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	17
4.5 Wrap 192 bits of Key Data with a 256-bit KEK	24
4.6 Wrap 256 bits of Key Data with a 256-bit KEK	30

5.	Security Considerations	39
6.	References	39
7.	Acknowledgments	39
8.	Authors' Addresses	39
9.	Full Copyright Statement	40

#### 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 nonlinear 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) AES-1(K, W) MSB(j, W) LSB(j, W) B1 ^ B2 B1   B2 K n s P[i] C[i] A R[i]	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 Concatenate B1 and B2 The key-encryption key K The number of 64-bit key data blocks The number of steps in the wrapping process, s = 6n The ith plaintext key data block The ith ciphertext data block The 64-bit integrity check register 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). Ciphertext, (n+1) 64-bit values  $\{C0, C1, \ldots, Cn\}$ . Outputs:

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 \mid 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 {CO, Cl, ..., 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 {CO, Cl, ..., Cn}, and
        Key, K (the KEK).
Outputs: Plaintext, n 64-bit values {PO, 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:

000102030405060708090A0B0C0D0E0F KEK: Key Data: 00112233445566778899AABBCCDDEEFF

Wrap:

```
Step t A
              R1
                        R2
```

1

In A6A6A6A6A6A6A6A 0011223344556677 8899AABBCCDDEEFF Enc F4740052E82A2251 74CE86FBD7B805E7 8899AABBCCDDEEFF XorT F4740052E82A2250 74CE86FBD7B805E7 8899AABBCCDDEEFF

2

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

3

06BA4EBDE7768D09 74CE86FBD7B805E7 D132EE38147E76F8 In 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
In 93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC
Enc E3EE986344D878F7 25F5A3ADC2195401 F14863BB1E9CA90A
XorT E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
7
    E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
In
Enc 2BFC21B2C20E4006 B556D35ED8CEF052 F14863BB1E9CA90A
XorT 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
8
In 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
Enc 4BE8CE99C0A43A7D B556D35ED8CEF052 64BAE5818D0570BB
XorT 4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB
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
   1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5
In
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
  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
    02A97C5897140591 BC164F51E20CC983 05FC2D8F8FF4B919
In
Enc 15D4B63F66583817 429487269D3A0016 05FC2D8F8FF4B919
XorT 15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919
6
In 15D4B63F66583812 429487269D3A0016 05FC2D8F8FF4B919
Enc AE2D0B76A6951EEA 429487269D3A0016 05A2D8FB4DD5BD7A
XorT AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A
In AE2D0B76A6951EEC 429487269D3A0016 05A2D8FB4DD5BD7A
Enc 79F849444F4B8AA8 D40B091CDBAC0340 05A2D8FB4DD5BD7A
XorT 79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A
8
    79F849444F4B8AAF D40B091CDBAC0340 05A2D8FB4DD5BD7A
In
Enc 5933A9195B5F5E21 D40B091CDBAC0340 89F0D6C06F8CA9B4
XorT 5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4
9
In 5933A9195B5F5E29 D40B091CDBAC0340 89F0D6C06F8CA9B4
Enc 57ADA800299C2E85 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
XorT 57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
10
    57ADA800299C2E8C 4D5B3DFE7C04ABBA 89F0D6C06F8CA9B4
In
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	R	1	R	2
12 In XorT Dec	96778B25	5AE6CA435 5AE6CA439 0AE815444	F92B5B97	C050AED2 C050AED2 C050AED2	468AB8A1 468AB8A1 EB24CCFA	7AD84E5D
11 In XorT Dec	B68BF270	)AE815444 )AE81544F A9BC80169	F92B5B97	C050AED2 C050AED2 7C04ABBA	EB24CCFA EB24CCFA EB24CCFA	52EA9078
10 In XorT Dec	BF17BD6A	A9BC80169 A9BC80163 )299C2E8C	4D5B3DFE	7C04ABBA 7C04ABBA 7C04ABBA	EB24CCFA EB24CCFA 89F0D6C0	52EA9078
9 In XorT Dec	57ADA800	)299C2E8C )299C2E85 )5B5F5E29		7C04ABBA 7C04ABBA DBAC0340	89F0D6C0 89F0D6C0 89F0D6C0	6F8CA9B4
8 In XorT Dec	5933A919	95B5F5E29 95B5F5E21 14F4B8AAF	D40B091C D40B091C D40B091C		89F0D6C0 89F0D6C0 05A2D8FB	6F8CA9B4
7 In XorT Dec	79F84944	14F4B8AAF 14F4B8AA8 5A6951EEC	D40B091C D40B091C 42948726		05A2D8FB 05A2D8FB 05A2D8FB	4DD5BD7A
6 In XorT Dec	AE2D0B76	5A6951EEC 5A6951EEA 766583812	42948726	9D3A0016 9D3A0016 9D3A0016	05A2D8FB 05A2D8FB 05FC2D8F	4DD5BD7A
5 In XorT Dec	15D4B63E	766583812 766583817 397140591	42948726	9D3A0016 9D3A0016 E20CC983	05FC2D8F 05FC2D8F 05FC2D8F	8FF4B919
4 In XorT Dec	02A97C58	397140591 397140595 CA51CF8A8	BC164F51	E20CC983 E20CC983 E20CC983	05FC2D8F 05FC2D8F 51F22F32	8FF4B919

```
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 A6A6A6A6A6A6A6A 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:
                             R1
  Step t A
                                               R2
  1
  In A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
  Enc 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
  XorT 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
  2
       794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
  In
  Enc D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
  XorT D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
  In D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
  Enc 85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8
  XorT 85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
```

```
4
    85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
In
Enc 738C291128B7226D 5602001BFA07AD8B 58924F777C3F678C
XorT 738C291128B72269 5602001BFA07AD8B 58924F777C3F678C
5
    738C291128B72269 5602001BFA07AD8B 58924F777C3F678C
In
Enc 2656A02DFFF054DC F4DF378183E3D5B2 58924F777C3F678C
XorT 2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
In 2656A02DFFF054D9 F4DF378183E3D5B2 58924F777C3F678C
Enc DDFD0C0E8B52A63A F4DF378183E3D5B2 91AC1D36A964F41B
XorT DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
7
    DDFD0C0E8B52A63C F4DF378183E3D5B2 91AC1D36A964F41B
In
Enc 39AB00D4AE4399EA 5271D5CED80F34ED 91AC1D36A964F41B
XorT 39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B
8
In 39AB00D4AE4399ED 5271D5CED80F34ED 91AC1D36A964F41B
Enc 4CE414878463EAAC 5271D5CED80F34ED 67D8ED899E7929B8
XorT 4CE414878463EAA4 5271D5CED80F34ED 67D8ED899E7929B8
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
    78E40190807CC15A 63E9777905818A2A 3472D5993D318FD2
In
Enc 64E8C3F9CE0F5BAE 63E9777905818A2A 93C8191E7D6E8AE7
XorT 64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
Output:
Ciphertext: 64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
```

