

IP Security Protocol Working Group (IPSEC)
INTERNET-DRAFT
[draft-ietf-ipsec-ike-modp-groups-04.txt](#)
Expires: 13 June 2002

T. Kivinen
and M. Kojo
SSH Communications Security
13 December 2001

More MODP Diffie-Hellman groups for IKE

Status of This Memo

This document is a submission to the IETF IP Security Protocol (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@lists.tislabs.com) or to the editor.

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document defines new MODP groups for the IKE [[RFC-2409](#)] protocol. It documents the well know and used 1536 bit group 5, and also defines new 2048, 3072, 4096, 6144, and 8192 bit Diffie-Hellman groups. The selection of the primes for theses groups follows the criteria established by Richard Schroepel as described in [[RFC-2412](#)].

Table of Contents

1.	Introduction	2
2.	Specification of Requirements	2
3.	1536-bit MODP Group	2
4.	2048-bit MODP Group	3
5.	3072-bit MODP Group	3
6.	4096-bit MODP Group	4
7.	6144-bit MODP Group	4
8.	8192-bit MODP Group	5
9.	Security Considerations	6
10.	References	7
11.	Authors' Addresses	7

[1.](#) Introduction

Current Diffie-Hellman groups defined in the IKE [[RFC-2409](#)] have only strength that matches strength of symmetric key of 70-80 bits. The new AES cipher needs stronger groups. For the 128-bit AES we need about 3200-bit group [[Orman01](#)]. The 192 and 256-bit keys would need groups that are about 8000 and 15400 bits respectively. Another source [[RSA13](#)] [[Rousseau00](#)] estimates that the security equivalent key size for the 192-bit symmetric cipher is 2500 bits instead of 8000 bits, and the equivalent key size 256-bit symmetric cipher is 4200 bits instead of **[15400](#) bits**.

Because of this disagreement this document just specifies different groups without specifying which group should be using 128, 192 or 256-bit AES. In the current hardware groups bigger than 8192-bits are too slow for practical use, thus this document does not provide any groups bigger than 8192-bits.

Also the exponent size used in the Diffie-Hellman must be selected so that it matches other parts of the system. The exponent size should be selected so that it is not the weakest link in the security system, meaning that it should be at least the double of the estimated strength of selected group. I.e if you use group whose strength is 128 bits, you must use more than 256 bits of randomness in the exponent used in the Diffie-Hellman calculation.

[2.](#) Specification of Requirements

This document shall use the keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" to describe requirements. They are to be interpreted as described in [[RFC-2119](#)] document.

[3.](#) 1536-bit MODP Group

The 1536 bit MODP group has been used for the implementations for quite a long time, but it has not been documented in the current RFCs or

[I. Kivinen, et. al.](#)

[page 2]

drafts. This group has already been used as having group id 5.

The prime is: $2^{1536} - 2^{1472} - 1 + 2^{64} * \{ [2^{1406} \text{ pi}] + 741804 \}$
 Its hexadecimal value is

```

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

```

The generator is: 2.

4. 2048-bit MODP Group

This group is assigned id XX.

This prime is: $2^{2048} - 2^{1984} - 1 + 2^{64} * \{ [2^{1918} \text{ pi}] + 124476 \}$
 Its hexadecimal value is

```

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

```

The generator is: 2.

5. 3072-bit MODP Group

This group is assigned id XX + 1.

This prime is: $2^{3072} - 2^{3008} - 1 + 2^{64} * \{ [2^{2942} \text{ pi}] + 1690314 \}$
 Its hexadecimal value is

```

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

```

The generator is: 2.

6. 4096-bit MODP Group

This group is assigned id XX + 2.

This prime is: $2^{4096} - 2^{4032} - 1 + 2^{64} * \{ [2^{3966} \text{ pi}] + 240904 \}$
 Its hexadecimal value is

```

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

```

The generator is: 2.

7. 6144-bit MODP Group

This group is assigned id XX + 3.

This prime is: $2^{6144} - 2^{6080} - 1 + 2^{64} * \{ [2^{6014} \text{ pi}] + 929484 \}$
 Its hexadecimal value is

```

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

```

The generator is: 2.

8. 8192-bit MODP Group

This group is assigned id XX + 4.

This prime is: $2^{8192} - 2^{8128} - 1 + 2^{64} * \{ [2^{8062} \text{ pi}] + 4743158 \}$

Its hexadecimal value is

```

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

```

The generator is: 2.

9. Security Considerations

This document describes new stronger groups to be used in the IKE. The strengths of the groups defined here is always an estimate and there are as many methods to estimate them as there are cryptographers. For the strength estimates below we took the both ends of the scale so the actual strength estimate can be between those two numbers given here.

+-----+-----+-----+-----+-----+					
Group	Strength Estimate 1		Strength Estimate 2		
	+-----+-----+-----+-----+				
		exponent		exponent	
	in bits	size	in bits	size	
+-----+-----+-----+-----+-----+					
1536-bit	90	180-	120	240-	
2048-bit	110	220-	160	320-	
3072-bit	130	260-	210	420-	
4096-bit	150	300-	240	480-	
6144-bit	170	340-	270	540-	
8192-bit	190	380-	310	620-	

+-----+-----+-----+

ECPP certificats for all primes p and $p-1/2$ can be found from the
<http://ftp.ssh.com/pub/ietf/ecpp-certificates/>.

[T. Kivinen](#), et. al.

[page 6]

10. References

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

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

[RFC-2119] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", March 1997

[Orman01] Orman, H., Hoffman, P. "Determining Strengths For Public Keys Used For Exchanging Symmetric Keys", November 2001, Work in progress, [draft-orman-public-key-lengths-04.txt](#).

[RSA13] Silverman, R. "RSA Bulleting #13: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths", April 2001, <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>

11. Authors' Addresses

Tero Kivinen
SSH Communications Security Corp
Fredrikinkatu 42
FIN-00100 HELSINKI
Finland
E-mail: kivinen@ssh.fi

Mika Kojo
HELSINKI
Finland
E-mail: mrskojo@cc.helsinki.fi

