Groupe de travail Réseau
Request for Comments : 3394
Catégorie : Information
Traduction Claude Brière de L'Isle

J. Schaad, Soaring Hawk Consulting
R. Housley, RSA Laboratories
September 2002

Algorithme d'enveloppe de clés pour la norme de chiffrement évoluée (AES)

Résumé
L'objet de ce document est de mettre à la disposition de la communauté de l'Internet sous une forme pratique l'algorithme d'enveloppe de clés pour la norme de chiffrement évoluée (AES, *Advanced Encryption Standard*). Le gouvernement des États-Unis d'Amérique a adopté AES comme nouvelle norme de chiffrement. L'algorithme d'enveloppe de clés AES sera probablement adopté par les USA pour le chiffrement des clés AES. Les auteurs ont tiré la plus grande partie du texte de ce document du projet Enveloppe de clés AES publié par le NIST.

Table des matières

1. Introduction

Note : La plus grande partie du texte qui suit est tirée de [AES-WRAP], et les assertions concernant la sécurité de l'algorithme AES Key Wrap sont faites par le gouvernement des États-Unis d'Amérique, et non par les auteurs du présent document.

La présente spécification est destinée à satisfaire à l'exigence d'enveloppe de clé de l'Institut national des normes et technologies (NIST, *National Institute of Standards et Technology*) de concevoir un algorithme de chiffrement appelé une enveloppe de clé *(Key Wrap)* qui utilise la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) comme primitive pour chiffrer en toute sécurité une ou plusieurs clés en clair avec des informations et des données d'intégrité associées, de telle façon que leur combinaison puisse être plus longue que la largeur de la taille de bloc AES (128 bits). Chaque bit du texte chiffré devrait être une fonction non linéaire de chaque bit de texte en clair, et (lors du développement) chaque bit de texte en clair devrait être une fonction non linéaire de chaque bit de texte chiffré. Il est suffisant d'approximer une permutation pseudo aléatoire idéale de telle sorte que l'exploitation des phénomènes indésirables soit aussi improbable que de deviner la clé du moteur AES.

Cet algorithme d'enveloppe de clé donne une sécurité suffisante pour protéger les clés dans le contexte d'une architecture de gestion de clés conçue avec prudence.

Tout au long du présent document, toutes les données qui sont enveloppées seront appelées les données de clé *(key data)*. Il ne fait aucune différence pour l'algorithme que les données enveloppées soient ou non une clé ; en fait, il y a souvent de bonnes raisons pour inclure d'autres données avec la clé, d'envelopper plusieurs clés ensemble, ou d'envelopper des données qui ne sont pas strictement parlant une clé. Ainsi, le terme de "données de clé" est utilisé au sens large pour signifier toutes les données qui sont enveloppées, mais en particulier les clés, car c'est principalement un algorithme d'enveloppe de clé. La clé utilisée pour faire l'enveloppe sera appelée clé de chiffrement de clé (KEK, *key-encryption key*).

Dans le présent document, une KEK peut être toute clé valide prise en charge par le dictionnaire AES. C'est-à-dire que une KEK peut être une clé de 128 bits, de 192 bits ou de 256 bits.

2. Généralités

L'algorithme d'enveloppe de clé AES est conçu pour envelopper ou chiffrer les données de clé. L'enveloppe de clé opère sur des blocs de 64 bits. Avant d'être enveloppées, les données de clé sont analysées en blocs de 64 bits.

La seule restriction que l'algorithme d'enveloppe de clé place sur n est que n soit supérieur ou égal à deux. (Pour les données de clé d'une longueur inférieure ou égale à 64 bits, le champ constant utilisé dans la présente spécification et les données de clé forment une seule entrée de dictionnaire de 128 bits qui rend inutile cette enveloppe de clé.) L'algorithme d'enveloppe de clé s'accommode de toutes les tailles de clé AES prises en charge. Cependant, d'autres valeurs cryptographiques ont souvent besoin d'être enveloppées. Une telle valeur est celle du germe du générateur de nombres aléatoires pour DSS. Cette valeur de germe exige que n soit supérieur à quatre. Il ne fait pas de doute que d'autres valeurs exigent ce type de protection. Donc, aucune limite supérieure n'est imposée à n.

L'enveloppe de clé AES peut être configurée de façon à utiliser n'importe laquelle des trois tailles de clé prises en charge par le dictionnaire AES. Le choix d'une taille de clé affecte la sécurité globale fournie par l'enveloppe de clé, mais il n'altère pas la description de l'algorithme d'enveloppe de clé. Donc, dans la description qui suit, l'enveloppe de clé est décrite de façon générique ; aucune taille de clé n'est spécifiée pour la KEK.

2.1 Notation et définitions

La notation suivante esr utilisée dans la description des algorithmes d'enveloppe de clés :

AES(K, W)	Chiffre W en utilisant le dictionnaire AES avec la clé K
AES-1(K, W)	Déchiffre W en utilisant le dictionnaire AES avec la clé K
MSB(j, W)	Retourne les j bits de poids fort de W
LSB(j, W)	Retourne les j bits de moindre poids de W
B1 ^ B2	Opération OU exclusif au bit près (OUX) sur B1 et B2
B1 | B2	Enchaînement de B1 et B2
K	Clé de chiffrement de clé K
n	Nombre de blocs de données de clé de 64 bits
s	Nombre d'étapes dans le processus d'enveloppe, s = 6n
P[i]	i^e bloc de données de clé en clair
C[i]	i^e bloc de données chiffrées
A	Registre de vérification d'intégrité de 64 bits
R[i]	Matrice de registres de 64 bits où i = 0, 1, 2, ..., n
A[t], R[i][t]	Contenu des registres A et R[i] après l'étape de chiffrement t.
IV	Valeur initiale de 64 bits utilisée durant le processus d'enveloppe.

Dans l'algorithme d'enveloppe de clé, la fonction d'enchaînement sera utilisée pour concaténer des quantités de 64 bits pour former l'entrée de 128 bits dans le dictionnaire AES. Les fonctions d'extraction seront utilisées pour partager le résultat de 128 bits tiré du dictionnaire AES en deux quantités de 64 bits.

2.2 Algorithmes

La spécification de l'algorithme d'enveloppe de clé exige l'utilisation du dictionnaire AES [AES]. Les trois paragraphes

qui suivent décrivent l'algorithme d'enveloppe de clé, l'algorithme de développement de clé, et la vérification d'intégrité des données inhérentes.

2.2.1 Enveloppe de clé

Les entrées au processus d'enveloppe de clé sont la KEK et le texte en clair à envelopper. Le texte en clair consiste en n blocs de 64 bits, qui contiennent les données de clé qui vont être enveloppées. Le processus d'enveloppe de clé est décrit ci-dessous.