### Unwrap:

```
Step t A
                            R1
                                             R2
12
   64E8C3F9CE0F5BA2 63E9777905818A2A 93C8191E7D6E8AE7
In
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
       85DBDF1879D5C0A6 5602001BFA07AD8B F60E0CDB7F429FE8
  In
  XorT 85DBDF1879D5C0A5 5602001BFA07AD8B F60E0CDB7F429FE8
  Dec D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
  2
  In D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
  XorT D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
  Dec 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
  In 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
  XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
  Dec A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
  Plaintext A6A6A6A6A6A6A6A 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
  1
       A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
       0001020304050607
  Enc DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
       0001020304050607
  XorT DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
       0001020304050607
  2
       DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
       0001020304050607
  Enc 9D9B32B9ED742E02 351D385096CCFB29 51F22F3286758A2D
       0001020304050607
  XorT 9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
```

0001020304050607

```
3
     9D9B32B9ED742E00 351D385096CCFB29 51F22F3286758A2D
In
     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
    5A994895D81644B0 926ED65A9E853FD9 AE82BC1118A5DEA4
In
    D1E708FD13778787
Enc 864F408C8AB8CDCF 926ED65A9E853FD9 552A09E141D08AE3
    D1E708FD13778787
XorT 864F408C8AB8CDC7 926ED65A9E853FD9 552A09E141D08AE3
    D1E708FD13778787
```

