 91AC1D36A964F41B
Dec  DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B

6
In   DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
XorT DDFD0C0E8B52A63A F4DF378183E3D5B2 91AC1D36A964F41B
Dec  2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C

5
In   2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
XorT 2656A02DFFF054DC F4DF378183E3D5B2 58924F777C3F678C
Dec  738C291128B72269 5602001BFA07AD8B 58924F777C3F678C

4
In   738C291128B72269 5602001BFA07AD8B 58924F777C3F678C
XorT 738C291128B7226D 5602001BFA07AD8B 58924F777C3F678C
Dec  85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
```

```
   3
   In   85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
   XorT 85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8
   Dec  D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8

   2
   In   D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
   XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
   Dec  794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF

   1
   In   794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
   XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
   Dec  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:
   KEK:       000102030405060708090A0B0C0D0E0F1011121314151617
   Key Data:  00112233445566778899AABBCCDDEEFF0001020304050607

   Wrap:

   Step t     A/R3             R1               R2

   1
   In   A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
        0001020304050607
   Enc  DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
   XorT DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607

   2
   In   DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
   Enc  9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
   XorT 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
```

```
   3
   In   9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
   Enc  2C8E19A519025B7C 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3
   XorT 2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3

   4
   In   2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3
   Enc  E727C7BDF822602E A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3
   XorT E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3

   5
   In   E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3
   Enc  15B61F7B25D51700 A08DAA041D17BBBA AE82BC1118A5DEA4
        FF540E514DE120A3
   XorT 15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
        FF540E514DE120A3

   6
   In   15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
        FF540E514DE120A3
   Enc  A187755AEA64719C A08DAA041D17BBBA AE82BC1118A5DEA4
        D1E708FD13778787
   XorT A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
        D1E708FD13778787

   7
   In   A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
        D1E708FD13778787
   Enc  5A994895D81644B7 926ED65A9E853FD9 AE82BC1118A5DEA4
        D1E708FD13778787
   XorT 5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
        D1E708FD13778787

   8
   In   5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
        D1E708FD13778787
   Enc  864F408C8AB8CDCF 926ED65A9E853FD9 552A09E141D08AE3
        D1E708FD13778787
   XorT 864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
        D1E708FD13778787
```

```
   9
   In   864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
        D1E708FD13778787
   Enc  53F4373F575EB7A4 926ED65A9E853FD9 552A09E141D08AE3
        ED5E8456E61BD295
   XorT 53F4373F575EB7AD 926ED65A9E853FD9 552A09E141D08AE3
        ED5E8456E61BD295

   10
   In   53F4373F575EB7AD 926ED65A9E853FD9 552A09E141D08AE3
        ED5E8456E61BD295
   Enc  9EAA4CDA0B1BA5FF 98883EDC6B080FB5 552A09E141D08AE3
        ED5E8456E61BD295
   XorT 9EAA4CDA0B1BA5F5 98883EDC6B080FB5 552A09E141D08AE3
        ED5E8456E61BD295

   11
   In   9EAA4CDA0B1BA5F5 98883EDC6B080FB5 552A09E141D08AE3
        ED5E8456E61BD295
   Enc  B1B9902C68E0EB52 98883EDC6B080FB5 63F6D88A0663FEF9
        ED5E8456E61BD295
   XorT B1B9902C68E0EB59 98883EDC6B080FB5 63F6D88A0663FEF9
        ED5E8456E61BD295

   12
   In   B1B9902C68E0EB59 98883EDC6B080FB5 63F6D88A0663FEF9
        ED5E8456E61BD295
   Enc  FCE591D77709A6E0 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5
   XorT FCE591D77709A6EC 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5

   13
   In   FCE591D77709A6EC 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5
   Enc  428428D2BD88CF58 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5
   XorT 428428D2BD88CF55 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5