Entrées : Texte en clair, n valeurs de 64 bits {P1, P2, ..., Pn}, et la clé, K (la KEK).
Résultats : Texte chiffré, (n+1) valeurs de 64 bits {C0, C1, ..., Cn}.

1) Initialiser les variables.
    Régler A0 à une valeur initiale (voir en 2.2.3)
    Pour i = 1 à n
        R[0][i] = P[i]
2) Calculer les valeurs intermédiaires.
    Pour t = 1 à s, où s = 6n
        A[t] = MSB(64, AES(K, A[t-1] | R[t-1][1])) ^ t
    Pour i = 1 à 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) Sortir le résultat.
    Régler C[0] = A[t]
    Pour i = 1 à n
        C[i] = R[t][i]

Une autre description de l'algorithme d'enveloppe de clé implique d'indexer plutôt que d'opérer un décalage. Cette approche permet de calculer la clé enveloppée en place, évitant la rotation de la description précédente. Cela produit un résultat identique et est plus facilement mis en œuvre dans les logiciels.

Entrées : Texte en clair, n valeurs de 64 bits {P1, P2, ..., Pn}, et la clé, K (la KEK).
Résultats : Texte chiffré, (n+1) valeurs de 64 bits {C0, C1, ..., Cn}.

1) Initialiser les variables.
    Régler A = IV, une valeur initiale (voir en 2.2.3)
    Pour i = 1 à n
        R[i] = P[i]

2) Calculer les valeurs intermédiaires.
    Pour j = 0 à 5
    Pour i = 1 à n
        B = AES(K, A | R[i])
        A = MSB(64, B) ^ t où t = (n*j)+i
        R[i] = LSB(64, B)

3) Sortir les résultats.
    Régler C[0] = A
    Pour i = 1 à n
        C[i] = R[i]

2.2.2 Développement de clé

Les entrées au processus de développement sont la KEK et (n+1) blocs de 64 bits de texte chiffré consistant en la clé enveloppée précédemment. Il retourne n blocs de texte en clair consistant en les n blocs de 64 bits des données de clé déchiffrées.

Entrées : Texte chiffré, (n+1) valeurs de 64 bits {C0, C1, ..., Cn}, et la clé, K (la KEK).
Résultats : Texte en clair, n valeurs de 64 bits {P1, P2, ..., Pn}.

1) Initialiser les variables.

```
    Régler A[s] = C[0]              où s = 6n
    Pour i = 1 à n
        R[s][i] = C[i]
```

2) Calculer les valeurs intermédiaires.

```
    Pour t = s à 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]))
    Pour i = 2 à n
        R[t-1][i] = R[t][i-1]
```

3) Sortir le résultat.

```
    Si A[0] est une valeur initiale appropriée (voir en 2.2.3),
    Alors
    Pour i = 1 à n
        P[i] = R[0][i]
    Autrement
        Retourner une erreur
```

L'algorithme de développement peut aussi être spécifié comme une opération fondée sur un indice, ce qui permet que le calcul soit fait en place. Là encore, cela donne le même résultat que l'approche du décalage de registre.

Entrées : Texte chiffré, (n+1) valeurs de 64 bits {C0, C1, ..., Cn}, et la clé, K (la KEK).
Résultats : Texte en clair, n valeurs de 64 bits {P0, P1, K, Pn}.

1) Initialiser les variables.

```
    Régler A = C[0]
    Pour i = 1 à n
        R[i] = C[i]
```

2) Calculer les valeurs intermédiaires.

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

3) Sortie des résultats.

```
    Si A est une valeur initiale appropriée (voir en 2.2.3),
    Alors
    Pour i = 1 à n
        P[i] = R[i]
    Autrement
        Retourner une erreur
```

2.2.3 Clé d'intégrité des données -- valeur initiale

La valeur initiale (IV) se réfère à la valeur allouée à A[0] dans la première étape du processus d'enveloppement. Cette valeur est utilisée pour obtenir une vérification d'intégrité sur les données de clé. Dans l'étape finale du processus de développement, la valeur récupérée de A[0] est comparée à la valeur attendue de A[0]. Si il y a correspondance, la clé est acceptée comme valide, et l'algorithme de développement la retourne. Si il n'y a pas correspondance, la clé est alors rejetée, et l'algorithme de développement retourne une erreur.

Les propriétés exactes réalisées par cette vérification d'intégrité dépendent de la définition de la valeur initiale. Des applications différentes peuvent invoquer des propriétés quelque peu différentes ; par exemple, si il est besoin de déterminer l'intégrité des données de clé tout au long de son cycle de vie ou juste quand elle est développée. La présente spécification définit une valeur initiale par défaut qui prend en charge l'intégrité des données de clé durant la période où elle est enveloppée (2.2.3.1). Des dispositions sont aussi prises pour prendre en charge d'autres valeurs initiales (2.2.3.2).

2.2.3.1 Valeur initiale par défaut

La valeur initiale (IV) par défaut est définie comme étant la constante hexadécimale :

A[0] = IV = A6A6A6A6A6A6A6A6

L'utilisation d'une constante telle que la IV prend en charge une forte vérification d'intégrité sur les données de clé durant la période qui est enveloppée. Si le développement produit A[0] = A6A6A6A6A6A6A6A6, la probabilité que les données de clé soient corrompues est alors de 2^-64. Si le développement produit toute autre valeur de A[0], le développement doit alors retourner une erreur et ne retourner aucune données de clé.

2.2.3.2 Valeurs initiales de remplacement

Lorsque l'enveloppe de clé est utilisée au titre d'un protocole ou système de gestion de clé plus large, la portée désirée pour l'intégrité des données peut être plus que les simples données de clé ou la durée désirée être plus que la seule période d'enveloppe. Aussi, si les données de clé ne sont pas une simple clé AES, elles peuvent n'être pas toujours un multiple de 64 bits. D'autres définitions de la valeur initiale peuvent être utilisées pour traiter un tel problème. Le NIST définira d'autres valeurs initiales dans de futures publications de gestion de clé en tant que de besoin. Afin de s'accommoder d'un ensemble de solutions de remplacement qui pourra évoluer avec le temps, les mises en œuvre d'enveloppe de clé qui ne sont pas spécifiques de l'application devront avoir une certaine souplesse dans la façon dont la valeur initiale est établie et vérifiée.

3. Identifiants d'objet

Le NIST a alloué les identifiants d'objet suivants pour identifier les algorithmes d'enveloppe de clé avec la valeur initiale par défaut spécifiée au paragraphe 2.2.3.1. Un identifiant d'objet est alloué pour être utilisé avec chaque taille de KEK AES.