9 Tm	064E400G07D0GDG7	926ED65A9E853FD9	552A09E141D08AE3
In	864F408C8AB8CDC7 D1E708FD13778787	920ED03A9E033FD9	552AU9E141DU6AE3
Enc	53F4373F575EB7A4 ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
XorT	53F4373F575EB7AD ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
10			
In	53F4373F575EB7AD ED5E8456E61BD295	926ED65A9E853FD9	552A09E141D08AE3
Enc	9EAA4CDA0B1BA5FF ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
XorT	9EAA4CDA0B1BA5F5 ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
11			
In	9EAA4CDA0B1BA5F5 ED5E8456E61BD295	98883EDC6B080FB5	552A09E141D08AE3
Enc	B1B9902C68E0EB52 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
XorT	B1B9902C68E0EB59 ED5E8456E61BD295	98883EDC6B080FB5	63F6D88A0663FEF9
12			
12 In	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9
	ED5E8456E61BD295 FCE591D77709A6E0	98883EDC6B080FB5 98883EDC6B080FB5	63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC		
In Enc	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5	98883EDC6B080FB5 98883EDC6B080FB5	63F6D88A0663FEF9
In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 FCE591D77709A6EC	98883EDC6B080FB5 98883EDC6B080FB5	63F6D88A0663FEF9
In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc XorT  13 In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5 428428D2BD88CF55	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5 C46965F34EFB2261	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc XorT  13 In Enc	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5 428428D2BD88CF55 463437433A93EFE5	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5 C46965F34EFB2261	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc XorT  13 In Enc XorT	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5  FCE591D77709A6EC 463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5 428428D2BD88CF55 463437433A93EFE5 428428D2BD88CF55 463437433A93EFE5 6AC861AB961DA578	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5 C46965F34EFB2261 C46965F34EFB2261	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9
In Enc XorT  13 In Enc XorT  14 In Enc	ED5E8456E61BD295 FCE591D77709A6E0 463437433A93EFE5 FCE591D77709A6EC 463437433A93EFE5  FCE591D77709A6EC 463437433A93EFE5 428428D2BD88CF58 463437433A93EFE5 428428D2BD88CF55 463437433A93EFE5	98883EDC6B080FB5 98883EDC6B080FB5 98883EDC6B080FB5 C46965F34EFB2261 C46965F34EFB2261 C46965F34EFB2261	63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 63F6D88A0663FEF9 53F6D88A0663FEF9 56E3CEE892BBEFC4

15 In	6AC861AB961DA576 463437433A93EFE5	C46965F34EFB2261	56E3CEE892BBEFC4
Enc	E80DB49CC9A1EA61 84943C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
XorT	E80DB49CC9A1EA6E 84943C8C67FCFD53	C46965F34EFB2261	56E3CEE892BBEFC4
16 In		C46965F34EFB2261	56E3CEE892BBEFC4
Enc	84943C8C67FCFD53 ABEE3534AC465C2C 84943C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
XorT		68F24EC260743EDC	56E3CEE892BBEFC4
17		60-04-6060543	5.5-2.5-2.0.0-2-2-4
In	84943C8C67FCFD53	68F24EC260743EDC	
Enc	E7CC8D8CEDE62BF7 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	E7CC8D8CEDE62BE6 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
18 In	#7CC8D8C#D#62B#6	68F24EC260743EDC	F1C6C7DDFF725x93
	84943C8C67FCFD53		
Enc	031D33264E15D320 6BA814915C6762D2	68F24EC260743EDC	EIC6C7DDEE725A93
XorT	031D33264E15D332 6BA814915C6762D2	68F24EC260743EDC	E1C6C7DDEE725A93
Outp Ciph			0743EDC E1C6C7DDEE725A93
Unwr	ap:		
Step	t A/R3	R1	R2
18 In	031D33264E15D332 6BA814915C6762D2	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	031D33264E15D320	68F24EC260743EDC	E1C6C7DDEE725A93
Dec	6BA814915C6762D2 E7CC8D8CEDE62BE6 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93

17			
In	E7CC8D8CEDE62BE6 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
XorT	E7CC8D8CEDE62BF7 84943C8C67FCFD53	68F24EC260743EDC	E1C6C7DDEE725A93
Dec	ABEE3534AC465C3C 84943C8C67FCFD53	68F24EC260743EDC	56E3CEE892BBEFC4
16 Tn	ADEE2524AC465C2C	68F24EC260743EDC	56E3CEE892BBEFC4
In	ABEE3534AC465C3C 84943C8C67FCFD53		50E3CEE092BBEFC4
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	FCE591D77709A6EC 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
12			
In	FCE591D77709A6EC 463437433A93EFE5	98883EDC6B080FB5	63F6D88A0663FEF9
XorT	FCE591D77709A6E0	98883EDC6B080FB5	63F6D88A0663FEF9
Dec	463437433A93EFE5 B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9