   14
   In   428428D2BD88CF55 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5
   Enc  6AC861AB961DA578 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5
   XorT 6AC861AB961DA576 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5
```

```
   15
   In   6AC861AB961DA576 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5
   Enc  E80DB49CC9A1EA61 C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53
   XorT E80DB49CC9A1EA6E C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53

   16
   In   E80DB49CC9A1EA6E C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53
   Enc  ABEE3534AC465C2C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53
   XorT ABEE3534AC465C3C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53

   17
   In   ABEE3534AC465C3C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53
   Enc  E7CC8D8CEDE62BF7 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53
   XorT E7CC8D8CEDE62BE6 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53

   18
   In   E7CC8D8CEDE62BE6 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53
   Enc  031D33264E15D320 68F24EC260743EDC E1C6C7DDEE725A93
        6BA814915C6762D2
   XorT 031D33264E15D332 68F24EC260743EDC E1C6C7DDEE725A93
        6BA814915C6762D2

   Output:
   Ciphertext  031D33264E15D332 68F24EC260743EDC E1C6C7DDEE725A93
               6BA814915C6762D2

   Unwrap:

   Step t     A/R3             R1               R2

   18
   In   031D33264E15D332 68F24EC260743EDC E1C6C7DDEE725A93
        6BA814915C6762D2
   XorT 031D33264E15D320 68F24EC260743EDC E1C6C7DDEE725A93
        6BA814915C6762D2
   Dec  E7CC8D8CEDE62BE6 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53
```

```
   17
   In   E7CC8D8CEDE62BE6 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53
   XorT E7CC8D8CEDE62BF7 68F24EC260743EDC E1C6C7DDEE725A93
        84943C8C67FCFD53
   Dec  ABEE3534AC465C3C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53

   16
   In   ABEE3534AC465C3C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53
   XorT ABEE3534AC465C2C 68F24EC260743EDC 56E3CEE892BBEFC4
        84943C8C67FCFD53
   Dec  E80DB49CC9A1EA6E C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53

   15
   In   E80DB49CC9A1EA6E C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53
   XorT E80DB49CC9A1EA61 C46965F34EFB2261 56E3CEE892BBEFC4
        84943C8C67FCFD53
   Dec  6AC861AB961DA576 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5

   14
   In   6AC861AB961DA576 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5
   XorT 6AC861AB961DA578 C46965F34EFB2261 56E3CEE892BBEFC4
        463437433A93EFE5
   Dec  428428D2BD88CF55 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5

   13
   In   428428D2BD88CF55 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5
   XorT 428428D2BD88CF58 C46965F34EFB2261 63F6D88A0663FEF9
        463437433A93EFE5
   Dec  FCE591D77709A6EC 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5

   12
   In   FCE591D77709A6EC 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5
   XorT FCE591D77709A6E0 98883EDC6B080FB5 63F6D88A0663FEF9
        463437433A93EFE5
   Dec  B1B9902C68E0EB59 98883EDC6B080FB5 63F6D88A0663FEF9
        ED5E8456E61BD295
```

```
11
In   B1B9902C68E0EB59 98883EDC6B080FB5 63F6D88A0663FEF9
     ED5E8456E61BD295
XorT B1B9902C68E0EB52 98883EDC6B080FB5 63F6D88A0663FEF9
     ED5E8456E61BD295
Dec  9EAA4CDA0B1BA5F5 98883EDC6B080FB5 552A09E141D08AE3
     ED5E8456E61BD295

10
In   9EAA4CDA0B1BA5F5 98883EDC6B080FB5 552A09E141D08AE3
     ED5E8456E61BD295
XorT 9EAA4CDA0B1BA5FF 98883EDC6B080FB5 552A09E141D08AE3
     ED5E8456E61BD295
Dec  53F4373F575EB7AD 926ED65A9E853FD9 552A09E141D08AE3
     ED5E8456E61BD295