IDENTIFIANT D'OBJET aes ::= { joint-iso-itu-t(2) country(16)

us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 1 }

IDENTIFIANT D'OBJET id-aes128-wrap ::= { aes 5 }
IDENTIFIANT D'OBJET id-aes192-wrap ::= { aes 25 }
IDENTIFIANT D'OBJET id-aes256-wrap ::= { aes 45 }

4. Vecteurs d'essai

Les exemples de cette section ont été générés en utilisant la mise en œuvre fondée sur l'indice de l'algorithme d'enveloppe de clé. L'utilisation de cette approche permet une mise en œuvre logicielle directe de l'algorithme d'enveloppe de clé.

4.1 Enveloppe de 128 bits de données de clé avec une KEK de 128 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F
Données de clé : 00112233445566778899AABBCCDDEEFF

Enveloppement :

Étape 1	A	R1	R2
Entrée	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
Codage	F4740052E82A2251	74CE86FBD7B805E7	8899AABBCCDDEEFF
OUX	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
Étape 2			
Entrée	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
Codage	06BA4EBDE7768D0B	74CE86FBD7B805E7	D132EE38147E76F8
OUX	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
Étape 3			
Entrée	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
Codage	FC967627BE937208	FE6E8D679C5D3460	D132EE38147E76F8
OUX	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8

Étape 4
Entrée FC967627BE93720B FE6E8D679C5D3460 D132EE38147E76F8
Codage 5896EA9028EE203B FE6E8D679C5D3460 07B2BD973E36A6FC
OUX 5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC

Étape 5
Entrée 5896EA9028EE203F FE6E8D679C5D3460 07B2BD973E36A6FC
Codage 93AEA71B258D90C3 25F5A3ADC2195401 07B2BD973E36A6FC
OUX 93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC

Étape 6
Entrée 93AEA71B258D90C6 25F5A3ADC2195401 07B2BD973E36A6FC
Codage E3EE986344D878F7 25F5A3ADC2195401 F14863BB1E9CA90A
OUX E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A

Étape 7
Entrée E3EE986344D878F1 25F5A3ADC2195401 F14863BB1E9CA90A
Codage 2BFC21B2C20E4006 B556D35ED8CEF052 F14863BB1E9CA90A
OUX 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A

Étape 8
Entrée 2BFC21B2C20E4001 B556D35ED8CEF052 F14863BB1E9CA90A
Codage 4BE8CE99C0A43A7D B556D35ED8CEF052 64BAE5818D0570BB
OUX 4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB

Étape 9
Entrée 4BE8CE99C0A43A75 B556D35ED8CEF052 64BAE5818D0570BB
Codage EBE1CE91067024F3 BE114B343EB00981 64BAE5818D0570BB
OUX EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB

Étape 10
Entrée EBE1CE91067024FA BE114B343EB00981 64BAE5818D0570BB
Codage 5A9C7B1F5B1C3B46 BE114B343EB00981 4FD3D2B7D74FBB42
OUX 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42

Étape 11
Entrée 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42
Codage 93B71967EED41FFC AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
OUX 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42

Étape 12
Entrée 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
Codage 1FA68B0A8112B44B AEF34BD8FB5A7B82 9D3E862371D2CFE5
OUX 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5

Résultat : :
Texte chiffré : 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5

Développement :
Étape 12 A R1 R2
Entrée 1FA68B0A8112B447 AEF34BD8FB5A7B82 9D3E862371D2CFE5
OUX 1FA68B0A8112B44B AEF34BD8FB5A7B82 9D3E862371D2CFE5
Décodage 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42

Étape 11
Entrée 93B71967EED41FF7 AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
OUX 93B71967EED41FFC AEF34BD8FB5A7B82 4FD3D2B7D74FBB42
Décodage 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42

Étape 10
Entrée 5A9C7B1F5B1C3B4C BE114B343EB00981 4FD3D2B7D74FBB42
OUX 5A9C7B1F5B1C3B46 BE114B343EB00981 4FD3D2B7D74FBB42

Décodage	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
Étape 9			
Entrée	EBE1CE91067024FA	BE114B343EB00981	64BAE5818D0570BB
OUX	EBE1CE91067024F3	BE114B343EB00981	64BAE5818D0570BB
Décodage	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
Étape 8			
Entrée	4BE8CE99C0A43A75	B556D35ED8CEF052	64BAE5818D0570BB
OUX	4BE8CE99C0A43A7D	B556D35ED8CEF052	64BAE5818D0570BB
Décodage	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
Étape 7			
Entrée	2BFC21B2C20E4001	B556D35ED8CEF052	F14863BB1E9CA90A
OUX	2BFC21B2C20E4006	B556D35ED8CEF052	F14863BB1E9CA90A
Décodage	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
Étape 6			
Entrée	E3EE986344D878F1	25F5A3ADC2195401	F14863BB1E9CA90A
OUX	E3EE986344D878F7	25F5A3ADC2195401	F14863BB1E9CA90A
Décodage	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
Étape 5			
Entrée	93AEA71B258D90C6	25F5A3ADC2195401	07B2BD973E36A6FC
OUX	93AEA71B258D90C3	25F5A3ADC2195401	07B2BD973E36A6FC
Décodage	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
Étape 4			
Entrée	5896EA9028EE203F	FE6E8D679C5D3460	07B2BD973E36A6FC
OUX	5896EA9028EE203B	FE6E8D679C5D3460	07B2BD973E36A6FC
Décodage	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
Étape 3			
Entrée	FC967627BE93720B	FE6E8D679C5D3460	D132EE38147E76F8
OUX	FC967627BE937208	FE6E8D679C5D3460	D132EE38147E76F8
Décodage	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
Étape 2			
Entrée	06BA4EBDE7768D09	74CE86FBD7B805E7	D132EE38147E76F8
OUX	06BA4EBDE7768D0B	74CE86FBD7B805E7	D132EE38147E76F8
Décodage	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
Étape 1			
Entrée	F4740052E82A2250	74CE86FBD7B805E7	8899AABBCCDDEEFF
OUX	F4740052E82A2251	74CE86FBD7B805E7	8899AABBCCDDEEFF
Décodage	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
Texte en clair :	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

Résultat :
Données de clé : 00112233445566778899AABBCCDDEEFF

4.2 Enveloppe de 128 bits de données de clé avec une KEK de 192 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F1011121314151617
Données de clé : 00112233445566778899AABBCCDDEEFF

Enveloppement :

Étape 1	A	R1	R21
Entrée	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

Codage	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF
OUX	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF

Étape 2

Entrée	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
Codage	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D
OUX	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D

Étape 3

Entrée	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
Codage	7B8E343CA51CF8AB	BC164F51E20CC983	51F22F3286758A2DOUX
	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D