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

```
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
     2C8E19A519025B7F 351D385096CCFB29 51F22F3286758A2D
In
     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
     DFE8FD5D1A3786A6 351D385096CCFB29 8899AABBCCDDEEFF
     0001020304050607
XorT DFE8FD5D1A3786A7 351D385096CCFB29 8899AABBCCDDEEFF
     0001020304050607
Dec A6A6A6A6A6A6A6A 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 6CA405593A3B5154	0CC86A4D9B9C6A31	F60E0CDB7F429FE8
Enc	BF213BFD04E8A24F 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT	BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
6			
In	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
0			
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	01271BA91D9804FF 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
10			
In	01271BA91D9804FF 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
Enc	A3223BD7237F7033 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
XorT	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD

11			
In	A3223BD7237F7039 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
Enc	B50C330616E7B1C7 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
XorT	B50C330616E7B1CC 740A273461ED82C6	FB1611A83BEB567F	73EDC8CB9322C34E
12	DE 0.0220616E7D100	FB1611A83BEB567F	73EDC8CB9322C34E
In	B50C330616E7B1CC 740A273461ED82C6		/3EDC6CB9322C34E
Enc	FB8AFF3F083E12CE 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
XorT	FB8AFF3F083E12C2 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
13			
In	FB8AFF3F083E12C2 0B08CFDF48020F0D	FB1611A83BEB567F	73EDC8CB9322C34E
Enc	82F597607784A33C 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
XorT	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
14			
In	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
Enc	D48E5E83B7C906DB 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
15			
In	D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Enc	1BF2B1CD947311B6 C490C33642717146	FB1F2965FCE1E783	D36F4FFBA2C82ED9
XorT	1BF2B1CD947311B9 C490C33642717146	FB1F2965FCE1E783	D36F4FFBA2C82ED9
16			
In	1BF2B1CD947311B9 C490C33642717146	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Enc	C9F5F26A378011DE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9
XorT	C490C33642717146 C9F5F26A378011CE C490C33642717146	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9

17			
In	C9F5F26A3780110	CE F6E6F4FBE30E71E4	D36F4FFRA2C82FD9
111	C490C3364271714		D30F 4FFBAZC0ZED9
Enc		40 AO F6E6F4FBE30E71E4	760000007220006
EIIC			709C0B0UA32CB095
	C490C336427171		4 560 60 50 50 50 650 65
Xor'l'		3B1 F6E6F4FBE30E71E	4 769C8B80A32CB895
	C490C336427171	16	
18			
In		31 F6E6F4FBE30E71E4	769C8B80A32CB895
	C490C336427171	16	
Enc	A8F9BC1612C68B	2D F6E6F4FBE30E71E4	769C8B80A32CB895
	8CD5D17D6B254D2	A1	
XorT	A8F9BC1612C68B	3F F6E6F4FBE30E71E4	769C8B80A32CB895
	8CD5D17D6B254D2	A1	
Ciphe	ertext A8F9BC	1612C68B3F F6E6F4FB	E30E71E4
01111		30A32CB895 8CD5D17D	
	, 0,000	30113262633	0223 12111
Unwra	an:		
Oliwic	λp·		
Cton	t A/R3	R1	R2
Step	t A/R3	KI	RZ
1.0			
18	7.0E0DG1.C1.0GC0D	)	760000000000000000
18 In		3F F6E6F4FBE30E71E4	769C8B80A32CB895
In	8CD5D17D6B254D2	A1	
In	8CD5D17D6B254D2 A8F9BC1612C68B2	A1 2D F6E6F4FBE30E71E4	
In XorT	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2	A1 2D F6E6F4FBE30E71E4 A1	769C8B80A32CB895
In	8CD5D17D6B254D2 A8F9BC1612C68B2 8CD5D17D6B254D2 39128CE5E435F31	A1 2D F6E6F4FBE30E71E4 A1 B1 F6E6F4FBE30E71E4	769C8B80A32CB895
In XorT	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2	A1 2D F6E6F4FBE30E71E4 A1 B1 F6E6F4FBE30E71E4	769C8B80A32CB895
In XorT	8CD5D17D6B254D2 A8F9BC1612C68B2 8CD5D17D6B254D2 39128CE5E435F31	A1 2D F6E6F4FBE30E71E4 A1 B1 F6E6F4FBE30E71E4	769C8B80A32CB895
In XorT	8CD5D17D6B254D2 A8F9BC1612C68B2 8CD5D17D6B254D2 39128CE5E435F31	A1 2D F6E6F4FBE30E71E4 A1 B1 F6E6F4FBE30E71E4	769C8B80A32CB895
In XorT Dec	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F31 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 B1 F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895
In XorT Dec	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F31 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F31 C490C3364271714 39128CE5E435F31 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F31 C490C3364271714 39128CE5E435F31 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In XorT	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In XorT	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F32 C490C3364271714 C9F5F26A3780116	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In XorT Dec	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F32 C490C3364271714 C9F5F26A3780116	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895
In XorT Dec 17 In XorT Dec	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 C9F5F26A3780116 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 31 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 D36F4FFBA2C82ED9
