

Groupe de travail Réseau  
**Request for Comments : 3526**  
Catégorie : En cours de normalisation  
Traduction Claude Brière de L'Isle

T. Kivinen  
M. Kojo  
SSH Communications Security  
mai 2003

# Groupes supplémentaires d'exponentiation modulaire (MODP) Diffie-Hellman pour l'échange de clés Internet (IKE)

**Statut du présent mémoire**

Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à discussion et suggestions en vue de son amélioration. Prière de se rapporter à l'édition en cours des "Internet Official Protocol Standards" (normes officielles du protocole Internet) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est pas soumise à restrictions.

**Déclaration de copyright**

Copyright (C) The Internet Society (2003). Tous droits réservés

**Résumé**

Le présent document définit de nouveaux groupes d'exponentiation modulaire (MODP, *Modular Exponential*) pour le protocole d'échange de clés Internet (IKE, *Internet Key Exchange*). Il documente le groupe 5 bien connu et largement utilisé de 1536 bits, et définit aussi de nouveaux groupes Diffie-Hellman de 2048, 3072, 4096, 6144, et 8192 bits numérotés à partir de 14. La sélection des nombres premiers pour ces groupes suit les critères établis par Richard Schroepel.

## Table des Matières

1. Introduction.....	1
2. Groupe MODP à 1536 bits.....	2
3. Groupe MODP à 2048 bits.....	2
4. Groupe MODP à 3072 bits.....	2
5. Groupe MODP à 4096 bits.....	3
6. Groupe MODP à 6144 bits.....	3
7. Groupe MODP à 8192 bits.....	4
8. Considérations pour la sécurité.....	4
9. Considérations relatives à l'IANA.....	5
10. Références normatives.....	5
11. Références non normatives.....	5
12. Adresse des auteurs.....	5
13. Déclaration complète de copyright.....	6

## 1. Introduction

Un des paramètres importants du protocole négociés par l'échange de clés Internet (IKE) [RFC-2409] est le "groupe" Diffie-Hellman qui sera utilisé pour certaines opérations cryptographiques. Actuellement, IKE définit quatre groupes. Ces groupes sont approximativement aussi forts qu'une clé symétrique de 70-80 bits.

Le nouveau chiffrement de la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) [AES], qui a plus de force, a besoin de groupes plus forts. Pour l'AES à 128 bits, on a besoin d'un groupe d'environ 3200 bits [Orman01]. Les clés de 192 et 256 bits auraient besoin de groupes ayant respectivement environ 8000 et 15 400 bits. Une autre source [RSA13] [Rousseau00] estime que la taille de clé de sécurité équivalente pour le chiffrement symétrique à 192 bits est de 2 500 bits au lieu de 8 000 bits, et que la taille de clé équivalente au chiffrement symétrique à 256 bits est 4 200 bits au lieu de 15 400 bits.

À cause de ce désaccord, nous spécifions simplement différents groupes sans spécifier quel groupe devrait être utilisé avec l'AES à 128, 192 ou 256 bits. Avec les matériels actuels, les groupes supérieurs à 8 192-bits étant trop lents pour une utilisation pratique, le présent document ne fournit aucun groupe supérieur à 8 192-bits.

La taille d'exposant utilisée dans le Diffie-Hellman doit être choisie de telle sorte qu'elle corresponde aux autres parties du système. Il ne devrait pas être le maillon faible du système de sécurité. Il devrait avoir une entropie double de la force du système tout entier, c'est-à-dire que si vous utilisez un groupe dont la force est de 128 bits, vous devez utiliser plus de 256 bits d'aléa dans l'exposant du calcul Diffie-Hellman.

## 2. Groupe MODP à 1536 bits

Le groupe MODP à 1536 bits a été utilisé depuis assez longtemps pour les applications, mais il n'était pas défini dans la RFC 2409 (IKE). Les mises en œuvre utilisent le terme groupe 5 pour désigner ce groupe, Cette pratique est normalisée par la présente.

