Groupe de travail Réseau
Request for Comments : 3602
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Frankel & R. Glenn, NIST
S. Kelly, Airespace
septembre 2003

L'algorithme de chiffrement AES-CBC et son utilisation avec IPsec

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit l'utilisation de l'algorithme de chiffrement de la norme de chiffrement évoluée (AES, *Advanced Encryption Standard*) en mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) avec un vecteur d'initialisation (IV, *Initialization Vector*) explicite, comme mécanisme de confidentialité dans le contexte de la charge utile de sécurité encapsulée (ESP, *Encapsulating Security Payload*) IPsec.

Table des Matières

1. Introduction

Au terme d'un processus de compétition de quatre ans, le NIST (Institut National des Normes et Technologies américain) a sélectionné la norme de chiffrement évoluée (AES, *Advanced Encryption Standard*) comme successeur de la vénérable norme de chiffrement de données (DES, *Data Encryption Standard*). La compétition était ouverte, avec participation

publique et commentaires sollicités à chaque étape du processus. [AES], anciennement connu sous le nom de Rijndael, a été choisi parmi les cinq finalistes.

Le choix d'AES a été fait sur la base de plusieurs caractéristiques :
+ sécurité
+ non couvert par le secret défense
+ publication
+ disponible dans le monde entier sans redevance
+ capable de traiter une taille de bloc d'au moins 128 bits
+ au minimum, capable de traiter des tailles de clé de 128, 192, et 256 bits
+ efficacité de calcul et exigences de mémoire acceptées sur un grand nombre de logiciels et matériels, y compris des cartes à mémoire
+ souplesse, simplicité et facilité de mise en œuvre.

AES sera le mode de chiffrement désigné du gouvernement américain. Il est prévu que AES va suffire pour protéger les informations sensibles (non couvertes par le secret défense) du gouvernement jusqu'au moins le siècle prochain. Il est aussi prévu qu'il soit largement adopté par les milieux d'affaires et les institutions financières.

L'intention du groupe de travail IPsec de l'IETF est que AES soit finalement adopté comme chiffrement ESP IPsec par défaut et qu'il obtienne le statut de DOIT être inclus dans les mises en œuvre IPsec conformes.

La suite du présent document spécifie l'utilisation d'AES dans le contexte de ESP IPsec. Pour plus d'informations sur la façon dont les diverses pièces d'ESP s'assemblent pour fournir des services de sécurité, se référer à [RFC2401], [RFC2406], et [RFC2411].

1.1 Spécification des exigences

Dans le présent document, les mots clés "DOIT, "NE DOIT PAS", "DEVRA", "NE DEVRA PAS", "DEVRAIT", et "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", "FACULTATIF", sont à interpréter comme décrit dans la [RFC2119].

2. Algorithme de chiffrement AES

Tous les algorithmes de chiffrement par bloc symétrique partagent des caractéristiques et variables communes parmi lesquelles sont le mode, la taille de clé, les clés faibles, la taille de bloc, et les tours de chiffrement. Les paragraphes qui suivent contiennent des descriptions des caractéristiques pertinentes pour le chiffrement AES.

2.1 Mode

Le NIST a défini cinq modes de fonctionnement pour AES et les autres chiffrements approuvés par FIPS [MODES] : le chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining)*, le mode dictionnaire (ECB, *Electronic CodeBook*), le mode rebouclage du chiffrement (CFB, *Cipher FeedBack*), le rebouclage de la sortie (OFB, *Output FeedBack*) et le mode compteur (CTR, *Counter*). Le mode CBC est bien défini et bien compris pour les chiffrements symétriques, et est actuellement exigé pour tous les autres chiffrements ESP. Le présent document spécifie l'utilisation du chiffrement AES en mode CBC au sein de ESP. Ce mode exige un vecteur d'initialisation (IV, *Initialization Vector*) qui soit de la même taille que celle du bloc. L'utilisation d'un IV généré de façon aléatoire empêche de générer un texte chiffré identique à partir de paquets qui ont des données identiques qui s'étendent sur le premier bloc de la taille de bloc de l'algorithme de chiffrement.

Le IV est OUXé avec le premier bloc de texte en clair avant qu'il soit chiffré. Puis pour les blocs successifs, le précédent bloc de texte chiffré est OUXé avec le texte en clair actuel, avant qu'il soit chiffré.