9
In   53F4373F575EB7AD 926ED65A9E853FD9 552A09E141D08AE3
     ED5E8456E61BD295
XorT 53F4373F575EB7A4 926ED65A9E853FD9 552A09E141D08AE3
     ED5E8456E61BD295
Dec  864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
     D1E708FD13778787

8
In   864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
     D1E708FD13778787
XorT 864F408C8AB8CDCF 926ED65A9E853FD9 552A09E141D08AE3
     D1E708FD13778787
Dec  5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
     D1E708FD13778787

7
In   5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
     D1E708FD13778787
XorT 5A994895D81644B7 926ED65A9E853FD9 AE82BC1118A5DEA4
     D1E708FD13778787
Dec  A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787

6
In   A187755AEA64719A A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787
XorT A187755AEA64719C A08DAA041D17BBBA AE82BC1118A5DEA4
     D1E708FD13778787
Dec  15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
     FF540E514DE120A3
```

```
   5
   In   15B61F7B25D51705 A08DAA041D17BBBA AE82BC1118A5DEA4
        FF540E514DE120A3
   XorT 15B61F7B25D51700 A08DAA041D17BBBA AE82BC1118A5DEA4
        FF540E514DE120A3
   Dec  E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3

   4
   In   E727C7BDF822602A A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3
   XorT E727C7BDF822602E A08DAA041D17BBBA 51F22F3286758A2D
        FF540E514DE120A3
   Dec  2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3

   3
   In   2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3
   XorT 2C8E19A519025B7C 351D385096CCFB29 51F22F3286758A2D
        FF540E514DE120A3
   Dec  9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
        0001020304050607

   2
   In   9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
   XorT 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
        0001020304050607
   Dec  DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607

   1
   In   DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
   XorT DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
        0001020304050607
   Dec  A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
        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

   2
   In   794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
        0001020304050607
   Enc  D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607
   XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607

   3
   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
     6CA405593A3B5154
Enc  BF213BFD04E8A24F 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     6CA405593A3B5154
XorT BF213BFD04E8A24A 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     6CA405593A3B5154

6
In   BF213BFD04E8A24A 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     6CA405593A3B5154
Enc  6F85BFBDB7E880E3 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B
XorT 6F85BFBDB7E880E5 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B

7
In   6F85BFBDB7E880E5 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B
Enc  D532789E4E79D819 444F92BF78E77BB1 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B
XorT D532789E4E79D81E 444F92BF78E77BB1 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B

8
In   D532789E4E79D81E 444F92BF78E77BB1 AEBE2D5C8BF747A9
     39EBC1A1A53FF55B
Enc  2A5FFCEF1F1916D8 444F92BF78E77BB1 C6874607903270CD
     39EBC1A1A53FF55B
XorT 2A5FFCEF1F1916D0 444F92BF78E77BB1 C6874607903270CD
     39EBC1A1A53FF55B

9
In   2A5FFCEF1F1916D0 444F92BF78E77BB1 C6874607903270CD
     39EBC1A1A53FF55B
Enc  01271BA91D9804F6 444F92BF78E77BB1 C6874607903270CD
     740A273461ED82C6
XorT 01271BA91D9804FF 444F92BF78E77BB1 C6874607903270CD
     740A273461ED82C6

10
In   01271BA91D9804FF 444F92BF78E77BB1 C6874607903270CD
     740A273461ED82C6
Enc  A3223BD7237F7033 FB1611A83BEB567F C6874607903270CD
     740A273461ED82C6
XorT A3223BD7237F7039 FB1611A83BEB567F C6874607903270CD
     740A273461ED82C6
```

```
   11
   In   A3223BD7237F7039 FB1611A83BEB567F C6874607903270CD
        740A273461ED82C6
   Enc  B50C330616E7B1C7 FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6
   XorT B50C330616E7B1CC FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6

   12
   In   B50C330616E7B1CC FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6
   Enc  FB8AFF3F083E12CE FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D
   XorT FB8AFF3F083E12C2 FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D