Le nombre premier est :  $2^{1536} - 2^{1472} - 1 + 2^{64} * \{ [2^{1406} \text{ pi}] + 741804 \}$

Sa valeur hexadécimale est :

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22
514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6
F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB
9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA237327 FFFFFFFF FFFFFFFF
```

Le générateur est : 2.

## 3. Groupe MODP à 2048 bits

L'identifiant alloué à ce groupe est 14.

Ce nombre premier est :  $2^{2048} - 2^{1984} - 1 + 2^{64} * \{ [2^{1918} \text{ pi}] + 124476 \}$

Sa valeur hexadécimale est :

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22
514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6
F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB
9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603
9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
15728E5A 8AAACAA6 FFFFFFFF FFFFFFFF
```

Le générateur est : 2.

## 4. Groupe MODP à 3072 bits

L'identifiant alloué à ce groupe est 15.

Ce nombre premier est :  $2^{3072} - 2^{3008} - 1 + 2^{64} * \{ [2^{2942} \text{ pi}] + 1690314 \}$

Sa valeur hexadécimale est :

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22
514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6
F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB
9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603
9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D
```

B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864  
 D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31  
 43DB5BFC E0FD108E 4B82D120 A93AD2CA FFFFFFFF FFFFFFFF

Le générateur est : 2.

## 5. Groupe MODP à 4096 bits

L'identifiant alloué à ce groupe est 16.

Ce nombre premier est :  $2^{4096} - 2^{4032} - 1 + 2^{64} * \{ [2^{3966} \text{ pi}] + 240904 \}$

Sa valeur hexadécimale est :

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22  
 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6  
 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D  
 C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB  
 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603  
 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510  
 15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D  
 B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864  
 D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31  
 43DB5BFC E0FD108E 4B82D120 A9210801 1A723C12 A787E6D7 88719A10 BDBA5B26 99C32718 6AF4E23C  
 1A946834 B6150BDA 2583E9CA 2AD44CE8 DBBBC2DB 04DE8EF9 2E8EFC14 1FBECBA6 287C5947 4E6BC05D  
 99B2964F A090C3A2 233BA186 515BE7ED 1F612970 CEE2D7AF B81BDD76 2170481C D0069127 D5B05AA9  
 93B4EA98 8D8FDDC1 86FFB7DC 90A6C08F 4DF435C9 34063199 FFFFFFFF FFFFFFFF

Le générateur est : 2.

## 6. Groupe MODP à 6144 bits

L'identifiant alloué à ce groupe est 17.

Ce nombre premier est :  $2^{6144} - 2^{6080} - 1 + 2^{64} * \{ [2^{6014} \text{ pi}] + 929484 \}$

Sa valeur hexadécimale est :

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22  
 514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6  
 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D  
 C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB  
 9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603  
 9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510  
 15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D  
