16 November 2001

AES Key Wrap Specification

1 Introduction

This specification is intended to satisfy the 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 a plaintext key(s) with any associated integrity information and data, such that the combination could be longer than the width of the AES blocksize (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 a 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 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.) It is recognized that $n \le 4$ will accommodate 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 $n > 4$. 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 will be described generically; i.e. no key size will be specified for the KEK.

2.1 Notation and Definitions

The following notation will be used in the description of the key wrapping algorithms.

Table 1: Notation and Functions

$\mathbf{AES}_\mathbf{K}(W)$	Encrypt *W* using the AES codebook with key *K*
$\mathbf{AES}_\mathbf{K}^{-1}(W)$	Decrypt *W* using the AES codebook with key *K*
$\mathbf{MSB}_j(W)$	Return the most significant *j* bits of *W*
$\mathbf{LSB}_j(W)$	Return the least significant *j* bits of *W*
$B_1 \oplus B_2$	The bitwise exclusive or (XOR) of B_1 and B_2
$B_1 \mid B_2$	Concatenate B_1 and B_2
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 i^{th} plaintext key data block
C_i	The i^{th} ciphertext data block
A	The 64-bit integrity check register
R_i	An array of 64-bit registers where $i = 0, 1, 2, 3, \ldots, n$.
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.

The operation of several of the functions from Table 1 is shown below. Given the binary values:

$$B_1 = 11010100$$
$$B_2 = 100101101$$

The concatenation of B_1 and B_2 is:

$$B_1 \mid B_2 = 11010100100101101$$

To extract portions of B_1:

$$\mathbf{MSB_4}(B_1) = 1101$$
$$\mathbf{LSB_3}(B_1) = 100$$

While these functions describe a general class of extraction functions only the case $j = 64$ will be used in this document.

In the key wrap, 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 as shown in Section 2.2.

2.2 Algorithms

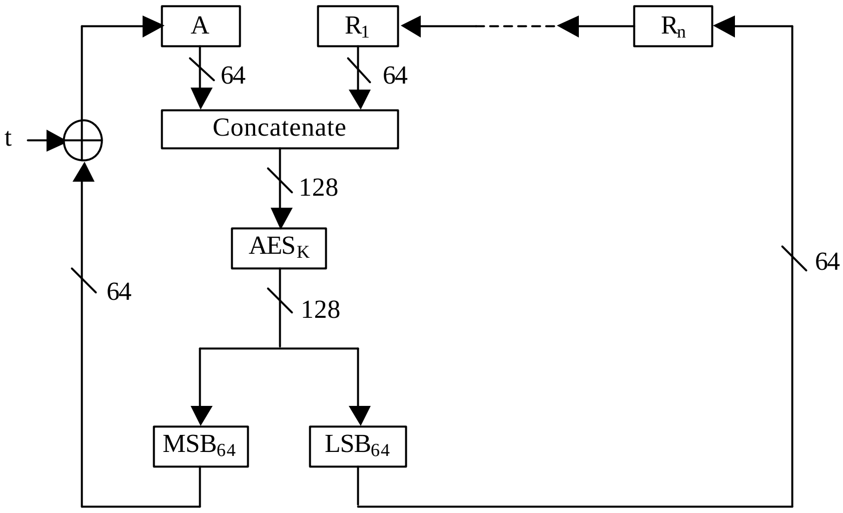
The specification of the key wrap algorithm requires the use of the AES codebook (see reference [1]). The next three sections will describe the key wrap algorithm, the key unwrap algorithm, and the inherent data integrity check.

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 $\{P_1, P_2, \ldots, P_n\}$,
                Key, $K$ (the KEK).
        Outputs: Ciphertext, (n+1) 64-bit values $\{C_0, C_1, \ldots, C_n\}$.
1) Initialize variables
   Set $A^0 = IV$, an initial value (see 2.2.3)
   For $i = 1, \ldots, n$
       $R_i^0 = P_i$
2) Calculate intermediate values
   For $t = 1, \ldots, s$, where $s = 6n$
       $A^t = \mathbf{MSB_{64}}\left(\mathbf{AES_K}\left(A^{t-1} \mid R_1^{t-1}\right)\right) \oplus t$
       For $i = 1, \ldots, n-1$
               $R_i^t = R_{i+1}^{t-1}$
       $R_n^t = \mathbf{LSB_{64}}\left(\mathbf{AES_K}\left(A^{t-1} \mid R_1^{t-1}\right)\right)$
3) Output the results
   Set $C_0 = A^t$
   For $i = 1, \ldots, n$
       $C_i = R_i^t$
```

The motion of the key wrap is shown below.



An alternative description of the key wrap involves indexing rather than shifting. This approach allows you 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. This is the method used to generate the test vectors in Section 4.

