Network Working Group
Request for Comments: 3526
Category: Standards Track

T. Kivinen
M. Kojo
SSH Communications Security

May 2003

Группы DH MODP для IKE

More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

Статус документа

Этот документ содержит спецификацию проекта стандартного протокола Internet и служит приглашением к дискуссии в целях развития протокола. Текущее состояние стандартизации и статус протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Авторские права

Тезисы

Этот документ определяет новые группы MODP[1] для протокола обмена ключами в Internet (IKE[2]). Описана общеизвестная 1536-битовая с номером 5 и добавлены новые группы Diffie-Hellman размером 2048, 3072, 4096, 6144 и 8192 бита, номера которых начинаются с 14. Выбор простых чисел для этих групп выполнен в соответствии с критериями Richard Schroeppel.

Оглавление

1. Введение

Одних из важных протокольных параметров, согласуемых с помощью IKE [RFC-2409], является группа Diffie-Hellman, которая будет применяться в некоторых криптографических операциях. IKE в настоящее время включает 4 таких группы. Криптостойкость этих групп приблизительно соответствует симметричным ключам размером 70 - 80 битов.

Новый шифр AES[3] [AES] обеспечивает большую криптостойкость и требует более сильных групп. Для 128-битового AES нужна группа размером около 3200 битов [Orman01]. Ключи размером 192 и 256 битов будут требовать новых групп с размерами около 8000 и 15400 битов, соответственно. Другие источники [RSA13] [Rousseau00] оценивают для ключей, криптографически эквивалентных симметричному ключу размером 192 бита, необходимость группы размером 2500 вместо 8000 битов, а для эквивалента 256-битовых симметричных ключей - 4200 битов вместо 15400.

В силу такой существенной разницы в оценках здесь просто предлагается набор групп без указания какую из них следует применять со 128, 192 или 256-битовыми ключами AES. С учетом того, что современные аппаратные реализации групп размером более 8192 битов слишком медленны, в документе не предложены группы с размером больше 8192 битов.

Размер показателя, используемого методом Diffie-Hellman, должен выбираться в соответствии с другими параметрами системы. Он не должен быть самым слабым звеном в системе защиты. Следует выбирать значение показателя, обеспечивающее двойное превышение по энтропии в сравнении с энтропией системы в целом. Например, при использовании группы со стойкостью 128 битов, требуется обеспечить более 256 битов хаотичности в показателе, применяемом для расчетов Diffie-Hellman.

2. 1536-битовая группа MODP

1536-битовая группа MODP достаточно давно применяется в реализациях, но не была включена в RFC 2409 (IKE). Реализации применяли для обозначения данной группы номер 5, который стандартизуется в этом документе.

Простое число

```
2^1536 - 2^1472 - 1 + 2^64 * { [2^1406 pi] + 741804 }
```

[1]Modular Exponential.
[2]Internet Key Exchange.
[3]Advanced Encryption Standard — прогрессивный стандарт шифрования.

Шестнадцатеричное представление

```
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
```

Генератор - 2.

3. 2048-битовая группа MODP

Этой группе присвоен номер 14.

Простое число

```
2^2048 - 2^1984 - 1 + 2^64 * { [2^1918 pi] + 124476 }
```

Шестнадцатеричное представление

```
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 8AACAA68 FFFFFFFF FFFFFFFF
```

Генератор - 2.

4. 3072-битовая группа MODP

Этой группе присвоен номер 15.

Простое число

```
2^3072 - 2^3008 - 1 + 2^64 * { [2^2942 pi] + 1690314 }
```

Шестнадцатеричное представление

```
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
```

Генератор - 2.

5. 4096-битовая группа MODP

Этой группе присвоен номер 16.

Простое число

```
2^4096 - 2^4032 - 1 + 2^64 * { [2^3966 pi] + 240904 }
```

Шестнадцатеричное представление

```
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 1FBECAA6
287C5947 4E6BC05D 99B2964F A090C3A2 233BA186 515BE7ED
1F612970 CEE2D7AF B81BDD76 2170481C D0069127 D5B05AA9
93B4EA98 8D8FDDC1 86FFB7DC 90A6C08F 4DF435C9 34063199
FFFFFFFF FFFFFFFF
```

Генератор - 2.

6. 6144-битовая группа MODP

Этой группе присвоен номер 17.

Простое число

```
2^6144 - 2^6080 - 1 + 2^64 * { [2^6014 pi] + 929484 }
```

Шестнадцатеричное представление

```
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 1FBECAA6 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
```

Генератор - 2.

7. 8192-битовая группа MODP

Этой группе присвоен номер 18.

Простое число

```
2^8192 - 2^8128 - 1 + 2^64 * { [2^8062 pi] + 4743158 }
```

Шестнадцатеричное представление

```
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 1FBECAA6
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
```

Генератор - 2.

8. Вопросы безопасности

Этот документ описывает новые более сильные группы для применения в IKE. Стойкость определенных здесь групп оценивалась многократно, но методов оценки существует столько же, скольку существует криптографов. Для приведенных в таблице оценок взяты крайние из известных значений оценок.

Группа	Модуль (в битах)	Оценка стойкости 1		Оценка стойкости 2	
		в битах	размер показателя	в битах	размер показателя
5	1536	90	180-	120	-240
14	2048	110	220-	160	320-
15	3072	130	260-	210	420-
16	4096	150	300-	240	480-
17	6144	170	340-	270	540-
18	8192	190	380-	310	620-

9. Согласование с IANA

В IKE [RFC-2409] определены 4 группы Diffie-Hellman с номерами от 1 до 44.

Этот документ определяет новые группы 5 и 14 - 18. Запросы на выделение новых значений выполнены по процедуре IETF Consensus, как описано в RFC 2434 [RFC-2434]. Предполагается, что новые группы будут документированы в разрабатываемых RFC категории Standards Track.

10. Нормативные документы

[RFC-2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409[1], November 1998.

[RFC-2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

11. Дополнительная литература

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

[RFC-2412] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[Orman01] Orman, H. and P. Hoffman, "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", Work in progress[2].

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

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

[1]Документ признан устаревшим и заменен RFC 4306, а затем - RFC 5926 и RFC 7996. *Прим. перев.*
[2]Работа завершена и опубликована в RFC 3766. *Прим. перев.*

12. Адрес авторов

Tero Kivinen

SSH Communications Security Corp

Fredrikinkatu 42

FIN-00100 HELSINKI

Finland

EMail: kivinen@ssh.fi

Mika Kojo

HELSINKI

Finland

EMail: mika.kojo@helsinki.fi

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

13. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.