In XorT Dec 17 In XorT Dec	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F32 C490C3364271714 C9F5F26A3780116 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 A6 B1 F6E6F4FBE30E71E4 A0 F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 D36F4FFBA2C82ED9
In XorT Dec 17 In XorT Dec 16 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F31 C490C3364271714 39128CE5E435F32 C490C3364271714 39128CE5E435F32 C490C3364271714 C9F5F26A3780116 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 46 B1 F6E6F4FBE30E71E4 46 A0 F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4 46 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 D36F4FFBA2C82ED9
In XorT Dec 17 In XorT Dec 16 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 39128CE5E435F33 C490C3364271714 C9F5F26A3780116 C490C3364271714 C9F5F26A3780116 C490C3364271714	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 A6 B1 F6E6F4FBE30E71E4 A0 F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 D36F4FFBA2C82ED9
In XorT Dec 17 In XorT Dec 16 In	8CD5D17D6B254D2 A8F9BC1612C68B3 8CD5D17D6B254D2 39128CE5E435F33 C490C3364271712 39128CE5E435F33 C490C3364271712 39128CE5E435F33 C490C3364271712 C9F5F26A3780110 C490C3364271712 C9F5F26A37801110 C490C3364271712	A1 2D F6E6F4FBE30E71E4 A1 31 F6E6F4FBE30E71E4 A6 B1 F6E6F4FBE30E71E4 A0 F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4 A6 CE F6E6F4FBE30E71E4	769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 769C8B80A32CB895 D36F4FFBA2C82ED9 D36F4FFBA2C82ED9

C490C33642717146

15 In	1BF2B1CD947311B9	FB1F2965FCE1E783	D26E4EED32C02ED0
	C490C33642717146		
XorT	1BF2B1CD947311B6 C490C33642717146	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Dec	D48E5E83B7C906D5 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
14 In	D48E5E83B7C906D5	FB1F2965FCE1E783	D36E4EED33C03ED0
T11	0B08CFDF48020F0D		
XorT	D48E5E83B7C906DB 0B08CFDF48020F0D	FB1F2965FCE1E783	D36F4FFBA2C82ED9
Dec	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
13			
In	82F597607784A331 0B08CFDF48020F0D	FB1F2965FCE1E783	73EDC8CB9322C34E
XorT	82F597607784A33C 0B08CFDF48020F0D	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	FB1611A83BEB567F	73EDC8CB9322C34E
Dec	740A273461ED82C6 A3223BD7237F7039 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
10			
In	A3223BD7237F7039 740A273461ED82C6	FB1611A83BEB567F	C6874607903270CD
XorT	A3223BD7237F7033	FB1611A83BEB567F	C6874607903270CD
Dec	740A273461ED82C6 01271BA91D9804FF 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD

9	0100107010000400	444500555055555	GC0E4C0E0020E0GD
In	01271BA91D9804FF 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
XorT	01271BA91D9804F6 740A273461ED82C6	444F92BF78E77BB1	C6874607903270CD
Dec		444F92BF78E77BB1	C6874607903270CD
8			
In	2A5FFCEF1F1916D0 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
XorT	2A5FFCEF1F1916D8 39EBC1A1A53FF55B	444F92BF78E77BB1	C6874607903270CD
Dec		444F92BF78E77BB1	AEBE2D5C8BF747A9
7			
In	D532789E4E79D81E 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
XorT	D532789E4E79D819 39EBC1A1A53FF55B	444F92BF78E77BB1	AEBE2D5C8BF747A9
Dec		0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
6			
O			
In	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
	39EBC1A1A53FF55B 6F85BFBDB7E880E3	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	
	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A		AEBE2D5C8BF747A9
XorT	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9
XorT Dec	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9
XorT Dec	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9
XorT Dec 5 In	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9
XorT Dec 5 In	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154 F1D28EA6295891E8	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9
XorT Dec 5 In XorT	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9
XorT Dec 5 In XorT	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154 F1D28EA6295891E8	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 F60E0CDB7F429FE8
XorT Dec  5 In XorT Dec  4 In	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154 F1D28EA6295891E8 6CA405593A3B5154	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 F60E0CDB7F429FE8 F60E0CDB7F429FE8
XorT Dec  5 In XorT Dec  4 In	39EBC1A1A53FF55B 6F85BFBDB7E880E3 39EBC1A1A53FF55B BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24A 6CA405593A3B5154 BF213BFD04E8A24F 6CA405593A3B5154 F1D28EA6295891E8 6CA405593A3B5154 F1D28EA6295891E8 6CA405593A3B5154 F1D28EA6295891E8 6CA405593A3B5154 F1D28EA6295891E7 6CA405593A3B5154	0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31 0CC86A4D9B9C6A31	AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 AEBE2D5C8BF747A9 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8