On trouvera plus d'informations sur le mode CBC dans [MODES] et [CRYPTOS]. Pour l'utilisation du mode CBC dans ESP avec un chiffrement à 64 bits, voir la [RFC2451].

2.2 Taille de clé et nombre de tours

AES accepte trois tailles de clé : 128 bits, 192 bits, et 256 bits. La taille de clé par défaut est 128 bits, et toutes les mises en œuvre DOIVENT accepter cette taille de clé. Les mises en œuvre PEUVENT aussi accepter des tailles de clé de 192 bits et 256 bits.

AES utilise un nombre de tours différent pour chacune des tailles de clé définies. Lorsque on utilise une clé de 128 bits, la

mise en œuvre DOIT utiliser 10 tours. Lorsque on utilise une clé de 192 bits, la mise en œuvre DOIT utiliser 12 tours. Avec une clé de 256 bits, la mise en œuvre DOIT utiliser 14 tours.

2.3 Clés faibles

Au moment de la rédaction du présent document, il n'y a pas de clé faible connue pour AES.

Certains algorithmes de chiffrement ont des clés faibles ou des clés qui NE DOIVENT PAS être utilisées à cause de leur interaction avec certains aspects de la définition du chiffrement. Si on découvrait des clés faibles pour l'AES, ces clés faibles DEVRAIENT être vérifiées et éliminées lors d'une gestion de clé manuelle. Avec une gestion de clé dynamique, telle que dans la [RFC2409], les vérifications de clés faibles NE DEVRAIENT PAS être effectuées car elles sont vues comme une complexité supplémentaire inutile du code qui pourrait affaiblir le niveau de sécurité voulu [EVALUA].

2.4 Taille de bloc et bourrage

AES utilise une taille de bloc de seize octets (128 bits).

Le bourrage est exigé par AES pour maintenir une taille de bloc de 16 octets (128 bits). Le bourrage DOIT être ajouté, comme spécifié dans la [RFC2406], de façon que les données à chiffrer (qui incluent les champs ESP Longueur de bourrage et Prochain en-tête) aient une longueur qui soit un multiple de 16 octets.

À cause des exigences de bourrage spécifiques de l'algorithme, aucun bourrage supplémentaire n'est exigé pour s'assurer que le texte chiffré se termine sur une limite de quatre octets (c'est-à-dire, de maintenir une taille de bloc garantie de 16 octets que les champs ESP Longueur de bourrage et Prochain en-tête seront alignés à droite dans un mot de quatre octets). Un bourrage supplémentaire PEUT être inclus, comme spécifié dans la [RFC2406], pour autant que la taille de 16 octets soit maintenue.

2.5 Informations supplémentaires

AES a été inventé par Joan Daemen de Banksys/PWI et Vincent Rijmen de ESAT-COSIC, tous deux belges, et est disponible gratuitement dans le monde entier. Il n'est couvert par aucun brevet, et la page d'accueil de Rijndael contient la déclaration suivante : "Rijndael est disponible gratuitement. Vous pouvez l'utiliser pour tout objet à votre convenance, sans considération de sa désignation ou non comme AES". On trouvera la description d'AES dans [AES]. La page d'accueil de Rijndael est : http://www.esat.kuleuven.ac.be/~rijmen/rijndael/ .

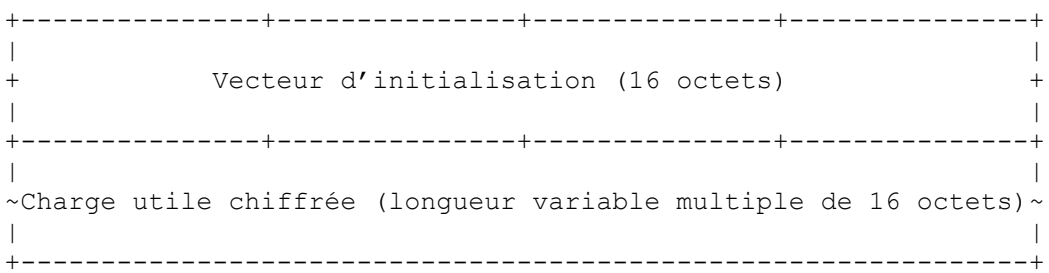
La page d'accueil AES, http://www.nist.gov/aes , contient une quantité d'informations sur AES, y compris une description définitive de l'algorithme d'AES, des statistiques de performances, des vecteurs d'essai et des informations de propriété intellectuelle. Ce site contient aussi des informations sur la façon d'obtenir une mise en œuvre de référence d'AES de la part du NIST.