 B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864  
 D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31  
 43DB5BFC E0FD108E 4B82D120 A9210801 1A723C12 A787E6D7 88719A10 BDBA5B26 99C32718 6AF4E23C  
 1A946834 B6150BDA 2583E9CA 2AD44CE8 DBBBC2DB 04DE8EF9 2E8EFC14 1FBECBA6 287C5947 4E6BC05D  
 99B2964F A090C3A2 233BA186 515BE7ED 1F612970 CEE2D7AF B81BDD76 2170481C D0069127 D5B05AA9  
 93B4EA98 8D8FDDC1 86FFB7DC 90A6C08F 4DF435C9 34028492 36C3FAB4 D27C7026 C1D4DCB2 602646DE  
 C9751E76 3DBA37BD F8FF9406 AD9E530E E5DB382F 413001AE B06A53ED 9027D831 179727B0 865A8918  
 DA3EDBEB CF9B14ED 44CE6CBA CED4BB1B DB7F1447 E6CC254B 33205151 2BD7AF42 6FB8F401 378CD2BF  
 5983CA01 C64B92EC F032EA15 D1721D03 F482D7CE 6E74FEF6 D55E702F 46980C82 B5A84031 900B1C9E  
 59E7C97F BEC7E8F3 23A97A7E 36CC88BE 0F1D45B7 FF585AC5 4BD407B2 2B4154AA CC8F6D7E BF48E1D8  
 14CC5ED2 0F8037E0 A79715EE F29BE328 06A1D58B B7C5DA76 F550AA3D 8A1FBFF0 EB19CCB1 A313D55C  
 DA56C9EC 2EF29632 387FE8D7 6E3C0468 043E8F66 3F4860EE 12BF2D5B 0B7474D6 E694F91E 6DCC4024

FFFFFFFF FFFFFFFF

Le générateur est : 2.

7. Groupe MODP à 8192 bits

L’identifiant alloué à ce groupe est 18.

Ce nombre premier est :  $2^{8192} - 2^{8128} - 1 + 2^{64} * \{ [2^{8062} \text{ pi}] + 4743158 \}$

Sa valeur hexadécimale est :

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1 29024E08 8A67CC74 020BBEA6 3B139B22  
514A0879 8E3404DD EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245 E485B576 625E7EC6  
F44C42E9 A637ED6B 0BFF5CB6 F406B7ED EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D  
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F 83655D23 DCA3AD96 1C62F356 208552BB  
9ED52907 7096966D 670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B E39E772C 180E8603  
9B2783A2 EC07A28F B5C55DF0 6F4C52C9 DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510  
15728E5A 8AAAC42D AD33170D 04507A33 A85521AB DF1CBA64 ECFB8504 58DBEF0A 8AEA7157 5D060C7D  
B3970F85 A6E1E4C7 ABF5AE8C DB0933D7 1E8C94E0 4A25619D CEE3D226 1AD2EE6B F12FFA06 D98A0864  
D8760273 3EC86A64 521F2B18 177B200C BBE11757 7A615D6C 770988C0 BAD946E2 08E24FA0 74E5AB31  
43DB5BFC E0FD108E 4B82D120 A9210801 1A723C12 A787E6D7 88719A10 BDBA5B26 99C32718 6AF4E23C  
1A946834 B6150BDA 2583E9CA 2AD44CE8 DBBBC2DB 04DE8EF9 2E8EFC14 1FBECBA6 287C5947 4E6BC05D  
99B2964F A090C3A2 233BA186 515BE7ED 1F612970 CEE2D7AF B81BDD76 2170481C D0069127 D5B05AA9  
93B4EA98 8D8FDDC1 86FFB7DC 90A6C08F 4DF435C9 34028492 36C3FAB4 D27C7026 C1D4DCB2 602646DE  
C9751E76 3DBA37BD F8FF9406 AD9E530E E5DB382F 413001AE B06A53ED 9027D831 179727B0 865A8918  
DA3EDBEB CF9B14ED 44CE6CBA CED4BB1B DB7F1447 E6CC254B 33205151 2BD7AF42 6FB8F401 378CD2BF  
5983CA01 C64B92EC F032EA15 D1721D03 F482D7CE 6E74FEF6 D55E702F 46980C82 B5A84031 900B1C9E  
59E7C97F BEC7E8F3 23A97A7E 36CC88BE 0F1D45B7 FF585AC5 4BD407B2 2B4154AA CC8F6D7E BF48E1D8  
14CC5ED2 0F8037E0 A79715EE F29BE328 06A1D58B B7C5DA76 F550AA3D 8A1FBFF0 EB19CCB1 A313D55C  
DA56C9EC 2EF29632 387FE8D7 6E3C0468 043E8F66 3F4860EE 12BF2D5B 0B7474D6 E694F91E 6DBE1159  
74A3926F 12FEE5E4 38777CB6 A932DF8C D8BEC4D0 73B931BA 3BC832B6 8D9DD300 741FA7BF 8AFC47ED  
2576F693 6BA42466 3AAB639C 5AE4F568 3423B474 2BF1C978 238F16CB E39D652D E3FDB8BE FC848AD9  
22222E04 A4037C07 13EB57A8 1A23F0C7 3473FC64 6CEA306B 4BCBC886 2F8385DD FA9D4B7F A2C087E8  
79683303 ED5BDD3A 062B3CF5 B3A278A6 6D2A13F8 3F44F82D DF310EE0 74AB6A36 4597E899 A0255DC1  