```
3
    9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
In
     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
    794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
In
    0001020304050607
XorT 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
    0001020304050607
Dec A6A6A6A6A6A6A6A 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	A/R3	R1/R4	R2
1				
In	A6A6A6 <i>A</i>	A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
_		0304050607	08090A0B0C0D0E0F	
Enc		0454E3FDE1	F661BD9F31FBFA31 08090A0B0C0D0E0F	8899AABBCCDDEEFF
XorT		0454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020	0304050607	08090A0B0C0D0E0F	
2				
2 In	794314T	0454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
		0304050607	08090A0B0C0D0E0F	
Enc		5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8
		0304050607	08090A0B0C0D0E0F	TC0T0GDDFT100TT0
Xor'l'		5C5BBCB563 0304050607	F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8
	0001020	3301030007	00070710200020201101	
3				
In		5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
Enc		0304050607 405FBC00C1	08090A0B0C0D0E0F F661BD9F31FBFA31	F60E0CDB7F429FE8
EIIC		593A3B5154	08090A0B0C0D0E0F	FOOEOCDB/F4ZJFEO
XorT		405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA4055	593A3B5154	08090A0B0C0D0E0F	
4				
In	9DF8F54	405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA4055	593A3B5154	08090A0B0C0D0E0F	
Enc		FDD0DD2EA4	F661BD9F31FBFA31	F60E0CDB7F429FE8
XorT		593A3B5154 FDD0DD2EA0	E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8
XOLI		593A3B5154	E5923CB9FDB56FBC	FOOEOCDB/F4ZJFEO
5	564400		-6610-2121	-60-00-0-0-0-0
In		FDD0DD2EA0 593A3B5154	F661BD9F31FBFA31 E5923CB9FDB56FBC	F60E0CDB7F429FE8
Enc		DD3146AFBB	E7D1194D853E53F8	F60E0CDB7F429FE8
		593A3B5154	E5923CB9FDB56FBC	
XorT		DD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8
	6CA4055	593A3B5154	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
V III	C365B66943E2D760	E5923CB9FDB56FBC	HED 40D 3 20 40 4 F F 7 C
XorT	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	E5923CB9FDB56FBC	
8			
In	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576
T11	C365B66943E2D760	E5923CB9FDB56FBC	EFD40BA304943370
Enc	C58B9D3AC6D5B94E	E7D1194D853E53F8	EFD48BA304945576
BIIC	C365B66943E2D760	73E3B6CBE5D05D74	EFD 10DA30 17 13370
XorT	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
11011	C365B66943E2D760	73E3B6CBE5D05D74	E1 D 10 D113 0 19 13 3 7 0
	000000000000000000000000000000000000000	, 5252 5 622 5 2 5 2 7 1	
9			
9 In	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
	C58B9D3AC6D5B946 C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
			EFD48BA304945576 EFD48BA304945576
In	C365B66943E2D760	73E3B6CBE5D05D74	
In	C365B66943E2D760 1A681354E84C41F8	73E3B6CBE5D05D74 D6AE29ECE7192D43	
In Enc	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
In Enc	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576
In Enc	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576
In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576
In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576
In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576 EFD48BA304945576
In Enc XorT  10 In Enc	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA
In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576
In Enc XorT  10 In Enc	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760  DBA417FB51F9E3C1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760  DBA417FB51F9E3C1 C365B66943E2D760	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760  DBA417FB51F9E3C1 C365B66943E2D760 0629EB29A42E4FD9	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760  DBA417FB51F9E3C1 C365B66943E2D760 0629EB29A42E4FD9 F56701DAF0388216	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA
In Enc XorT  10 In Enc XorT	C365B66943E2D760 1A681354E84C41F8 C365B66943E2D760 1A681354E84C41F1 C365B66943E2D760  1A681354E84C41F1 C365B66943E2D760 DBA417FB51F9E3CB C365B66943E2D760 DBA417FB51F9E3C1 C365B66943E2D760  DBA417FB51F9E3C1 C365B66943E2D760 0629EB29A42E4FD9	73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74 D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576 EFD48BA304945576 EFD48BA304945576 FBEC169FA5C0F6BA FBEC169FA5C0F6BA FBEC169FA5C0F6BA