2.6 Performances

Pour un tableau de comparaison des vitesses estimée d'AES et des autres algorithmes de chiffrement, prière de se reporter à [PERF-1], [PERF-2], [PERF-3], ou [PERF-4]. La page d'accueil de AES a des pointeurs sur d'autres analyses.

3. Charge utile ESP

La charge utile ESP est constituée de l'IV suivi par le texte chiffré brut. Donc, le champ de charge utile, comme défini dans la [RFC2406], est découpé selon le diagramme suivant :



Le champ IV DOIT avoir la même taille que le bloc de l'algorithme de chiffrement utilisé. L'IV DOIT être choisi au hasard, et DOIT être imprévisible.

Inclure l'IV dans chaque datagramme assure que le déchiffrement de chaque datagramme reçu peut être effectué, même lorsque certains datagrammes sont abandonnés, ou que des datagrammes sont réarrangés dans le transit.

Pour éviter un chiffrement en CBC de blocs de texte en clair très similaires dans différents paquets, les mises en œuvre NE DOIVENT PAS utiliser un compteur ou autre source de distance de Hamming faible pour les IV.

3.1 Interactions algorithmiques d'ESP

Il n'y a actuellement pas de problème connu concernant des interactions entre AES et d'autres aspects de ESP, comme l'utilisation de certains schémas d'authentification.

3.2 Matériel de clé

Le nombre minimum de bits envoyés du protocole d'échange de clés à l'algorithme ESP doit être supérieur ou égal à la taille de clé.

La clé de chiffrement et de déchiffrement est tirée des <x> premiers bits du matériel de clé, où <x> représente la taille de clé requise.

4. Vecteurs d'essai

Les quatre premiers cas d'essai vérifient le chiffrement AES-CBC. Chaque essai comporte la clé, le texte en clair, et le texte chiffré résultant. Les valeurs des clés et des données sont soit en nombres hexadécimaux (précédés de "0x") soit en chaînes de caractères ASCII (entourées de doubles guillemets). Si une valeur est une chaîne de caractères ASCII, le calcul AES-CBC pour le cas d'essai correspondant NE COMPORTE PAS de caractère nul ('\0') en queue de la chaîne. Les valeurs de texte chiffré calculées sont toutes des nombres hexadécimaux.

Les quatre derniers cas d'essai illustrent des échantillons de paquets ESP qui utilisent AES-CBC pour le chiffrement. Toutes les données sont des nombres hexadécimaux (non précédés de "0x").

Ces cas d'essai ont été vérifiés en utilisant deux mises en œuvre indépendantes : la mise en œuvre AES-CBC de référence du NIST et une mise en œuvre fournie par les auteurs de l'algorithme de Rijndael (disponible à http://csrc.nist.gov/encryption/aes/rijndael/rijndael-unix-refc.tar).

Cas n° 1 : Chiffrement de 16 octets (1 bloc) en utilisant AES-CBC avec une clé de 128 bits
Clé : 0x06a9214036b8a15b512e03d534120006
IV : 0x3dafba429d9eb430b422da802c9fac41
Texte en clair : "Single block msg"
Texte chiffré : 0xe353779c1079aeb82708942dbe77181a

Cas n° 2 : Chiffrement de 32 octets (2 blocs) en utilisant AES-CBC avec une clé de 128 bits
Clé : 0xc286696d887c9aa0611bbb3e2025a45a
IV : 0x562e17996d093d28ddb3ba695a2e6f58
Texte clair : 0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
Texte chiffré : 0xd296cd94c2cccf8a3a863028b5e1dc0a7586602d253cfff91b8266bea6d61ab1

Cas n° 3 : Chiffrement de 48 octets (3 blocs) en utilisant AES-CBC avec une clé de 128 bits
Clé : 0x6c3ea0477630ce21a2ce334aa746c2cd
IV : 0xc782dc4c098c66cbd9cd27d825682c81
Texte clair : "This is a 48-byte message (exactly 3 AES blocks)"
Texte chiffré :
0xd0a02b3836451753d493665d33f0e8862dea54cdb293abc7506939276772f8d5021c19216bad525c8579695d83ba2684