Étape 4

Entrée	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
Codage	02A97C5897140595	BC164F51E20CC983	05FC2D8F8FF4B919
OUX	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919

Étape 5

Entrée	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
Codage	15D4B63F66583817	429487269D3A0016	05FC2D8F8FF4B919
OUX	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919

Étape 6

Entrée	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
Codage	AE2D0B76A6951EEA	429487269D3A0016	05A2D8FB4DD5BD7A
OUX	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A

Étape 7

Entrée	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
Codage	79F849444F4B8AA8	D40B091CDBAC0340	05A2D8FB4DD5BD7A
OUX	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A

Étape 8

Entrée	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
Codage	5933A9195B5F5E21	D40B091CDBAC0340	89F0D6C06F8CA9B4
OUX	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4

Étape 9

Entrée	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
Codage	57ADA800299C2E85	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
OUX	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4

Étape 10

Entrée	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
Codage	BF17BD6A9BC80163	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
OUX	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078

Étape 11

Entrée	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
Codage	B68BF270AE81544F	F92B5B97C050AED2	EB24CCFA52EA9078
OUX	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078

Étape 12

Entrée	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
Codage	96778B25AE6CA439	F92B5B97C050AED2	468AB8A17AD84E5D
OUX	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D

Résultat :

Texte chiffré :	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D

Développement :

Étape 12	A	R1	R2
Entrée	96778B25AE6CA435	F92B5B97C050AED2	468AB8A17AD84E5D
OUX	96778B25AE6CA439	F92B5B97C050AED2	468AB8A17AD84E5D
Décodage	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
Étape 11			
Entrée	B68BF270AE815444	F92B5B97C050AED2	EB24CCFA52EA9078
OUX	B68BF270AE81544F	F92B5B97C050AED2	EB24CCFA52EA9078
Décodage	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
Étape 10			
Entrée	BF17BD6A9BC80169	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
OUX	BF17BD6A9BC80163	4D5B3DFE7C04ABBA	EB24CCFA52EA9078
Décodage	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
Étape 9			
Entrée	57ADA800299C2E8C	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
OUX	57ADA800299C2E85	4D5B3DFE7C04ABBA	89F0D6C06F8CA9B4
Décodage	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
Étape 8			
Entrée	5933A9195B5F5E29	D40B091CDBAC0340	89F0D6C06F8CA9B4
OUX	5933A9195B5F5E21	D40B091CDBAC0340	89F0D6C06F8CA9B4
Décodage	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
Étape 7			
Entrée	79F849444F4B8AAF	D40B091CDBAC0340	05A2D8FB4DD5BD7A
OUX	79F849444F4B8AA8	D40B091CDBAC0340	05A2D8FB4DD5BD7A
Décodage	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
Étape 6			
Entrée	AE2D0B76A6951EEC	429487269D3A0016	05A2D8FB4DD5BD7A
OUX	AE2D0B76A6951EEA	429487269D3A0016	05A2D8FB4DD5BD7A
Décodage	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
Étape 5			
Entrée	15D4B63F66583812	429487269D3A0016	05FC2D8F8FF4B919
OUX	15D4B63F66583817	429487269D3A0016	05FC2D8F8FF4B919
Décodage	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
Étape 4			
Entrée	02A97C5897140591	BC164F51E20CC983	05FC2D8F8FF4B919
OUX	02A97C5897140595	BC164F51E20CC983	05FC2D8F8FF4B919
Décodage	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
Étape 3			
Entrée	7B8E343CA51CF8A8	BC164F51E20CC983	51F22F3286758A2D
OUX	7B8E343CA51CF8AB	BC164F51E20CC983	51F22F3286758A2D
Décodage	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
Étape 2			
Entrée	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D
OUX	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D
Décodage	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
Étape 1			
Entrée	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF
OUX	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF
Décodage	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
Texte en clair	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

Résultat :
Données de clé : 00112233445566778899AABBCCDDEEFF

4.3 Enveloppe de 128 bits de données de clé avec une KEK de 256 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Données de clé : 00112233445566778899AABBCCDDEEFF

Enveloppement :

Étape1	A	R1	R2
Entrée	6A6A6A6A6A6A6A6	011223344556677	899AABBCCDDEEFF
Codage	94314D454E3FDE1	661BD9F31FBFA31	899AABBCCDDEEFF
OUX	94314D454E3FDE0	661BD9F31FBFA31	899AABBCCDDEEFF
Étape 2			
Entrée	94314D454E3FDE0	661BD9F31FBFA31	8899AABBCCDDEEFF
Codage	450EA5C5BBCB561	661BD9F31FBFA31	60E0CDB7F429FE8
OUX	450EA5C5BBCB563	661BD9F31FBFA31	60E0CDB7F429FE8
Étape 3			
Entrée	450EA5C5BBCB563	661BD9F31FBFA31	60E0CDB7F429FE8
Codage	5DBDF1879D5C0A5	602001BFA07AD8B	60E0CDB7F429FE8
OUX	5DBDF1879D5C0A6	602001BFA07AD8B	60E0CDB7F429FE8
Étape 4			
Entrée	5DBDF1879D5C0A6	602001BFA07AD8B	60E0CDB7F429FE8
Codage	38C291128B7226D	602001BFA07AD8B	8924F777C3F678C
OUX	38C291128B72269	602001BFA07AD8B	8924F777C3F678C
Étape 5			
Entrée	38C291128B72269	602001BFA07AD8B	8924F777C3F678C
Codage	656A02DFFF054DC	4DF378183E3D5B2	8924F777C3F678C
OUX	656A02DFFF054D9	4DF378183E3D5B2	8924F777C3F678C
Étape 6			
Entrée	656A02DFFF054D9	4DF378183E3D5B2	8924F777C3F678C
Codage	DFD0C0E8B52A63A	F4DF378183E3D5B2	1AC1D36A964F41B
OUX	DFD0C0E8B52A63C	4DF378183E3D5B2	1AC1D36A964F41B
Étape 7			
Entrée	DFD0C0E8B52A63C	4DF378183E3D5B2	1AC1D36A964F41B
Codage	9AB00D4AE4399EA	271D5CED80F34ED	1AC1D36A964F41B
OUX	9AB00D4AE4399ED	271D5CED80F34ED	1AC1D36A964F41B
Étape 8			
Entrée	9AB00D4AE4399ED	271D5CED80F34ED	1AC1D36A964F41B
Codage	CE414878463EAAC	271D5CED80F34ED	7D8ED899E7929B8
OUX	CE414878463EAA4	271D5CED80F34ED	7D8ED899E7929B8
Étape 9			
Entrée	CE414878463EAA4	271D5CED80F34ED	7D8ED899E7929B8
Codage	BB44DB106AA0789	DF7E50829123648	7D8ED899E7929B8
OUX	BB44DB106AA0780	DF7E50829123648	7D8ED899E7929B8
Étape 10			
Entrée	BB44DB106AA0780	DF7E50829123648	7D8ED899E7929B8
Codage	77112A7308ADCC5	DF7E50829123648	472D5993D318FD2
OUX	77112A7308ADCCF	DF7E50829123648	472D5993D318FD2