12			
In	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
Enc	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
XorT	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
1.2			
13 In	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
111	F56701DAF0388216	3CF149E90E8C04D9	F BECTO F AJCOF OBA
Enc	2E8E2B6BB2016696	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
XorT	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
14	000000000000000000000000000000000000000	4545056752225015	EDEG1 (0E3 EG0ECD3
In	2E8E2B6BB201669B F56701DAF0388216	4745856AF333F01F 3CF149E90E8C04D9	FBEC169FA5C0F6BA
Enc	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B
шис	F56701DAF0388216	3CF149E90E8C04D9	Deniiobbi /Delioob
XorT	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
15			
15 In	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
In	F56701DAF0388216	3CF149E90E8C04D9	
	F56701DAF0388216 33FE29365885C4B7	3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B
In	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F	
In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B
In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B
In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B
In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT 16 In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT 16 In	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT 16 In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT 16 In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT  16 In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT  16 In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT  16 In Enc XorT	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT  16 In Enc XorT  17 In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9  5075496800978B5A C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In Enc XorT  16 In Enc XorT  17 In Enc	F56701DAF0388216 33FE29365885C4B7 C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9  5075496800978B5A C272E9466AAE98F9 A5382A26B47551F1	3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 1BB8C765A84195E7	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B

18			
In	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Enc	F19D80D437EFE8F9	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
YorT	C272E9466AAE98F9 F19D80D437EFE8EB	1BB8C765A84195E7	F7FDAD518C960D36
MOLI	C272E9466AAE98F9	40F68C91DB49702C	F /EDADJ10CJ00D30
19			
In	F19D80D437EFE8EB C272E9466AAE98F9	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
Enc	B422B444B87A190B	1BB8C765A84195E7	F7FDAD518C960D36
EIIC	1CFBF6B4C24CB982	40F68C91DB49702C	r /EDADJIOCJOODJO
XorT	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
0.0			
20 In	B422B444B87A1918	1pp9C765x94195F7	F7EDAD518C960D36
111	1CFBF6B4C24CB982	40F68C91DB49702C	r /EDAD310C900D30
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	
			F7EDAD518C960D36 F7EDAD518C960D36
	1CFBF6B4C24CB982 C89A96CA7B163ED9	07DFE775B9687E73 CBCCB35CFB87F826	
XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36
XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	
XorT 22 In	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36 F7EDAD518C960D36
XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	F7EDAD518C960D36
XorT  22 In Enc	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	F7EDAD518C960D36 F7EDAD518C960D36
XorT  22 In Enc	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326
XorT  22 In  Enc  XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326
XorT  22 In Enc	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326
XorT  22 In Enc XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326 3F5786E2D80ED326
XorT  22 In Enc XorT	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326 3F5786E2D80ED326
XorT  22 In Enc XorT  23 In Enc	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982 CABBEACESSESSESSESSESSESSESSESSESSESSESSESSESS	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326 3F5786E2D80ED326 3F5786E2D80ED326
XorT  22 In Enc XorT  23 In Enc	1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 C89A96CA7B163ED9 1CFBF6B4C24CB982 39D02FE7435870ED 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982 39D02FE7435870FB 1CFBF6B4C24CB982 CFBF6B4C24CB982 0AEB82AE3146A91B CBC7F0E71A99F43B 0AEB82AE3146A90C	07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73  CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73 CBCCB35CFB87F826 07DFE775B9687E73	F7EDAD518C960D36 F7EDAD518C960D36 3F5786E2D80ED326 3F5786E2D80ED326

```
24
     0AEB82AE3146A90C CBCCB35CFB87F826 3F5786E2D80ED326
In
    CBC7F0E71A99F43B 07DFE775B9687E73
Enc 28C9F404C4B810EC CBCCB35CFB87F826 3F5786E2D80ED326
     CBC7F0E71A99F43B FB988B9B7A02DD21
XorT 28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
    CBC7F0E71A99F43B FB988B9B7A02DD21
Ciphertext 28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
           CBC7F0E71A99F43B FB988B9B7A02DD21
Unwrap:
                          R1/R4
Step t A/R3
                                   R2
24
    28C9F404C4B810F4 CBCCB35CFB87F826 3F5786E2D80ED326
In
    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
    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 1CFBF6B4C24CB982	1BB8C765A84195E7 07DFE775B9687E73	F7EDAD518C960D36
XorT	D058823360F88A37 1CFBF6B4C24CB982	1BB8C765A84195E7 07DFE775B9687E73	F7EDAD518C960D36
Dec	B422B444B87A1918 1CFBF6B4C24CB982	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
19			
In	B422B444B87A1918 1CFBF6B4C24CB982	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
XorT	B422B444B87A190B 1CFBF6B4C24CB982	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
Dec	F19D80D437EFE8EB C272E9466AAE98F9	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
18			
In	F19D80D437EFE8EB C272E9466AAE98F9	1BB8C765A84195E7 40F68C91DB49702C	F7EDAD518C960D36
XorT	F19D80D437EFE8F9	1BB8C765A84195E7	F7EDAD518C960D36
Dec	C272E9466AAE98F9 A5382A26B47551E0	40F68C91DB49702C 1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