Cas n° 4 : Chiffrement de 64 octets (4 blocs) en utilisant AES-CBC avec une clé de 128 bits
Clé : 0x56e47a38c5598974bc46903dba290349
IV : 0x8ce82eefbea0da3c44699ed7db51b7d9
Texte clair :

0xa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1
d2d3d4d5d6d7d8d9dadbdcdddedf
Texte chiffré :
0xc30e32ffedc0774e6aff6af0869f71aa0f3af07a9a31a9c684db207eb0ef8e4e35907aa632c3ffdf868bb7b29d3d46ad83ce9f
9a102ee99d49a53e87f4c3da55

Cas n° 5 : Échantillon de paquet ESP en mode transport (ping 192.168.123.100)
Clé : 90d382b4 10eeba7a d938c46c ec1a82bf
SPI : 4321
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.100
Numéro de séquence : 1
IV : e96e8c08 ab465763 fd098d45 dd3ff893
Paquet d'origine :
En-tête IP (20 octets) : 45000054 08f20000 4001f9fe c0a87b03 c0a87b64
Données (64 octets) :
08000ebd a70a0000 8e9c083d b95b0700 08090a0b 0c0d0e0f 10111213 1415161718191a1b 1c1d1e1f 20212223
24252627 28292a2b 2c2d2e2f 30313233 34353637
Augmentation des données avec :
Bourrage : 01020304 05060708 090a0b0c 0d0e
Longueur de bourrage : 0e
Prochain en-tête : 01 (ICMP)
Données pré-chiffrement avec bourrage, longueur de bourrage et nouvel en-tête (80 octets) :
08000ebd a70a0000 8e9c083d b95b0700 08090a0b 0c0d0e0f 10111213 1415161718191a1b 1c1d1e1f 20212223
24252627 28292a2b 2c2d2e2f 30313233 3435363701020304 05060708 090a0b0c 0d0e0e01
Paquet après chiffrement avec SPI, numéro de séquence , IV :
En-tête IP : 4500007c 08f20000 4032f9a5 c0a87b03 c0a87b64
N° de SPI/séquence : 00004321 00000001
IV : e96e8c08 ab465763 fd098d45 dd3ff893
Données chiffrées (80 octets) :
f663c25d 325c18c6 a9453e19 4e120849 a4870b66 cc6b9965 330013b4 898dc856a4699e52 3a55db08 0b59ec3a
8e4b7e52 775b07d1 db34ed9c 538ab50c 551b874aa269add0 47ad2d59 13ac19b7 cfbad4a6

Cas n° 6 : Échantillon de paquet en mode transport (ping -p 77 -s 20 192.168.123.100)
Clé : 90d382b4 10eeba7a d938c46c ec1a82bf
SPI : 4321
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.100
Numéro de séquence : 8
IV : 69d08df7 d203329d b093fc49 24e5bd80
Paquet d'origine :
En-tête IP (20 octets) : 45000030 08fe0000 4001fa16 c0a87b03 c0a87b64
Données (28 octets) : 0800b5e8 a80a0500 a69c083d 0b660e00 77777777 77777777 77777777Données augmentées avec :
Bourrage : 0102
Longueur de bourrage : 02
Prochain en-tête : 01 (ICMP)
Données pré chiffrement avec bourrage, longueur de bourrage et prochain en-tête (32 octets) :
0800b5e8 a80a0500 a69c083d 0b660e00 77777777 77777777 77777777 01020201
Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500004c 08fe0000 4032f9c9 c0a87b03 c0a87b64
N° de SPI/séquence : 00004321 00000008
IV : 69d08df7 d203329d b093fc49 24e5bd80
Données chiffrées (32 octets) : f5199588 1ec4e0c4 488987ce 742e8109 689bb379 d2d750c0 d915dca3 46a89f75
Cas n° 7 : Échantillon de paquet ESP en mode tunnel (ping 192.168.123.200)
Clé : 01234567 89abcdef 01234567 89abcdef
SPI : 8765
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.200
Numéro de séquence : 2
IV : f4e76524 4f6407ad f13dc138 0f673f37
Paquet d'origine :
En-tête IP (20 octets) : 45000054 09040000 4001f988 c0a87b03 c0a87bc8
Données (64 octets) :