```
        Inputs: Plaintext, n 64-bit values $\{P_1, P_2, \ldots, P_n\}$
                Key, $K$ (the KEK).
        Outputs: Ciphertext, (n+1) 64-bit values $\{C_0, C_1, \ldots, C_n\}$
1) Initialize variables
    Set $A = IV$, an initial value(see 2.2.3)
    For $i = 1, \ldots, n$
        $R_i = P_i$
2) Calculate intermediate values
    For $j = 0, 1, \ldots, 5$
        For $i = 1, 2, \ldots, n$
            $B = \mathbf{AES}_{\mathbf{K}}\left(A \mid R_i\right)$
            $A = \mathbf{MSB}_{\mathbf{64}}(B) \oplus t$ where $t = (n \cdot j) + i$
            $R_i = \mathbf{LSB}_{64}(B)$
3) Output the results
    Set $C_0 = A$
    For $i = 1, \ldots, n$
        $C_i = R_i$
```

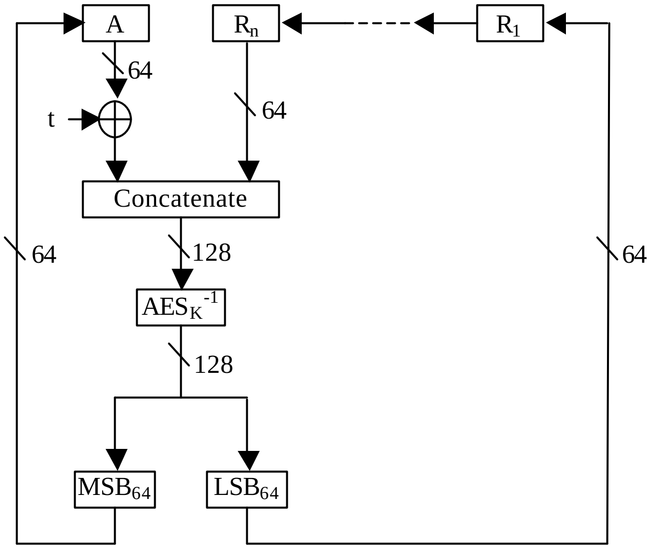
2.2.2 Key Unwrap

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 $\{C_0, C_1, \ldots, C_n\}$,
                Key, $K$ (the KEK)
        Outputs: Plaintext n 64-bit values $\{P_1, P_2, \ldots, P_n\}$
1) Initialize variables
    Set $A^s = C_0$ where $s = 6n$
    For $i = 1, \ldots, n$
        $R_i^s = C_i$
2) Calculate the intermediate values
    For $t = s, \ldots, 1$
        $A^{t-1} = \mathbf{MSB}_{64}\left(\mathbf{AES}_{\mathbf{K}}^{-1}\left(\left(A^t \oplus t\right) \mid R_n^t\right)\right)$
        $R_1^{t-1} = \mathbf{LSB}_{64}\left(\mathbf{AES}_{\mathbf{K}}^{\mathbf{-1}}\left(\left(A^t \oplus t\right) \mid R_n^t\right)\right)$
        For $i = 2, \ldots, n$
            $R_i^{t-1} = R_{i-1}^t$
```

```
3) Output the results
   If $A_0$ is an appropriate initial value (see 2.2.3),
   Then
       For $i = 1, \ldots, n$
               $P_i = R_i^0$
   Else
       Return an error
```

The motion of the AES key unwrap is shown below.