17			
17 In	A5382A26B47551E0 C272E9466AAE98E9	1BB8C765A84195E7 40F68C91DB49702C	BCA418BBF7DCE60B
	C272E9466AAE98F9 A5382A26B47551F1	40F68C91DB49702C 1BB8C765A84195E7	BCA418BBF7DCE60B BCA418BBF7DCE60B
In	C272E9466AAE98F9	40F68C91DB49702C	
In XorT	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C	BCA418BBF7DCE60B
In XorT Dec	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B
In XorT Dec	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B4A	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec 16 In	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec 16 In XorT	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec 16 In XorT	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 33FE29365885C4B8	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec 16 In XorT Dec	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec  16 In XorT Dec	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9  5075496800978B5A C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9  33FE29365885C4B8 C272E9466AAE98F9 33FE29365885C4B8	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F 3CF149E90E8C04D9 4745856AF333F01F	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B
In XorT Dec 16 In XorT Dec 15 In	C272E9466AAE98F9 A5382A26B47551F1 C272E9466AAE98F9 5075496800978B5A C272E9466AAE98F9  5075496800978B5A C272E9466AAE98F9 5075496800978B4A C272E9466AAE98F9 33FE29365885C4B8 C272E9466AAE98F9	40F68C91DB49702C 1BB8C765A84195E7 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 40F68C91DB49702C 4745856AF333F01F 3CF149E90E8C04D9	BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B BCA418BBF7DCE60B

1 4			
14 In	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
111	F56701DAF0388216	3CF149E90E8C04D9	DCA410DDF/DCE00D
XorT	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B
21011	F56701DAF0388216	3CF149E90E8C04D9	Deniiobbi /Delioob
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
111	F56701DAF0388216	3CF149E90E8C04D9	r becion ascoroba
XorT	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Dec	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
11			
In	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
XorT	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	EE 6701DAE020016	73E3B6CBE5D05D74	
Dec	F56701DAF0388216 DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
Dec	C365B66943E2D760	73E3B6CBE5D05D74	F BECTO F AJCOF OBA
	C303D00713D2D700	7313000013003071	
10			
In	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
XorT	DBA417FB51F9E3CB	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
Dec	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
0			
9	1760125450464151	DC10000000100040	HHD 40D3 20 40 4555
In	C365B66943E2D760	D6AE29ECE7192D43 73E3B6CBE5D05D74	EFD48BA304945576
Υονπ	1A681354E84C41F8		EFD48BA304945576
VOLI	C365B66943E2D760	73E3B6CBE5D05D74	EFDTODAJUT7133/0
Dec	C58B9D3AC6D5B946		EFD48BA304945576
	C365B66943E2D760		

8			
In	C58B9D3AC6D5B946 C365B66943E2D760	E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
XorT		E7D1194D853E53F8 73E3B6CBE5D05D74	EFD48BA304945576
Dec	66D7A8ADD086B9DA C365B66943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
7			
In	66D7A8ADD086B9DA C365B66943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
XorT	66D7A8ADD086B9DD C365B66943E2D760	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Dec	963AAFFD96B223EA 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
6			
In	963AAFFD96B223EA 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
XorT	963AAFFD96B223EC 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	EFD48BA304945576
Dec	4EF02EDD3146AFBE 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
5			
5 In	4EF02EDD3146AFBE 6CA405593A3B5154	E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
	6CA405593A3B5154 4EF02EDD3146AFBB	E5923CB9FDB56FBC E7D1194D853E53F8	F60E0CDB7F429FE8
In	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31	
In XorT	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC	F60E0CDB7F429FE8
In XorT	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8
In XorT Dec	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA0	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8
In XorT Dec	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec 4 In XorT	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec 4 In	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154  564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec 4 In XorT Dec	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154  564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154 9DF8F5405FBC00C2	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec 4 In XorT	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154 9DF8F5405FBC00C2 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec  4 In XorT Dec  3 In	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154  564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154 9DF8F5405FBC00C2 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec  4 In XorT Dec	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154  564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154 9DF8F5405FBC00C2 6CA405593A3B5154  9DF8F5405FBC00C2 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 08090A0B0C0D0E0F F661BD9F31FBFA31	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8
In XorT Dec  4 In XorT Dec  3 In	6CA405593A3B5154 4EF02EDD3146AFBB 6CA405593A3B5154 564408FDD0DD2EA0 6CA405593A3B5154  564408FDD0DD2EA0 6CA405593A3B5154 564408FDD0DD2EA4 6CA405593A3B5154 9DF8F5405FBC00C2 6CA405593A3B5154	E5923CB9FDB56FBC E7D1194D853E53F8 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 E5923CB9FDB56FBC F661BD9F31FBFA31 08090A0B0C0D0E0F	F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8 F60E0CDB7F429FE8

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

1 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

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.