   13
   In   FB8AFF3F083E12C2 FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D
   Enc  82F597607784A33C FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D
   XorT 82F597607784A331 FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D

   14
   In   82F597607784A331 FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D
   Enc  D48E5E83B7C906DB FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D
   XorT D48E5E83B7C906D5 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D

   15
   In   D48E5E83B7C906D5 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D
   Enc  1BF2B1CD947311B6 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146
   XorT 1BF2B1CD947311B9 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146

   16
   In   1BF2B1CD947311B9 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146
   Enc  C9F5F26A378011DE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146
   XorT C9F5F26A378011CE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146
```

```
   17
   In   C9F5F26A378011CE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146
   Enc  39128CE5E435F3A0 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146
   XorT 39128CE5E4325F3B1 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146

   18
   In   39128CE5E435F3B1 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146
   Enc  A8F9BC1612C68B2D F6E6F4FBE30E71E4 769C8B80A32CB895
        8CD5D17D6B254DA1
   XorT A8F9BC1612C68B3F F6E6F4FBE30E71E4 769C8B80A32CB895
        8CD5D17D6B254DA1

   Ciphertext   A8F9BC1612C68B3F F6E6F4FBE30E71E4
                769C8B80A32CB895 8CD5D17D6B254DA1

   Unwrap:

   Step t     A/R3             R1               R2

   18
   In   A8F9BC1612C68B3F F6E6F4FBE30E71E4 769C8B80A32CB895
        8CD5D17D6B254DA1
   XorT A8F9BC1612C68B2D F6E6F4FBE30E71E4 769C8B80A32CB895
        8CD5D17D6B254DA1
   Dec  39128CE5E435F3B1 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146

   17
   In   39128CE5E435F3B1 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146
   XorT 39128CE5E435F3A0 F6E6F4FBE30E71E4 769C8B80A32CB895
        C490C33642717146
   Dec  C9F5F26A378011CE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146

   16
   In   C9F5F26A378011CE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146
   XorT C9F5F26A378011DE F6E6F4FBE30E71E4 D36F4FFBA2C82ED9
        C490C33642717146
   Dec  1BF2B1CD947311B9 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146
```

```
   15
   In   1BF2B1CD947311B9 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146
   XorT 1BF2B1CD947311B6 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        C490C33642717146
   Dec  D48E5E83B7C906D5 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D

   14
   In   D48E5E83B7C906D5 FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D
   XorT D48E5E83B7C906DB FB1F2965FCE1E783 D36F4FFBA2C82ED9
        0B08CFDF48020F0D
   Dec  82F597607784A331 FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D

   13
   In   82F597607784A331 FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D
   XorT 82F597607784A33C FB1F2965FCE1E783 73EDC8CB9322C34E
        0B08CFDF48020F0D
   Dec  FB8AFF3F083E12C2 FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D

   12
   In   FB8AFF3F083E12C2 FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D
   XorT FB8AFF3F083E12CE FB1611A83BEB567F 73EDC8CB9322C34E
        0B08CFDF48020F0D
   Dec  B50C330616E7B1CC FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6

   11
   In   B50C330616E7B1CC FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6
   XorT B50C330616E7B1C7 FB1611A83BEB567F 73EDC8CB9322C34E
        740A273461ED82C6
   Dec  A3223BD7237F7039 FB1611A83BEB567F C6874607903270CD
        740A273461ED82C6

   10
   In   A3223BD7237F7039 FB1611A83BEB567F C6874607903270CD
        740A273461ED82C6
   XorT A3223BD7237F7033 FB1611A83BEB567F C6874607903270CD
        740A273461ED82C6
   Dec  01271BA91D9804FF 444F92BF78E77BB1 C6874607903270CD
        740A273461ED82C6
```