The unwrap 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 $\{C_0, C_1, \ldots, C_n\}$,
            Key, $K$ (the KEK)
    Outputs: Plaintext n 64-bit values $\{P_1, P_2, \ldots, P_n\}$
1) Initialize variables
   Set $A = C_0$
   For $i = 1, \ldots, n$
       $R_i = C_i$
2) Compute intermediate values
   For $j = 5, \ldots, 0$
       For $i = n, n-1, \ldots, 1$
               $B = \mathbf{AES}_{\mathbf{K}}^{-1}((A \oplus t) \mid R_i)$, where $t = (n \cdot j) + i$
               $A = \mathbf{MSB}_{\mathbf{64}}(B)$
               $R_i = \mathbf{LSB}_{\mathbf{64}}(B)$
```

```
3)  Output results
    If $A$ is an appropriate initial value (see 2.2.3),
    Then
        For $i = 1, \cdots, n$
                $P_i = R_i$
    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 it is returned by the unwrapping algorithm. If there is not a match, then the key is not accepted as valid, 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), if called for in other NIST publications on key management.

2.2.3.1 Default Initial Value

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

$$A_0 = IV = \text{A6A6A6A6A6A6A6A6}.$$

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 $A_0 = \text{A6A6A6A6A6A6A6A6}$, then the chance that the key data is corrupt is 2^{-64}. If unwrapping produces $A_0 \neq \text{A6A6A6A6A6A6A6A6}$, 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 References

[1] J. Daemon and V. Rijmen, *AES Proposal: Rijndael,* AES Algorithm Submission, September 3, 1999.

[2] Federal Information Processing Standards (FIPS) Publication XXX-X, *Advanced Encryption Standard (AES)* (DRAFT), U. S. DoC/NIST.

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 made the implementation of this algorithm in software a straightforward matter. In each example, the registers that are unaffected during a step have been shaded.

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

Input:

KEK:	000102030405060708090A0B0C0D0E0F
Key Data:	00112233445566778899AABBCCDDEEFF

Wrap:

Step t		A	R_1	R_2
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	AES encrypt	F4740052E82A2251	74CE86FBD7B805E7	8899AABBCCDDEEFF
	Add t	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
2	Input	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
	AES encrypt	06BA4EBDE7768D0B	74CE86FBD7B805E7	D132EE38147E76F8
	Add t	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
3	Input	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
	AES encrypt	FC967627BE937208	FE6E8D679C5D3460	D132EE38147E76F8
	Add t	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
4	Input	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
	AES encrypt	5896EA9028EE203B	FE6E8D679C5D3460	07B2BD973E36A6FC
	Add t	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
5	Input	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
	AES encrypt	93AEA71B258D90C3	25F5A3ADC2195401	07B2BD973E36A6FC
	Add t	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
6	Input	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
	AES encrypt	E3EE986344D878F7	25F5A3ADC2195401	F14863BB1E9CA90A
	Add t	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
7	Input	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
	AES encrypt	2BFC21B2C20E4006	B556D35ED8CEF052	F14863BB1E9CA90A
	Add t	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
8	Input	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
	AES encrypt	4BE8CE99C0A43A7D	B556D35ED8CEF052	64BAE5818D0570BB
	Add t	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
9	Input	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
	AES encrypt	EBE1CE91067024F3	BE114B343EB00981	64BAE5818D0570BB
	Add t	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
10	Input	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
	AES encrypt	5A9C7B1F5B1C3B46	BE114B343EB00981	4FD3D2B7D74FBB42
	Add t	5A9C7B1F5B1C3B4C	BE114B343EB00981	4FD3D2B7D74FBB42
11	Input	5A9C7B1F5B1C3B4C	BE114B343EB00981	4FD3D2B7D74FBB42
	AES encrypt	93B71967EED41FFC	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
	Add t	93B71967EED41FF7	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
12	Input	93B71967EED41FF7	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
	AES encrypt	1FA68B0A8112B44B	AEF34BD8FB5A7B82	9D3E862371D2CFE5
	Add t	1FA68B0A8112B447	AEF34BD8FB5A7B82	9D3E862371D2CFE5
	Ciphertext	1FA68B0A8112B447	AEF34BD8FB5A7B82	9D3E862371D2CFE5

Unwrap:

Step t		A	R_1	R_2
12	Input	1FA68B0A8112B447	AEF34BD8FB5A7B82	9D3E862371D2CFE5
	Add t	1FA68B0A8112B44B	AEF34BD8FB5A7B82	9D3E862371D2CFE5
	AES decrypt	93B71967EED41FF7	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
11	Input	93B71967EED41FF7	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
	Add t	93B71967EED41FFC	AEF34BD8FB5A7B82	4FD3D2B7D74FBB42
	AES decrypt	5A9C7B1F5B1C3B4C	BE114B343EB00981	4FD3D2B7D74FBB42
10	Input	5A9C7B1F5B1C3B4C	BE114B343EB00981	4FD3D2B7D74FBB42
	Add t	5A9C7B1F5B1C3B46	BE114B343EB00981	4FD3D2B7D74FBB42
	AES decrypt	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
9	Input	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
	Add t	EBE1CE91067024F3	BE114B343EB00981	64BAE5818D0570BB
	AES decrypt	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
8	Input	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
	Add t	4BE8CE99C0A43A7D	B556D35ED8CEF052	64BAE5818D0570BB
	AES decrypt	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
7	Input	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
	Add t	2BFC21B2C20E4006	B556D35ED8CEF052	F14863BB1E9CA90A
	AES decrypt	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
6	Input	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
	Add t	E3EE986344D878F7	25F5A3ADC2195401	F14863BB1E9CA90A
	AES decrypt	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
5	Input	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
	Add t	93AEA71B258D90C3	25F5A3ADC2195401	07B2BD973E36A6FC
	AES decrypt	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
4	Input	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
	Add t	5896EA9028EE203B	FE6E8D679C5D3460	07B2BD973E36A6FC
	AES decrypt	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
3	Input	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
	Add t	FC967627BE937208	FE6E8D679C5D3460	D132EE38147E76F8
	AES decrypt	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
2	Input	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
	Add t	06BA4EBDE7768D0B	74CE86FBD7B805E7	D132EE38147E76F8
	AES decrypt	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
1	Input	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
	Add t	F4740052E82A2251	74CE86FBD7B805E7	8899AABBCCDDEEFF
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

4.2 Wrap 128 bits of Key Data with a 192-bit KEK

Input:

KEK:	000102030405060708090A0B0C0D0E0F1011121314151617
Key Data:	00112233445566778899AABBCCDDEEFF

Wrap:

Step t		A	R_1	R_2
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	AES encrypt	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF
	Add t	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
2	Input	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
	AES encrypt	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D
	Add t	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
3	Input	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
	AES encrypt	7B8E343CA51CF8AB	BC164F51E20CC983	51F22F3286758A2D
	Add t	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
4	Input	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
	AES encrypt	02A97C5897140595	BC164F51E20CC983	05FC2D8F8FF4B919
	Add t	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
5	Input	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
	AES encrypt	15D4B63F66583817	429487269D3A0016	05FC2D8F8FF4B919
	Add t	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
6	Input	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
	AES encrypt	AE2D0B76A6951EEA	429487269D3A0016	05A2D8FB4DD5BD7A
	Add t	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
7	Input	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
	AES encrypt	79F849444F4B8AA8	D40B091CDBAC0340	05A2D8FB4DD5BD7A
	Add t	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
8	Input	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
	AES encrypt	5933A9195B5F5E21	D40B091CDBAC0340	89F0D6C06F8CA9B4
	Add t	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
9	Input	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
	AES encrypt	57ADA800299C2E85	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
	Add t	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
10	Input	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
	AES encrypt	BF17BD6A9BC80163	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
	Add t	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
11	Input	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
	AES encrypt	B68BF270AE81544F	F92B5B97C050AED2	EB24CCFA52EA9078
	Add t	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
12	Input	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
	AES encrypt	96778B25AE6CA439	F92B5B97C050AED2	468AB8A17AD84E5D
	Add t	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D
	Ciphertext	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D

Unwrap:

Step t		A	R_1	R_2
12	Input	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D
	Add t	96778B25AE6CA439	F92B5B97C050AED2	468AB8A17AD84E5D
	AES decrypt	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
11	Input	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
	Add t	B68BF270AE81544F	F92B5B97C050AED2	EB24CCFA52EA9078
	AES decrypt	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
10	Input	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
	Add t	BF17BD6A9BC80163	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
	AES decrypt	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
9	Input	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
	Add t	57ADA800299C2E85	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
	AES decrypt	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
8	Input	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
	Add t	5933A9195B5F5E21	D40B091CDBAC0340	89F0D6C06F8CA9B4
	AES decrypt	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
7	Input	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
	Add t	79F849444F4B8AA8	D40B091CDBAC0340	05A2D8FB4DD5BD7A
	AES decrypt	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
6	Input	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
	Add t	AE2D0B76A6951EEA	429487269D3A0016	05A2D8FB4DD5BD7A
	AES decrypt	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
5	Input	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
	Add t	15D4B63F66583817	429487269D3A0016	05FC2D8F8FF4B919
	AES decrypt	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
4	Input	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
	Add t	02A97C5897140595	BC164F51E20CC983	05FC2D8F8FF4B919
	AES decrypt	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
3	Input	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
	Add t	7B8E343CA51CF8AB	BC164F51E20CC983	51F22F3286758A2D
	AES decrypt	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
2	Input	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
	Add t	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D
	AES decrypt	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
1	Input	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
	Add t	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

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

Input:

KEK:	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Key Data:	00112233445566778899AABBCCDDEEFF

Wrap:

Step t		A	R1	R_2
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	AES encrypt	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF
	Add t	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
2	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	AES encrypt	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8
	Add t	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
3	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
	AES encrypt	85DBDF1879D5C0A5	5602001BFA07AD8B	F60E0CDB7F429FE8
	Add t	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
4	Input	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
	AES encrypt	738C291128B7226D	5602001BFA07AD8B	58924F777C3F678C
	Add t	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
5	Input	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
	AES encrypt	2656A02DFFF054DC	F4DF378183E3D5B2	58924F777C3F678C
	Add t	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
6	Input	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
	AES encrypt	DDFD0C0E8B52A63A	F4DF378183E3D5B2	91AC1D36A964F41B
	Add t	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
7	Input	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
	AES encrypt	39AB00D4AE4399EA	5271D5CED80F34ED	91AC1D36A964F41B
	Add t	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
8	Input	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
	AES encrypt	4CE414878463EAAC	5271D5CED80F34ED	67D8ED899E7929B8
	Add t	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
9	Input	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
	AES encrypt	FBB44DB106AA0789	0DF7E50829123648	67D8ED899E7929B8
	Add t	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
10	Input	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
	AES encrypt	877112A7308ADCC5	0DF7E50829123648	3472D5993D318FD2
	Add t	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
11	Input	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
	AES encrypt	78E40190807CC151	63E9777905818A2A	3472D5993D318FD2
	Add t	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
12	Input	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
	AES encrypt	64E8C3F9CE0F5BAE	63E9777905818A2A	93C8191E7D6E8AE7
	Add t	64E8C3F9CE0F5BA2	63E9777905818A2A	93C8191E7D6E8AE7
	Ciphertext	64E8C3F9CE0F5BA2	63E9777905818A2A	93C8191E7D6E8AE7

Unwrap:

Step t		A	R1	R_2
12	Input	64E8C3F9CE0F5BA2	63E9777905818A2A	93C8191E7D6E8AE7
	Add t	64E8C3F9CE0F5BAE	63E9777905818A2A	93C8191E7D6E8AE7
	AES decrypt	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
11	Input	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
	Add t	78E40190807CC151	63E9777905818A2A	3472D5993D318FD2
	AES decrypt	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
10	Input	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
	Add t	877112A7308ADCC5	0DF7E50829123648	3472D5993D318FD2
	AES decrypt	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
9	Input	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
	Add t	FBB44DB106AA0789	0DF7E50829123648	67D8ED899E7929B8
	AES decrypt	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
8	Input	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
	Add t	4CE414878463EAAC	5271D5CED80F34ED	67D8ED899E7929B8
	AES decrypt	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
7	Input	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
	Add t	39AB00D4AE4399EA	5271D5CED80F34ED	91AC1D36A964F41B
	AES decrypt	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
6	Input	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
	Add t	DDFD0C0E8B52A63A	F4DF378183E3D5B2	91AC1D36A964F41B
	AES decrypt	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
5	Input	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
	Add t	2656A02DFFF054DC	F4DF378183E3D5B2	58924F777C3F678C
	AES decrypt	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
4	Input	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
	Add t	738C291128B7226D	5602001BFA07AD8B	58924F777C3F678C
	AES decrypt	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
3	Input	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
	Add t	85DBDF1879D5C0A5	5602001BFA07AD8B	F60E0CDB7F429FE8
	AES decrypt	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
2	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
	Add t	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8
	AES decrypt	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
1	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	Add t	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