Étape 11			
Entrée	77112A7308ADCCF	DF7E50829123648	472D5993D318FD2
Codage	8E40190807CC151	3E9777905818A2A	472D5993D318FD2
OUX	8E40190807CC15A	3E9777905818A2A	472D5993D318FD2
Étape 12			
Entrée	8E40190807CC15A	3E9777905818A2A	472D5993D318FD2
Codage	4E8C3F9CE0F5BAE	3E9777905818A2A	3C8191E7D6E8AE7
OUX	4E8C3F9CE0F5BA2	3E9777905818A2A	3C8191E7D6E8AE7
Résultat : :			
Texte chiffré	64E8C3F9CE0F5BA2	63E9777905818A2A	93C8191E7D6E8AE7

Développpement :

Étape 12	A	R1	R2
Entrée	64E8C3F9CE0F5BA2	63E9777905818A2A	93C8191E7D6E8AE7
OUX	64E8C3F9CE0F5BAE	63E9777905818A2A	93C8191E7D6E8AE7
Décodage	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
Étape 11			
Entrée	78E40190807CC15A	63E9777905818A2A	3472D5993D318FD2
OUX	78E40190807CC151	63E9777905818A2A	3472D5993D318FD2
Décodage	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
Étape 10			
Entrée	877112A7308ADCCF	0DF7E50829123648	3472D5993D318FD2
OUX	877112A7308ADCC5	0DF7E50829123648	3472D5993D318FD2
Décodage	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
Étape 9			
Entrée	FBB44DB106AA0780	0DF7E50829123648	67D8ED899E7929B8
OUX	FBB44DB106AA0789	0DF7E50829123648	67D8ED899E7929B8
Décodage	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
Étape 8			
Entrée	4CE414878463EAA4	5271D5CED80F34ED	67D8ED899E7929B8
OUX	4CE414878463EAAC	5271D5CED80F34ED	67D8ED899E7929B8
Décodage	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
Étape 7			
Entrée	39AB00D4AE4399ED	5271D5CED80F34ED	91AC1D36A964F41B
OUX	39AB00D4AE4399EA	5271D5CED80F34ED	91AC1D36A964F41B
Décodage	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
Étape 6			
Entrée	DDFD0C0E8B52A63C	F4DF378183E3D5B2	91AC1D36A964F41B
OUX	DDFD0C0E8B52A63A	F4DF378183E3D5B2	91AC1D36A964F41B
Décodage	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
Étape 5			
Entrée	2656A02DFFF054D9	F4DF378183E3D5B2	58924F777C3F678C
OUX	2656A02DFFF054DC	F4DF378183E3D5B2	58924F777C3F678C
Décodage	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
Étape 4			
Entrée	738C291128B72269	5602001BFA07AD8B	58924F777C3F678C
OUX	738C291128B7226D	5602001BFA07AD8B	58924F777C3F678C
Décodage	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
Étape 3			
Entrée	85DBDF1879D5C0A6	5602001BFA07AD8B	F60E0CDB7F429FE8
OUX	85DBDF1879D5C0A5	5602001BFA07AD8B	F60E0CDB7F429FE8

Décodage	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
Étape 2			
Entrée	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
OUX	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8
Décodage	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
Étape 1			
Entrée	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
OUX	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF
Décodage	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
Texte en clair	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF

Résultat : :
Données de clé : 00112233445566778899AABBCCDDEEFF

4.4 Enveloppe de 192 bits de données de clé avec une KEK de 192 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F1011121314151617
Données de clé : 00112233445566778899AABBCCDDEEFF0001020304050607

Enveloppement :

Étape 1	A	R1	R2	R3
Entrée	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
Codage	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
OUX	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
Étape 2				
Entrée	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
Codage	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D	0001020304050607
OUX	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
Étape 3				
Entrée	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
Codage	2C8E19A519025B7C	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
OUX	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
Étape 4				
Entrée	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
Codage	E727C7BDF822602E	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
OUX	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
Étape 5				
Entrée	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
Codage	15B61F7B25D51700	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
OUX	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
Étape 6				
Entrée	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
Codage	A187755AEA64719C	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
OUX	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
Étape 7				
Entrée	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
Codage	5A994895D81644B7	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
OUX	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
Étape 8				
Entrée	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787

Codage	864F408C8AB8CDCF	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
OUX	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787

Étape 9

Entrée	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
Codage	53F4373F575EB7A4	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
OUX	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295

Étape 10

Entrée	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
Codage	9EAA4CDA0B1BA5FF	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
OUX	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295

Étape 11

Entrée	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
Codage	B1B9902C68E0EB52	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
OUX	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295

Étape 12

Entrée	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
Codage	FCE591D77709A6E0	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
OUX	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5

Étape 13

Entrée	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
Codage	428428D2BD88CF58	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
OUX	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5

Étape 14

Entrée	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
Codage	6AC861AB961DA578	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
OUX	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5

Étape 15

Entrée	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
Codage	E80DB49CC9A1EA61	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
OUX	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53

Étape 16

Entrée	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
Codage	ABEE3534AC465C2C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
OUX	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53

Étape 17

Entrée	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
Codage	E7CC8D8CEDE62BF7	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
OUX	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53

Étape 18

Entrée	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
Codage	031D33264E15D320	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
OUX	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2

Résultat : :

Texte chiffré	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2

Développement :

Étape 18	A	R1	R2	R3
Entrée	031D33264E15D332	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
OUX	031D33264E15D320	68F24EC260743EDC	E1C6C7DDEE725A93	6BA814915C6762D2
Décodage	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53