```
   9
   In   01271BA91D9804FF 444F92BF78E77BB1 C6874607903270CD
        740A273461ED82C6
   XorT 01271BA91D9804F6 444F92BF78E77BB1 C6874607903270CD
        740A273461ED82C6
   Dec  2A5FFCEF1F1916D0 444F92BF78E77BB1 C6874607903270CD
        39EBC1A1A53FF55B

   8
   In   2A5FFCEF1F1916D0 444F92BF78E77BB1 C6874607903270CD
        39EBC1A1A53FF55B
   XorT 2A5FFCEF1F1916D8 444F92BF78E77BB1 C6874607903270CD
        39EBC1A1A53FF55B
   Dec  D532789E4E79D81E 444F92BF78E77BB1 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B

   7
   In   D532789E4E79D81E 444F92BF78E77BB1 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B
   XorT D532789E4E79D819 444F92BF78E77BB1 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B
   Dec  6F85BFBDB7E880E5 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B

   6
   In   6F85BFBDB7E880E5 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B
   XorT 6F85BFBDB7E880E3 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        39EBC1A1A53FF55B
   Dec  BF213BFD04E8A24A 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        6CA405593A3B5154

   5
   In   BF213BFD04E8A24A 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        6CA405593A3B5154
   XorT BF213BFD04E8A24F 0CC86A4D9B9C6A31 AEBE2D5C8BF747A9
        6CA405593A3B5154
   Dec  F1D28EA6295891E8 0CC86A4D9B9C6A31 F60E0CDB7F429FE8
        6CA405593A3B5154

   4
   In   F1D28EA6295891E8 0CC86A4D9B9C6A31 F60E0CDB7F429FE8
        6CA405593A3B5154
   XorT F1D28EA6295891EC 0CC86A4D9B9C6A31 F60E0CDB7F429FE8
        6CA405593A3B5154
   Dec  9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154
```

```
   3
   In   9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154
   XorT 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154
   Dec  D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607

   2
   In   D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607
   XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607
   Dec  794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
        0001020304050607

   1
   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:
     00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F
```

Wrap:

```
Step t     A/R3             R1/R4            R2

1
In   A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
     0001020304050607 08090A0B0C0D0E0F
Enc  794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
     0001020304050607 08090A0B0C0D0E0F
XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
     0001020304050607 08090A0B0C0D0E0F

2
In   794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
     0001020304050607 08090A0B0C0D0E0F
Enc  D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607 08090A0B0C0D0E0F
XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607 08090A0B0C0D0E0F

3
In   D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
     0001020304050607 08090A0B0C0D0E0F
Enc  9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 08090A0B0C0D0E0F
XorT 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 08090A0B0C0D0E0F

4
In   9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 08090A0B0C0D0E0F
Enc  564408FDD0DD2EA4 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 E5923CB9FDB56FBC
XorT 564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 E5923CB9FDB56FBC

5
In   564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
     6CA405593A3B5154 E5923CB9FDB56FBC
Enc  4EF02EDD3146AFBB E7D1194D853E53F8 F60E0CDB7F429FE8
     6CA405593A3B5154 E5923CB9FDB56FBC
XorT 4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
     6CA405593A3B5154 E5923CB9FDB56FBC
```

```
   6
   In   4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC
   Enc  963AAFFD96B223EC E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC
   XorT 963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC

   7
   In   963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC
   Enc  66D7A8ADD086B9DD E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC
   XorT 66D7A8ADD086B9DA E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC

   8
   In   66D7A8ADD086B9DA E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC
   Enc  C58B9D3AC6D5B94E E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT C58B9D3AC6D5B946 E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74

   9
   In   C58B9D3AC6D5B946 E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   Enc  1A681354E84C41F8 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT 1A681354E84C41F1 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74

   10
   In   1A681354E84C41F1 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   Enc  DBA417FB51F9E3CB D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT DBA417FB51F9E3C1 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74