4.4 Wrap 192 bits of Key Data with a 192-bit KEK

Input:

KEK:	000102030405060708090A0B0C0D0E0F1011121314151617
Key Data:	00112233445566778899AABBCCDDEEFF0001020304050607

Wrap:

Step t		A	R_1	R_2	R_3
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
	AES encrypt	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
	Add t	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
2	Input	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
	AES encrypt	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D	0001020304050607
	Add t	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
3	Input	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
	AES encrypt	2C8E19A519025B7C	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
	Add t	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
4	Input	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
	AES encrypt	E727C7BDF822602E	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
	Add t	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
5	Input	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
	AES encrypt	15B61F7B25D51700	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
	Add t	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
6	Input	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
	AES encrypt	A187755AEA64719C	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
	Add t	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
7	Input	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
	AES encrypt	5A994895D81644B7	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
	Add t	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
8	Input	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
	AES encrypt	864F408C8AB8CDCF	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
	Add t	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
9	Input	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
	AES encrypt	53F4373F575EB7A4	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
	Add t	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
10	Input	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
	AES encrypt	9EAA4CDA0B1BA5FF	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
	Add t	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
11	Input	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
	AES encrypt	B1B9902C68E0EB52	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
	Add t	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
12	Input	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
	AES encrypt	FCE591D77709A6E0	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
	Add t	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
13	Input	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5

Step t		A	R_1	R_2	R_3
	AES encrypt	428428D2BD88CF58	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
	Add t	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
14	Input	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
	AES encrypt	6AC861AB961DA578	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
	Add t	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
15	Input	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
	AES encrypt	E80DB49CC9A1EA61	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
	Add t	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
16	Input	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
	AES encrypt	ABEE3534AC465C2C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
	Add t	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
17	Input	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
	AES encrypt	E7CC8D8CEDE62BF7	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
	Add t	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
18	Input	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
	AES encrypt	031D33264E15D320	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
	Add t	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
	Ciphertext	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2

Unwrap:

Step t		A	R1	R_2	R_3
18	Input	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
	Add t	031D33264E15D320	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
	AES decrypt	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
17	Input	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
	Add t	E7CC8D8CEDE62BF7	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
	AES decrypt	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
16	Input	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
	Add t	ABEE3534AC465C2C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
	AES decrypt	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
15	Input	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
	Add t	E80DB49CC9A1EA61	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
	AES decrypt	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
14	Input	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
	Add t	6AC861AB961DA578	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
	AES decrypt	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
13	Input	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
	Add t	428428D2BD88CF58	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
	AES decrypt	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
12	Input	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
	Add t	FCE591D77709A6E0	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
	AES decrypt	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
11	Input	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
	Add t	B1B9902C68E0EB52	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
	AES decrypt	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295

Step t		A	R1	R_2	R_3
10	Input	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
	Add t	9EAA4CDA0B1BA5FF	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
	AES decrypt	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
9	Input	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
	Add t	53F4373F575EB7A4	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
	AES decrypt	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
8	Input	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
	Add t	864F408C8AB8CDCF	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
	AES decrypt	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
7	Input	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
	Add t	5A994895D81644B7	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
	AES decrypt	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
6	Input	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
	Add t	A187755AEA64719C	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
	AES decrypt	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
5	Input	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
	Add t	15B61F7B25D51700	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
	AES decrypt	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
4	Input	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
	Add t	E727C7BDF822602E	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
	AES decrypt	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
3	Input	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
	Add t	2C8E19A519025B7C	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
	AES decrypt	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
2	Input	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
	Add t	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D	0001020304050607
	AES decrypt	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
1	Input	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
	Add t	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607

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

Input:

KEK:	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Key Data:	00112233445566778899AABBCCDDEEFF0001020304050607

Wrap:

Step t		A	R_1	R_2	R_3
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
	AES encrypt	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
	Add t	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
2	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
	AES encrypt	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
	Add t	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
3	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
	AES encrypt	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
	Add t	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
4	Input	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
	AES encrypt	F1D28EA6295891EC	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
	Add t	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
5	Input	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
	AES encrypt	BF213BFD04E8A24F	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
	Add t	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
6	Input	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
	AES encrypt	6F85BFBDB7E880E3	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	Add t	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
7	Input	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	AES encrypt	D532789E4E79D819	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	Add t	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
8	Input	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	AES encrypt	2A5FFCEF1F1916D8	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
	Add t	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
9	Input	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
	AES encrypt	01271BA91D9804F6	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
	Add t	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
10	Input	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
	AES encrypt	A3223BD7237F7033	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
	Add t	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
11	Input	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
	AES encrypt	B50C330616E7B1C7	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
	Add t	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
12	Input	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
	AES encrypt	FB8AFF3F083E12CE	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
	Add t	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
13	Input	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D

Step t		A	R_1	R_2	R_3
	AES encrypt	82F597607784A33C	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
	Add t	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
14	Input	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
	AES encrypt	D48E5E83B7C906DB	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
	Add t	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
15	Input	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
	AES encrypt	1BF2B1CD947311B6	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
	Add t	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
16	Input	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
	AES encrypt	C9F5F26A378011DE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
	Add t	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
17	Input	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
	AES encrypt	39128CE5E435F3A0	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
	Add t	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
18	Input	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
	AES encrypt	A8F9BC1612C68B2D	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
	Add t	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
	Ciphertext	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1

Unwrap:

Step t		A	R_1	R_2	R_3
18	Input	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
	Add t	A8F9BC1612C68B2D	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
	AES decrypt	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
17	Input	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
	Add t	39128CE5E435F3A0	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
	AES decrypt	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
16	Input	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
	Add t	C9F5F26A378011DE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
	AES decrypt	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
15	Input	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
	Add t	1BF2B1CD947311B6	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
	AES decrypt	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
14	Input	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
	Add t	D48E5E83B7C906DB	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
	AES decrypt	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
13	Input	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
	Add t	82F597607784A33C	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
	AES decrypt	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
12	Input	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
	Add t	FB8AFF3F083E12CE	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
	AES decrypt	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
11	Input	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
	Add t	B50C330616E7B1C7	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6

Step t		A	R_1	R_2	R_3
	AES decrypt	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
10	Input	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
	Add t	A3223BD7237F7033	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
	AES decrypt	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
9	Input	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
	Add t	01271BA91D9804F6	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
	AES decrypt	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
8	Input	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
	Add t	2A5FFCEF1F1916D8	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
	AES decrypt	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
7	Input	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	Add t	D532789E4E79D819	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	AES decrypt	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
6	Input	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	Add t	6F85BFBDB7E880E3	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
	AES decrypt	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
5	Input	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
	Add t	BF213BFD04E8A24F	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
	AES decrypt	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
4	Input	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
	Add t	F1D28EA6295891EC	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
	AES decrypt	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
3	Input	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
	Add t	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
	AES decrypt	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
2	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
	Add t	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
	AES decrypt	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
1	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
	Add t	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607

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

Input:

KEK:	000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Key Data:	00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

Wrap:

Step t		A	R_1	R_2	R_3	R_4
1	Input	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	AES encrypt	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	Add t	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
2	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	AES encrypt	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
	Add t	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
3	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
	AES encrypt	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
	Add t	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
4	Input	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
	AES encrypt	564408FDD0DD2EA4	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
5	Input	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	AES encrypt	4EF02EDD3146AFBB	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
6	Input	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	AES encrypt	963AAFFD96B223EC	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
7	Input	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
	AES encrypt	66D7A8ADD086B9DD	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC
	Add t	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC
8	Input	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC
	AES encrypt	C58B9D3AC6D5B94E	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
9	Input	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	AES encrypt	1A681354E84C41F8	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
10	Input	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	AES encrypt	DBA417FB51F9E3CB	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
11	Input	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
	AES encrypt	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
	Add t	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
12	Input	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
	AES encrypt	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	Add t	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
13	Input	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9