Étape 17				
Entrée	E7CC8D8CEDE62BE6	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
OUX	E7CC8D8CEDE62BF7	68F24EC260743EDC	E1C6C7DDEE725A93	84943C8C67FCFD53
Décodage	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
Étape 16				
Entrée	ABEE3534AC465C3C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
OUX	ABEE3534AC465C2C	68F24EC260743EDC	56E3CEE892BBEFC4	84943C8C67FCFD53
Décodage	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
Étape 15				
Entrée	E80DB49CC9A1EA6E	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
OUX	E80DB49CC9A1EA61	C46965F34EFB2261	56E3CEE892BBEFC4	84943C8C67FCFD53
Décodage	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
Étape 14				
Entrée	6AC861AB961DA576	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
OUX	6AC861AB961DA578	C46965F34EFB2261	56E3CEE892BBEFC4	463437433A93EFE5
Décodage	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
Étape 13				
Entrée	428428D2BD88CF55	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
OUX	428428D2BD88CF58	C46965F34EFB2261	63F6D88A0663FEF9	463437433A93EFE5
Décodage	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
Étape 12				
Entrée	FCE591D77709A6EC	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
OUX	FCE591D77709A6E0	98883EDC6B080FB5	63F6D88A0663FEF9	463437433A93EFE5
Décodage	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
Étape 11				
Entrée	B1B9902C68E0EB59	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
OUX	B1B9902C68E0EB52	98883EDC6B080FB5	63F6D88A0663FEF9	ED5E8456E61BD295
Décodage	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
Étape 10				
Entrée	9EAA4CDA0B1BA5F5	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
OUX	9EAA4CDA0B1BA5FF	98883EDC6B080FB5	552A09E141D08AE3	ED5E8456E61BD295
Décodage	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
Étape 9				
Entrée	53F4373F575EB7AD	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
OUX	53F4373F575EB7A4	926ED65A9E853FD9	552A09E141D08AE3	ED5E8456E61BD295
Décodage	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
Étape 8				
Entrée	864F408C8AB8CDC7	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
OUX	864F408C8AB8CDCF	926ED65A9E853FD9	552A09E141D08AE3	D1E708FD13778787
Décodage	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
Étape 7				
Entrée	5A994895D81644B0	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
OUX	5A994895D81644B7	926ED65A9E853FD9	AE82BC1118A5DEA4	D1E708FD13778787
Décodage	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
Étape 6				
Entrée	A187755AEA64719A	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
OUX	A187755AEA64719C	A08DAA041D17BBBA	AE82BC1118A5DEA4	D1E708FD13778787
Décodage	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
Étape 5				
Entrée	15B61F7B25D51705	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3
OUX	15B61F7B25D51700	A08DAA041D17BBBA	AE82BC1118A5DEA4	FF540E514DE120A3

Décodage	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3

Étape 4

Entrée	E727C7BDF822602A	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
OUX	E727C7BDF822602E	A08DAA041D17BBBA	51F22F3286758A2D	FF540E514DE120A3
Décodage	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3

Étape 3

Entrée	2C8E19A519025B7F	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
OUX	2C8E19A519025B7C	351D385096CCFB29	51F22F3286758A2D	FF540E514DE120A3
Décodage	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607

Étape 2

Entrée	9D9B32B9ED742E00	351D385096CCFB29	51F22F3286758A2D	0001020304050607
OUX	9D9B32B9ED742E02	351D385096CCFB29	51F22F3286758A2D	0001020304050607
Décodage	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607

Étape 1

Entrée	DFE8FD5D1A3786A6	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
OUX	DFE8FD5D1A3786A7	351D385096CCFB29	8899AABBCCDDEEFF	0001020304050607
Décodage	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607

Texte en clair	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607

Résultat : :
Données de clé : 00112233445566778899AABBCCDDEEFF0001020304050607

4.5 Enveloppe de 192 bits de données de clé avec une KEK de 256 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Données de clé : 00112233445566778899AABBCCDDEEFF0001020304050607

Enveloppement :

Étape 1	A	R1	R2	R3
Entrée	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
Codage	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
OUX	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607

Étape 2

Entrée	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
Codage	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
OUX	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607

Étape 3

Entrée	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
Codage	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
OUX	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154

Étape 4

Entrée	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
Codage	F1D28EA6295891EC	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
OUX	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154

Étape 5

Entrée	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
Codage	BF213BFD04E8A24F	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
OUX	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154

Étape 6

Entrée	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
Codage	6F85BFBDB7E880E3	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B

OUX	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Étape 7				
Entrée	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Codage	D532789E4E79D819	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
OUX	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Étape 8				
Entrée	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Codage	2A5FFCEF1F1916D8	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
OUX	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
Étape 9				
Entrée	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
Codage	01271BA91D9804F6	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
OUX	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
Étape 10				
Entrée	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
Codage	A3223BD7237F7033	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
OUX	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
Étape 11				
Entrée	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
Codage	B50C330616E7B1C7	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
OUX	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
Étape 12				
Entrée	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
Codage	FB8AFF3F083E12CE	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
OUX	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
Étape 13				
Entrée	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
Codage	82F597607784A33C	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
OUX	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
Étape 14				
Entrée	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
Codage	D48E5E83B7C906DB	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
OUX	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
Étape 15				
Entrée	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
Codage	1BF2B1CD947311B6	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
OUX	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
Étape 16				
Entrée	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
Codage	C9F5F26A378011DE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
OUX	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
Étape 17				
Entrée	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
Codage	39128CE5E435F3A0	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
OUX	39128CE5E4325F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
Étape 18				
Entrée	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
Codage	A8F9BC1612C68B2D	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
OUX	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
Texte chiffré	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1

Développement :

Étape 18	A	R1	R2	R3
Entrée	A8F9BC1612C68B3F	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
OUX	A8F9BC1612C68B2D	F6E6F4FBE30E71E4	769C8B80A32CB895	8CD5D17D6B254DA1
Décodage	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
Étape 17				
Entrée	39128CE5E435F3B1	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
OUX	39128CE5E435F3A0	F6E6F4FBE30E71E4	769C8B80A32CB895	C490C33642717146
Décodage	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
Étape 16				
Entrée	C9F5F26A378011CE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
OUX	C9F5F26A378011DE	F6E6F4FBE30E71E4	D36F4FFBA2C82ED9	C490C33642717146
Décodage	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
Étape 15				
Entrée	1BF2B1CD947311B9	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
OUX	1BF2B1CD947311B6	FB1F2965FCE1E783	D36F4FFBA2C82ED9	C490C33642717146
Décodage	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
Étape 14				
Entrée	D48E5E83B7C906D5	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
OUX	D48E5E83B7C906DB	FB1F2965FCE1E783	D36F4FFBA2C82ED9	0B08CFDF48020F0D
Décodage	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
Étape 13				
Entrée	82F597607784A331	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
OUX	82F597607784A33C	FB1F2965FCE1E783	73EDC8CB9322C34E	0B08CFDF48020F0D
Décodage	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
Étape 12				
Entrée	FB8AFF3F083E12C2	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
OUX	FB8AFF3F083E12CE	FB1611A83BEB567F	73EDC8CB9322C34E	0B08CFDF48020F0D
Décodage	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
Étape 11				
Entrée	B50C330616E7B1CC	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
OUX	B50C330616E7B1C7	FB1611A83BEB567F	73EDC8CB9322C34E	740A273461ED82C6
Décodage	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
Étape 10				
Entrée	A3223BD7237F7039	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
OUX	A3223BD7237F7033	FB1611A83BEB567F	C6874607903270CD	740A273461ED82C6
Décodage	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
Étape 9				
Entrée	01271BA91D9804FF	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
OUX	01271BA91D9804F6	444F92BF78E77BB1	C6874607903270CD	740A273461ED82C6
Décodage	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
Étape 8				
Entrée	2A5FFCEF1F1916D0	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
OUX	2A5FFCEF1F1916D8	444F92BF78E77BB1	C6874607903270CD	39EBC1A1A53FF55B
Décodage	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Étape 7				
Entrée	D532789E4E79D81E	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
OUX	D532789E4E79D819	444F92BF78E77BB1	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Décodage	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B