   11
   In   DBA417FB51F9E3C1 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74
   Enc  0629EB29A42E4FD9 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 73E3B6CBE5D05D74
   XorT 0629EB29A42E4FD2 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 73E3B6CBE5D05D74
```

```
   12
   In   0629EB29A42E4FD2 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 73E3B6CBE5D05D74
   Enc  F9ED8A1429515665 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   XorT F9ED8A1429515669 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9

   13
   In   F9ED8A1429515669 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   Enc  2E8E2B6BB2016696 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   XorT 2E8E2B6BB201669B 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9

   14
   In   2E8E2B6BB201669B 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   Enc  15342443CB95ADB1 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9
   XorT 15342443CB95ADBF 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9

   15
   In   15342443CB95ADBF 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9
   Enc  33FE29365885C4B7 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9
   XorT 33FE29365885C4B8 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9

   16
   In   33FE29365885C4B8 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9
   Enc  5075496800978B4A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   XorT 5075496800978B5A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C

   17
   In   5075496800978B5A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   Enc  A5382A26B47551F1 1BB8C765A84195E7 BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   XorT A5382A26B47551E0 1BB8C765A84195E7 BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
```

```
18
In   A5382A26B47551E0 1BB8C765A84195E7 BCA418BBF7DCE60B
     C272E9466AAE98F9 40F68C91DB49702C
Enc  F19D80D437EFE8F9 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C
XorT F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C

19
In   F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
     C272E9466AAE98F9 40F68C91DB49702C
Enc  B422B444B87A190B 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 40F68C91DB49702C
XorT B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 40F68C91DB49702C

20
In   B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 40F68C91DB49702C
Enc  D058823360F88A37 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73

21
In   D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
Enc  C89A96CA7B163ECC CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73

22
In   C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
     1CFBF6B4C24CB982 07DFE775B9687E73
Enc  39D02FE7435870ED CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73
XorT 39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73

23
In   39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
     1CFBF6B4C24CB982 07DFE775B9687E73
Enc  0AEB82AE3146A91B CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B 07DFE775B9687E73
XorT 0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B 07DFE775B9687E73
```

```
   24
   In   0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B 07DFE775B9687E73
   Enc  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
   In   28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B FB988B9B7A02DD21
   XorT 28C9F404C4B810EC CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B FB988B9B7A02DD21
   Dec  0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B 07DFE775B9687E73

   23
   In   0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B 07DFE775B9687E73
   XorT 0AEB82AE3146A91B CBCCB35CFB87F826 3F5786E2D80ED326
        CBC7F0E71A99F43B 07DFE775B9687E73
   Dec  39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
        1CFBF6B4C24CB982 07DFE775B9687E73

   22
   In   39D02FE7435870FB CBCCB35CFB87F826 3F5786E2D80ED326
        1CFBF6B4C24CB982 07DFE775B9687E73
   XorT 39D02FE7435870ED CBCCB35CFB87F826 3F5786E2D80ED326
        1CFBF6B4C24CB982 07DFE775B9687E73
   Dec  C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73

   21
   In   C89A96CA7B163ED9 CBCCB35CFB87F826 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73
   XorT C89A96CA7B163ECC CBCCB35CFB87F826 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73
   Dec  D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73
```

```
   20
   In   D058823360F88A23 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73
   XorT D058823360F88A37 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 07DFE775B9687E73
   Dec  B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 40F68C91DB49702C

   19
   In   B422B444B87A1918 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 40F68C91DB49702C
   XorT B422B444B87A190B 1BB8C765A84195E7 F7EDAD518C960D36
        1CFBF6B4C24CB982 40F68C91DB49702C
   Dec  F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
        C272E9466AAE98F9 40F68C91DB49702C