64F31CC5 0846851D F9AB4819 5DED7EA1 B1D510BD 7EE74D73 FAF36BC3 1ECFA268 359046F4 EB879F92  
4009438B 481C6CD7 889A002E D5EE382B C9190DA6 FC026E47 9558E447 5677E9AA 9E3050E2 765694DF  
C81F56E8 80B96E71 60C980DD 98EDD3DF FFFFFFFF FFFFFFFF

Le générateur est : 2.

8. Considérations pour la sécurité

Le présent document décrit de nouveaux groupes plus forts à utiliser dans IKE. La force des groupes définis ici est toujours estimée et il y a autant de méthodes d’estimation qu’il y a de cryptographes. Pour les estimations de force ci-dessous, on a pris les deux extrémités de l’échelle de sorte que l’estimation de la force réelle se situe vraisemblablement entre les deux valeurs données ci-dessous.

Groupe	Module	Estimation de force 1		Estimation de force 2	
		en bits	taille d’exposant	en bits	taille d’exposant
5	1536 bits	90	180-	120	240-
14	2048 bits	110	220-	160	320-
15	3072 bits	130	260-	210	420-
16	4096 bits	150	300-	240	480-
17	6144 bits	170	340-	270	540-
18	8192 bits	190	380-	310	620-

## 9. Considérations relatives à l'IANA

IKE [RFC-2409] définit quatre groupes Diffie-Hellman, numérotés de 1 à 4.

Le présent document définit un nouveau groupe 5, et de nouveaux groupes de 14 à 18. Les demandes pour des allocations supplémentaires sont via le "Consensus de l'IETF" comme défini dans la [RFC-2434]. Précisément, il est prévu que les nouveaux groupes soient documentés dans une RFC en voie de normalisation.

## 10. Références normatives

[RFC-2409] D. Harkins et D. Carrel, "Échange de clés Internet (IKE)", RFC 2409, novembre 1998.

[RFC-2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.

## 11. Références non normatives

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

[RFC-2412] H. Orman, H., "Protocole OAKLEY de détermination de clés", RFC 2412, novembre 1998.

[Orman01] H. Orman et P. Hoffman, "Détermination de la force des clés publiques utilisées pour l'échange de clés symétriques", Travail en cours.

[RSA13] R. Silverman, "RSA Bulletin #13: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths", avril 2000, <http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html>

[Rousseau00] F. Rousseau, "New Time and Space Based Key Size Equivalents for RSA and Diffie-Hellman", décembre 2000, <http://www.sandelman.ottawa.on.ca/ipsec/2000/12/msg00045.html>

## 12. Adresse des auteurs

Tero Kivinen  
SSH Communications Security Corp  
Fredrikinkatu 42  
FIN-00100 HELSINKI  
Finland  
mél : [kivinen@ssh.fi](mailto:kivinen@ssh.fi)

Mika Kojo  
HELSINKI  
Finland  
mél : [mika.kojo@helsinki.fi](mailto:mika.kojo@helsinki.fi)

## 13. Déclaration complète de copyright

Copyright (C) The Internet Society (2003). Tous droits réservés

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de copyright ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de copyright ou les références à la Internet Society ou aux autres organisations Internet,

excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de copyright définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou successeurs ou ayant droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et LE CONTRIBUTEUR, L'ORGANISATION QU'IL OU ELLE REPRÉSENTE OU QUI LE/LA FINANCE (S'IL EN EST), LA INTERNET SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI ENCLOSES NE VIOLE AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

**Remerciement**

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