Étape 6				
Entrée	6F85BFBDB7E880E5	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
OUX	6F85BFBDB7E880E3	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	39EBC1A1A53FF55B
Décodage	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
Étape 5				
Entrée	BF213BFD04E8A24A	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
OUX	BF213BFD04E8A24F	0CC86A4D9B9C6A31	AEBE2D5C8BF747A9	6CA405593A3B5154
Décodage	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
Étape 4				
Entrée	F1D28EA6295891E8	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
OUX	F1D28EA6295891EC	0CC86A4D9B9C6A31	F60E0CDB7F429FE8	6CA405593A3B5154
Décodage	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
Étape 3				
Entrée	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
OUX	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8	6CA405593A3B5154
Décodage	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
Étape 2				
Entrée	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
OUX	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8	0001020304050607
Décodage	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
Étape 1				
Entrée	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
OUX	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF	0001020304050607
Décodage	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607
Texte en clair	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF	0001020304050607

Résultat :
Données de clé : 00112233445566778899AABBCCDDEEFF0001020304050607

4.6 Enveloppe de256 bits de données de clé avec une KEK de 256 bits

Entrée :
KEK : 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
Données de clé : 00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

Enveloppement :

Étape 1	A/R3	R1/R4	R2
Entrée	A6A6A6A6A6A6A6A6	0011223344556677	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
Codage	794314D454E3FDE1	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
OUX	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
Étape 2			
Entrée	794314D454E3FDE0	F661BD9F31FBFA31	8899AABBCCDDEEFF
	0001020304050607	08090A0B0C0D0E0F	
Codage	D450EA5C5BBCB561	F661BD9F31FBFA31	F60E0CDB7F429FE8
	0001020304050607	08090A0B0C0D0E0F	
OUX	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
	0001020304050607	08090A0B0C0D0E0F	
Étape 3			
Entrée	D450EA5C5BBCB563	F661BD9F31FBFA31	F60E0CDB7F429FE8
	0001020304050607	08090A0B0C0D0E0F	

Codage	9DF8F5405FBC00C1	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	08090A0B0C0D0E0F	
OUX	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	08090A0B0C0D0E0F	

Étape 4

Entrée	9DF8F5405FBC00C2	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	08090A0B0C0D0E0F	
Codage	564408FDD0DD2EA4	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	
OUX	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	

Étape 5

Entrée	564408FDD0DD2EA0	F661BD9F31FBFA31	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	
Codage	4EF02EDD3146AFBB	E7D1194D853E53F8	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	
OUX	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	

Étape 6

Entrée	4EF02EDD3146AFBE	E7D1194D853E53F8	F60E0CDB7F429FE8
	6CA405593A3B5154	E5923CB9FDB56FBC	
Codage	963AAFFD96B223EC	E7D1194D853E53F8	EFD48BA304945576
	6CA405593A3B5154	E5923CB9FDB56FBC	
OUX	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576
	6CA405593A3B5154	E5923CB9FDB56FBC	

Étape 7

Entrée	963AAFFD96B223EA	E7D1194D853E53F8	EFD48BA304945576
	6CA405593A3B5154	E5923CB9FDB56FBC	
Codage	66D7A8ADD086B9DD	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	E5923CB9FDB56FBC	
OUX	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	E5923CB9FDB56FBC	

Étape 8

Entrée	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	E5923CB9FDB56FBC	
Codage	C58B9D3AC6D5B94E	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	

Étape 9

Entrée	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Codage	1A681354E84C41F8	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	

Étape 10

Entrée	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Codage	DBA417FB51F9E3CB	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	

Étape 11

Entrée	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA

	C365B66943E2D760	73E3B6CBE5D05D74	
Codage	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
OUX	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
Étape 12			
Entrée	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
Codage	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 13			
Entrée	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Codage	2E8E2B6BB2016696	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 14			
Entrée	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Codage	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 15			
Entrée	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
Codage	33FE29365885C4B7	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	
OUX	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	
Étape 16			
Entrée	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	
Codage	5075496800978B4A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Étape 17			
Entrée	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Codage	A5382A26B47551F1	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Étape 18			
Entrée	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Codage	F19D80D437EFE8F9	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	

Étape 19

Entrée	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	
Codage	B422B444B87A190B	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
OUX	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	

Étape 20

Entrée	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
Codage	D058823360F88A37	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	

Étape 21

Entrée	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
Codage	C89A96CA7B163ECC	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	

Étape 22

Entrée	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
Codage	39D02FE7435870ED	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	

Étape 23

Entrée	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	
Codage	0AEB82AE3146A91B	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	
OUX	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	

Étape 24

Entrée	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	
Codage	28C9F404C4B810EC	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	FB988B9B7A02DD21	
OUX	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	FB988B9B7A02DD21	

Résultat : :

Texte chiffré	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	FB988B9B7A02DD21	

Développement :

Étape 24	A/R3	R1/R4	R2
Entrée	28C9F404C4B810F4	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	FB988B9B7A02DD21	
OUX	28C9F404C4B810EC	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	FB988B9B7A02DD21	
Décodage	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	