08009f76 a90a0100 b49c083d 02a20400 08090a0b 0c0d0e0f 10111213 1415161718191a1b 1c1d1e1f 20212223
24252627 28292a2b 2c2d2e2f 30313233 34353637
Données augmentées avec :
Bourrage : 01020304 05060708 090a
Longueur de bourrage : 0a
Prochain en-tête : 04 (IP-in-IP)
Données avant chiffrement avec l'en-tête IP d'origine, le bourrage, longueur de bourrage et le prochain en-tête (96 octets) :
45000054 09040000 4001f988 c0a87b03 c0a87bc8 08009f76 a90a0100 b49c083d
02a20400 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f 20212223
24252627 28292a2b 2c2d2e2f 30313233 34353637 01020304 05060708 090a0a04
Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500008c 09050000 4032f91e c0a87b03 c0a87bc8
N° de SPI/séq : 00008765 00000002
IV : f4e76524 4f6407ad f13dc138 0f673f37
Données chiffrées (96 octets) :
773b5241 a4c44922 5e4f3ce5 ed611b0c 237ca96c f74a9301 3c1b0ea1 a0cf70f8
e4ecaec7 8ac53aad 7a0f022b 859243c6 47752e94 a859352b 8a4d4d2d ecd136e5
c177f132 ad3fbfb2 201ac990 4c74ee0a 109e0ca1 e4dfe9d5 a100b842 f1c22f0d

Cas n° 8 : Échantillon de paquet en mode tunnel ESP (ping -p ff -s 40 192.168.123.200)
Clé : 01234567 89abcdef 01234567 89abcdef
SPI : 8765
Adresse de source : 192.168.123.3
Adresse de destination : 192.168.123.200
Numéro de séquence : 5
IV : 85d47224 b5f3dd5d 2101d4ea 8dffab22
Paquet d'origine :
En-tête IP (20 octets) : 45000044 090c0000 4001f990 c0a87b03 c0a87bc8
Données (48 octets) : 0800d63c aa0a0200 c69c083d a3de0300 ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
Données augmentées par :
Bourrage : 01020304 05060708 090a
Longueur de bourrage : 0a
Prochain en-tête : 04 (IP-in-IP)
Données avant chiffrement avec en-tête IP d'origine, bourrage, longueur de bourrage et prochain en-tête (80 octets) :
45000044 090c0000 4001f990 c0a87b03 c0a87bc8 0800d63c aa0a0200 c69c083d a3de0300 ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff ffffffff ffffffff 01020304 05060708 090a0a04
Paquet après chiffrement avec SPI, numéro de séquence, IV :
En-tête IP : 4500007c 090d0000 4032f926 c0a87b03 c0a87bc8
N° de SPI/séq : 00008765 00000005
IV : 85d47224 b5f3dd5d 2101d4ea 8dffab22
Données chiffrées (80 octets) :
15b92683 819596a8 047232cc 00f7048f e45318e1 1f8a0f62 ede3c3fc 61203bb5
0f980a08 c9843fd3 a1b06d5c 07ff9639 b7eb7dfb 3512e5de 435e7207 ed971ef3
d2726d9b 5ef6affc 6d17a0de cbb13892

5. Interactions d'IKE

5.1 Identifiant de phase 1

Pour les négociations de phase 1, l'IANA a alloué un identifiant d'algorithme de chiffrement de 7 pour AES-CBC.

5.2 Identifiant de phase 2

Pour les négociations de phase 2, l'IANA a alloué un identifiant de transformation ESP de 12 pour ESP_AES.

5.3 Attribut de longueur de clé

Comme AES permet des longueurs de clé variables, l'attribut Longueur de clé DOIT être spécifié dans les deux échanges de phase 1 [RFC2404] et de phase 2 [RFC2407].

5.4 Considérations sur l'algorithme de hachage

Une autre compétition, pour choisir le successeur de SHA-1, l'algorithme de hachage largement utilisé, s'est récemment terminée. Les hachages résultants, appelés SHA-256, SHA-384 et SHA-512 [SHA2-1], [SHA2-2] sont capables de produire des résultats de trois longueurs différentes (256, 384 et 512 bits) suffisantes pour la génération (au sein de IKE) et l'authentification (au sein d'ESP) de trois tailles de clés AES (128, 192 et 256 bits).