Step t		A	R_1	R_2	R_3	R_4
	AES encrypt	2E8E2B6BB2016696	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	Add t	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
14	Input	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	AES encrypt	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
	Add t	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
15	Input	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
	AES encrypt	33FE29365885C4B7	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
	Add t	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
16	Input	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
	AES encrypt	507549680097 8B4A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	Add t	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
17	Input	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	AES encrypt	A5382A26B47551F1	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	Add t	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
18	Input	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	AES encrypt	F19D80D437EFE8F9	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
	Add t	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
19	Input	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
	AES encrypt	B422B444B87A190B	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
	Add t	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
20	Input	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
	AES encrypt	D058823360F88A37	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
21	Input	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	AES encrypt	C89A96CA7B163ECC	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
22	Input	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	AES encrypt	39D02FE7435870ED	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73
23	Input	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73
	AES encrypt	0AEB82AE3146A91B	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
	Add t	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
24	Input	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
	AES encrypt	28C9F404C4B810EC	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	FB988B9B7A02DD21
	Add t	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	FB988B9B7A02DD21
	Ciphertext	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	FB988B9B7A02DD21

Unwrap:

Step t		A	R_1	R_2	R_3	R_4
24	Input	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	FB988B9B7A02DD21
	Add t	28C9F404C4B810EC	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	FB988B9B7A02DD21
	AES decrypt	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
23	Input	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
	Add t	0AEB82AE3146A91B	CBCCB35CFB87F826	3F5786E2D80ED326	CBC7F0E71A99F43B	07DFE775B9687E73
	AES decrypt	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73

22	Input	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	39D02FE7435870ED	CBCCB35CFB87F826	3F5786E2D80ED326	1CFBF6B4C24CB982	07DFE775B9687E73
	AES decrypt	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
21	Input	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	C89A96CA7B163ECC	CBCCB35CFB87F826	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	AES decrypt	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
20	Input	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	Add t	D058823360F88A37	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	07DFE775B9687E73
	AES decrypt	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
19	Input	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
	Add t	B422B444B87A190B	1BB8C765A84195E7	F7EDAD518C960D36	1CFBF6B4C24CB982	40F68C91DB49702C
	AES decrypt	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
18	Input	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
	Add t	F19D80D437EFE8F9	1BB8C765A84195E7	F7EDAD518C960D36	C272E9466AAE98F9	40F68C91DB49702C
	AES decrypt	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
17	Input	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	Add t	A5382A26B47551F1	1BB8C765A84195E7	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	AES decrypt	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
16	Input	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	Add t	5075496800978B4A	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	40F68C91DB49702C
	AES decrypt	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
15	Input	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
	Add t	33FE29365885C4B7	4745856AF333F01F	BCA418BBF7DCE60B	C272E9466AAE98F9	3CF149E90E8C04D9
	AES decrypt	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
14	Input	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
	Add t	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B	F56701DAF0388216	3CF149E90E8C04D9
	AES decrypt	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
13	Input	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	Add t	2E8E2B6BB2016696	4745856AF333F01F	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	AES decrypt	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
12	Input	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	Add t	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	3CF149E90E8C04D9
	AES decrypt	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
11	Input	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
	Add t	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA	F56701DAF0388216	73E3B6CBE5D05D74
	AES decrypt	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
10	Input	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	DBA417FB51F9E3CB	D6AE29ECE7192D43	FBEC169FA5C0F6BA	C365B66943E2D760	73E3B6CBE5D05D74
	AES decrypt	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
9	Input	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	1A681354E84C41F8	D6AE29ECE7192D43	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	AES decrypt	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
8	Input	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	Add t	C58B9D3AC6D5B94E	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	73E3B6CBE5D05D74
	AES decrypt	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC
7	Input	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC

	Add t	66D7A8ADD086B9DD	E7D1194D853E53F8	EFD48BA304945576	C365B66943E2D760	E5923CB9FDB56FBC
	AES decrypt	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
6	Input	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	963AAFFD96B223EC	E7D1194D853E53F8	EFD48BA304945576	6CA405593A3B5154	E5923CB9FDB56FBC
	AES decrypt	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
5	Input	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	4EF02EDD3146AFBB	E7D1194D853E53F8	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	AES decrypt	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
4	Input	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	Add t	564408FDD0DD2EA4	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	E5923CB9FDB56FBC
	AES decrypt	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
3	Input	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
	Add t	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154	08090A0B0C0D0E0F
	AES decrypt	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
2	Input	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
	Add t	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607	08090A0B0C0D0E0F
	AES decrypt	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
1	Input	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	Add t	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	AES decrypt	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F
	Plaintext	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607	08090A0B0C0D0E0F