   18
   In   F19D80D437EFE8EB 1BB8C765A84195E7 F7EDAD518C960D36
        C272E9466AAE98F9 40F68C91DB49702C
   XorT F19D80D437EFE8F9 1BB8C765A84195E7 F7EDAD518C960D36
        C272E9466AAE98F9 40F68C91DB49702C
   Dec  A5382A26B47551E0 1BB8C765A84195E7 BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C

   17
   In   A5382A26B47551E0 1BB8C765A84195E7 BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   XorT A5382A26B47551F1 1BB8C765A84195E7 BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   Dec  5075496800978B5A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C

   16
   In   5075496800978B5A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   XorT 5075496800978B4A 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 40F68C91DB49702C
   Dec  33FE29365885C4B8 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9

   15
   In   33FE29365885C4B8 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9
   XorT 33FE29365885C4B7 4745856AF333F01F BCA418BBF7DCE60B
        C272E9466AAE98F9 3CF149E90E8C04D9
   Dec  15342443CB95ADBF 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9
```

```
   14
   In   15342443CB95ADBF 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9
   XorT 15342443CB95ADB1 4745856AF333F01F BCA418BBF7DCE60B
        F56701DAF0388216 3CF149E90E8C04D9
   Dec  2E8E2B6BB201669B 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9

   13
   In   2E8E2B6BB201669B 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   XorT 2E8E2B6BB2016696 4745856AF333F01F FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   Dec  F9ED8A1429515669 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9

   12
   In   F9ED8A1429515669 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   XorT F9ED8A1429515665 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 3CF149E90E8C04D9
   Dec  0629EB29A42E4FD2 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 73E3B6CBE5D05D74

   11
   In   0629EB29A42E4FD2 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        F56701DAF0388216 73E3B6CBE5D05D74
   XorT 0629EB29A42E4FD9 D6AE29ECE7192D43 FBEC169FA5C0F6BA

        F56701DAF0388216 73E3B6CBE5D05D74
   Dec  DBA417FB51F9E3C1 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74

   10
   In   DBA417FB51F9E3C1 D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT DBA417FB51F9E3CB D6AE29ECE7192D43 FBEC169FA5C0F6BA
        C365B66943E2D760 73E3B6CBE5D05D74
   Dec  1A681354E84C41F1 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74

   9
   In   1A681354E84C41F1 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT 1A681354E84C41F8 D6AE29ECE7192D43 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   Dec  C58B9D3AC6D5B946 E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
```

```
   8
   In   C58B9D3AC6D5B946 E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   XorT C58B9D3AC6D5B94E E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 73E3B6CBE5D05D74
   Dec  66D7A8ADD086B9DA E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC

   7
   In   66D7A8ADD086B9DA E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC
   XorT 66D7A8ADD086B9DD E7D1194D853E53F8 EFD48BA304945576
        C365B66943E2D760 E5923CB9FDB56FBC
   Dec  963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC

   6
   In   963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC
   XorT 963AAFFD96B223EC E7D1194D853E53F8 EFD48BA304945576
        6CA405593A3B5154 E5923CB9FDB56FBC
   Dec  4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC

   5
   In   4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC
   XorT 4EF02EDD3146AFBB E7D1194D853E53F8 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC
   Dec  564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC

   4
   In   564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC
   XorT 564408FDD0DD2EA4 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 E5923CB9FDB56FBC
   Dec  9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 08090A0B0C0D0E0F

   3
   In   9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 08090A0B0C0D0E0F
   XorT 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE8
        6CA405593A3B5154 08090A0B0C0D0E0F
   Dec  D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607 08090A0B0C0D0E0F
```

```
   2
   In   D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607 08090A0B0C0D0E0F
   XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
        0001020304050607 08090A0B0C0D0E0F
   Dec  794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
        0001020304050607 08090A0B0C0D0E0F

   1
   In   794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
        0001020304050607 08090A0B0C0D0E0F
   XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
        0001020304050607 08090A0B0C0D0E0F
   Dec  A6A6A6A6A6A6A6A6 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



## Acknowledgement

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