Cependant, HMAC-SHA-1 [RFC2404] et HMAC-MD5 [RFC2403] sont actuellement considérés comme de force suffisante pour servir à la fois comme générateurs IKE de clés AES de 128 bits et comme authentifiants ESP pour le chiffrement AES en utilisant des clés de 128 bits.

6. Considérations sur la sécurité

Les mises en œuvre sont invitées à utiliser les plus grandes tailles de clés qu'elles peuvent lorsque elles prennent en compte les considérations de performances pour leur configuration particulière de matériel et de logiciel. Noter que le chiffrement a nécessairement un impact sur les deux côtés d'un canal sécurisé, de sorte qu'une telle considération doit tenir compte non seulement du côté client, mais aussi de celui du serveur. Cependant, une taille de clé de 128 bits est considérée comme sûre pour l'avenir prévisible.

On trouvera plus d'informations sur la nécessité d'utiliser des valeurs d'IV aléatoires dans [CRYPTOB].

Pour plus d'informations sur les considérations sur la sécurité, le lecteur est invité à lire [AES].

7. Considérations relatives à l'IANA

L'IANA a alloué l'identifiant d'algorithme de chiffrement 7 à AES-CBC.
L'IANA a alloué l'identifiant de transformation ESP 12 à ESP_AES.

8. Déclaration de droits de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'IETF au sujet des droits contenus dans les documents en cours de normalisation et la documentation en rapport avec les normes se trouvent dans le BCP-11. Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

9. Références

9.1 Références normatives

[AES] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," novembre 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197 .{ps,pdf}

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

9.2 Références pour information

[CRYPTOB] Bellovin, S., "Probable Plaintext Cryptanalysis of the IP Security Protocols", Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, pp. 155-160, février 1997. http://www.research.att.com/~smb/papers/probtxt.pdf

[CRYPTOS] B. Schneier, "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995, ISBN 0-471-12845-7.

[EVALUA] Ferguson, N. and B. Schneier, "A Cryptographic Evaluation of IPsec," Counterpane Internet Security, Inc., janvier 2000. http://www.counterpane.com/ipsec.pdf

[MODES] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Methods and Techniques," NIST Special Publication 800-38A, décembre 2001. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[PERF-1] Bassham, L. III, "Efficiency Testing of ANSI C Implementations of Round1 Candidate Algorithms for the Advanced Encryption Standard." http://csrc.nist.gov/encryption/aes/round1/r1-ansic.pdf

[PERF-2] Lipmaa, Helger, "AES/Rijndael: speed." http://www.tcs.hut.fi/~helger/aes/rijndael.html

[PERF-3] Nechvetal, J., E. Barker, D. Dodson, M. Dworkin, J. Foti and E. Roback, "Status Report on the First Round of the Development of the Advanced Encryption Standard." http://csrc.nist.gov/encryption/aes/round1/r1report.pdf

[PERF-4] Schneier, B., J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions." http://www.counterpane.com/aes-performance.pdf

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir* 4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Remplacée par* RFC6071*)*

[SHA2-1] NIST, FIPS PUB 180-2 "Specifications for the Secure Hash Standard," August 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[SHA2-2] "Descriptions of SHA-256, SHA-384, and SHA-512." http://csrc.nist.gov/cryptval/shs/sha256-384-512.pdf

10. Remerciements

Des portions du présent texte, ainsi que sa structure générale, ont été empruntées à la [RFC2451].

Les auteurs tiennent à remercier Hilarie Orman qui a fourni l'appui de son expertise (et une vérification de cohérence) sur les tailles de clés,les exigences pour les groupes Diffie-Hellman, et les interactions IKE. Nos remerciements aussi à Scott Fluhrer pour ses précieux commentaires et recommandations .

11. Adresse des auteurs

Sheila Frankel
NIST
820 West Diamond Ave.
Room 677
Gaithersburg, MD 20899
USA
téléphone : +1 (301) 975-3297
mél : sheila.frankel@nist.gov

Scott Kelly
Airespace
110 Nortech Pkwy
San Jose CA 95134
USA
téléphone : +1 408 635 2000
mél : scott@hyperthought.com

Rob Glenn
NIST
820 West Diamond Ave.
Room 605
Gaithersburg, MD 20899
USA
téléphone : +1 (301) 975-3667
mél : rob.glenn@nist.gov

12. Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.