Étape 23			
Entrée	0AEB82AE3146A90C	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	
OUX	0AEB82AE3146A91B	CBCCB35CFB87F826	3F5786E2D80ED326
	CBC7F0E71A99F43B	07DFE775B9687E73	
Décodage	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	
Étape 22			
Entrée	39D02FE7435870FB	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	39D02FE7435870ED	CBCCB35CFB87F826	3F5786E2D80ED326
	1CFBF6B4C24CB982	07DFE775B9687E73	
Décodage	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
Étape 21			
Entrée	C89A96CA7B163ED9	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	C89A96CA7B163ECC	CBCCB35CFB87F826	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
Décodage	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36
1	CFBF6B4C24CB982	07DFE775B9687E73	
Étape 20			
Entrée	D058823360F88A23	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
OUX	D058823360F88A37	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	07DFE775B9687E73	
Décodage	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
Étape 19			
Entrée	B422B444B87A1918	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
OUX	B422B444B87A190B	1BB8C765A84195E7	F7EDAD518C960D36
	1CFBF6B4C24CB982	40F68C91DB49702C	
Décodage	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	
Étape 18			
Entrée	F19D80D437EFE8EB	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	F19D80D437EFE8F9	1BB8C765A84195E7	F7EDAD518C960D36
	C272E9466AAE98F9	40F68C91DB49702C	
Décodage	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Étape 17			
Entrée	A5382A26B47551E0	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	A5382A26B47551F1	1BB8C765A84195E7	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Décodage	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Étape 16			
Entrée	5075496800978B5A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
OUX	5075496800978B4A	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	40F68C91DB49702C	
Décodage	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	

Étape 15			
Entrée	33FE29365885C4B8	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	
OUX	33FE29365885C4B7	4745856AF333F01F	BCA418BBF7DCE60B
	C272E9466AAE98F9	3CF149E90E8C04D9	
Décodage	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 14			
Entrée	15342443CB95ADBF	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	15342443CB95ADB1	4745856AF333F01F	BCA418BBF7DCE60B
	F56701DAF0388216	3CF149E90E8C04D9	
Décodage	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 13			
Entrée	2E8E2B6BB201669B	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	2E8E2B6BB2016696	4745856AF333F01F	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Décodage	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Étape 12			
Entrée	F9ED8A1429515669	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
OUX	F9ED8A1429515665	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	3CF149E90E8C04D9	
Décodage	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
Étape 11			
Entrée	0629EB29A42E4FD2	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
OUX	0629EB29A42E4FD9	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	F56701DAF0388216	73E3B6CBE5D05D74	
Décodage	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
Étape 10			
Entrée	DBA417FB51F9E3C1	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	DBA417FB51F9E3CB	D6AE29ECE7192D43	FBEC169FA5C0F6BA
	C365B66943E2D760	73E3B6CBE5D05D74	
Décodage	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Étape 9			
Entrée	1A681354E84C41F1	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	1A681354E84C41F8	D6AE29ECE7192D43	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Décodage	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Étape 8			
Entrée	C58B9D3AC6D5B946	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
OUX	C58B9D3AC6D5B94E	E7D1194D853E53F8	EFD48BA304945576
	C365B66943E2D760	73E3B6CBE5D05D74	
Décodage	66D7A8ADD086B9DA	E7D1194D853E53F8	EFD48BA304945576

C365B66943E2D760 E5923CB9FDB56FBC

Étape 7
Entrée 66D7A8ADD086B9DA E7D1194D853E53F8 EFD48BA304945576
C365B66943E2D760 E5923CB9FDB56FBC
OUX 66D7A8ADD086B9DD E7D1194D853E53F8 EFD48BA304945576
C365B66943E2D760 E5923CB9FDB56FBC
Décodage 963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
6CA405593A3B5154 E5923CB9FDB56FBC

Étape 6
Entrée 963AAFFD96B223EA E7D1194D853E53F8 EFD48BA304945576
6CA405593A3B5154 E5923CB9FDB56FBC
OUX 963AAFFD96B223EC E7D1194D853E53F8 EFD48BA304945576
6CA405593A3B5154 E5923CB9FDB56FBC
Décodage 4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC

Étape 5
Entrée 4EF02EDD3146AFBE E7D1194D853E53F8 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC
OUX 4EF02EDD3146AFBB E7D1194D853E53F8 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC
Décodage 564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC

Étape 4
Entrée 564408FDD0DD2EA0 F661BD9F31FBFA31 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC
OUX 564408FDD0DD2EA4 F661BD9F31FBFA31 F60E0CDB7F429FE8
6CA405593A3B5154 E5923CB9FDB56FBC
Décodage 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
6CA405593A3B5154 08090A0B0C0D0E0F

Étape 3
Entrée 9DF8F5405FBC00C2 F661BD9F31FBFA31 F60E0CDB7F429FE8
6CA405593A3B5154 08090A0B0C0D0E0F
OUX 9DF8F5405FBC00C1 F661BD9F31FBFA31 F60E0CDB7F429FE86CA405593A3B5154
08090A0B0C0D0E0F
Décodage D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
0001020304050607 08090A0B0C0D0E0F

Étape 2
Entrée D450EA5C5BBCB563 F661BD9F31FBFA31 F60E0CDB7F429FE8
0001020304050607 08090A0B0C0D0E0F
OUX D450EA5C5BBCB561 F661BD9F31FBFA31 F60E0CDB7F429FE8
0001020304050607 08090A0B0C0D0E0F
Décodage 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
0001020304050607 08090A0B0C0D0E0F

Étape 1
Entrée 794314D454E3FDE0 F661BD9F31FBFA31 8899AABBCCDDEEFF
0001020304050607 08090A0B0C0D0E0F
OUX 794314D454E3FDE1 F661BD9F31FBFA31 8899AABBCCDDEEFF
0001020304050607 08090A0B0C0D0E0F
Décodage A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
0001020304050607 08090A0B0C0D0E0F

Texte en clair A6A6A6A6A6A6A6A6 0011223344556677 8899AABBCCDDEEFF
0001020304050607 08090A0B0C0D0E0F

Résultat :
Données de clé : 00112233445566778899AABBCCDDEEFF000102030405060708090A0B0C0D0E0F

5. Considérations pour la sécurité

L'algorithme d'enveloppe de clé comporte une vérification d'intégrité forte sur les données de clé. Si le développement donne la valeur de vérification attendue en A[0], la probabilité que les données de clé soient corrompues est de 2^-64. Si le développement produit une valeur inattendue, la mise en œuvre de l'algorithme DOIT retourner une erreur, et elle NE DOIT PAS retourner de données de clé.

Les mises en œuvre doivent protéger la KEK de la divulgation. La compromission de la KEK peut résulter en la divulgation de toutes les données de clé protégées par cette KEK.

6. Références

[AES] National Institute of Standards et Technology. FIPS Pub 197 : "Advanced Encryption Standard (AES)". 26 novembre 2001.

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

7. Remerciements

La plus grande partie du texte de ce document est tirée de [AES-WRAP]. Les auteurs de ce document sont responsables du développement de l'algorithme d'enveloppe de clé AES.

8. Adresse des auteurs

Russell Housley
RSA Laboratories
918 Spring Knoll Drive
Herndon, VA 20170 USA
mél : rhousley@rsasecurity.com

Jim Schaad
Soaring Hawk Consulting
mél : jimsch@exmsft.com

9. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuelement assuré par la Internet Society.