IJITKM Volume 7 • Number 2 Jan– June 2014 pp. 188-194 (ISSN 0973-4414)

Enhancing security by Authenticating the Diffie-Hellman Key Exchange Algorithm using RSA

Ritu Makani[1] · Navpreet Kaur[2]
1 Asst. Professor,Dept. of Computer Science & Engg.,GJUS&T, Hisar
2 M.Tech research student(CSE),GJUS&T, Hisar
ritu_nagpal22@yahoo.co.in, nav.waraich15@gmail.com

Abstract
The ability to distribute cryptographic keys has been a challenge for centuries. The Diffie-Hellman was the first practical solution to the problem. Diffie-Hellman is designed to provide two systems to share a secret key that can be used later. However, if the key exchange takes place in certain mathematical environment a very serious problem may occur during key exchange that problem is called Man-in-Middle Attack problem. This paper is an effort to solve this serious problem in Diffie-Hellman key exchange so that the algorithm can be made secure. In this paper we have used RSA algorithm along with Diffie-Hellman to solve the problem. We explore the Man-in-Middle attack, analyse the countermeasures against the attack.
Index Terms: Cryptography, Diffie-Hellman, Man-in-Middle attack, primality testing, discrete logarithm.

Introduction

Cryptography and encryption/decryption methods fall into two main Categories: symmetric and public key. In symmetric cryptography, sometimes called classical cryptography, parties share the same encryption/decryption key. Therefore, before using a symmetric cryptography system, the users must somehow come to an agreement on a key to use. An obvious problem arises when the parties are separated by large distances which is commonplace in today's worldwide digital communications. If the parties did not meet prior to their separation, how do they agree on the common key to use in their cryptosystem without a secure channel? They could send a trusted courier to exchange keys, but that is not feasible, if time is a critical factor in their communication.

The problem of securely distributing keys used in symmetric ciphers has challenged cryptographers for hundreds of years. If an unauthorized user gain access to the key, the cryptographic communication must be considered broken. Amazingly, in 1977, Whitfield Diffie and Martin Hellman published a paper in which they presented a key exchange protocol that provided the first practical solution to this dilemma. The protocol, named the Diffie-Hellman key exchange(or key agreement) protocol in their honour, allows two parties to derive a common secret key by communications over an unsecured channel, while sharing no secret keying material at prior .

Before conducting the key exchange using the Diffie-Hellman protocol, the parties must agree on a prime number that defines the mathematical environment in which the key exchange will take place. If the prime number is large enough, a brute force attack to find the secret key becomes infeasible. However, if the two parties agree on certain prime numbers, an active adversary can compromise their communication.

This paper investigates the Diffie-Hellman protocol and the difficulty of the discrete logarithm problem the protocol relies on. We then analyse the man-in-middle attack described above by developing an algorithm to conduct the attack. We then consider methods to defend against the attack and demonstrate their effectiveness.

BACKGROUND AND REVIEW

Before beginning a discussion of the Diffie-Hellman protocol and the man-in-middle attack, we investigate and present some basic definitions and theorems. This information is available in any standard algebra text, such as Fraleigh's Abstract Algebra, or discrete mathematics text, such as Rosen's Discrete Mathematics and Its Applications. It is assumed the reader is familiar with common mathematical, logical, and set notation.

NUMBER THEORY

If a and b are integers, then a is congruent to b modulo m if m divides a -b. We use the notation $a \equiv b \ (mod m)$ to indicate that a is congruent to b modulo m.

The great French mathematician *Pierre de Fermat (1601–1655)*demonstrated that the congruence$a^{p-1}=1 \ (mod \ p)$holds when p is a prime, and this gives us a theorem that will prove crucial in our analysis of the man-in-the-middle attack.

Fermat's Theorem: If $a \in Z$ and p is a prime not dividing a, then p divides a^{p-1}, that is,

$$a^{p-1} \equiv 1 \ (mod \ p)$$

Euler gave a generalization of Fermat's theorem, but we must first define Euler's Totient Function. Commonly referred to as Euler's Phi Function, the function gives the number of integers less than or equal to n which are relatively prime to n , and is denoted by $\phi(n)$. It is not hard to show that, if

$$n=\prod_{i=1}^{k} P_i^{\alpha i} \quad ,then$$

$$\phi(n)=n \prod_{i=1}^{k} P_i^{\alpha i} (1-1/P_i)$$

Euler's Theorem: If $a \in Z$ and is relatively prime to n, then $a^{\phi(n)}- 1$isdivisible by n, that is,

$a^{\varphi(n)} \equiv 1 \pmod{n}$.

GROUP THEORY

A **group** <G,*>is a set *G* which is closed under a binary operation *, such that the following conditions are satisfied:

Associativity: For all $a,b,c \in G$ $a*(b*c)=(a*b)*c$
Identity: There is an element *e* in *G* such that *for all* $a \in Z$
$a*e=e*a=a$
Inverse: Corresponding to each $a \in G$, there exist an element a' such that
$a*a'=a'*a=e$

If the set *G* has a finite number ofelements. In this case, the number of elements is called the ***order*** of *G*, denoted by $|G|$.
If *n* is a prime *p*, then the set $Z^*_p=Z_p-\{[0]_p\}$forms a group under multiplication modulo *n* . The Diffie-Hellman key exchange protocol sets this group as the environment for the key agreement.

Sub Group

Let G be a group and H be its subset. The subset H is called subgroup of G if following conditions are satisfied.
1. if a, b $\in$ H, the product ab also belongs to H.
2. e(identity element of G) belongs to H.
3.if a $\in$ H its inverse also belongs to H.

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Table 4. Group Table for $<Z^*_p, \bullet>$

The group $<Z^*_p, \bullet>$is always cyclic. An important property of cyclic groups is that every subgroup of a cyclic group is also cyclic. Another important property of groups in general is the Theorem of Lagrange.

Lagrange's Theorem: *Let H be a subgroup of a finite group G.*
Then the order of H is a divisor of the order of G.

Groups of Prime Order

A group g is called a group of prime order if it is:
1. a cyclic group having a prime number as its order.
2. isomorphic to the quotient of group of integers by a subgroup generated by a prime.
3. a simple abelian group.
4. adittive group of finite prime field.

The number of distinct subgroups of a group are either 0 or congruent to 1(mod p).
Let G be a group and H, K be its subgroups each of order p, where p is a prime then,
$H \cap K = \{e\}$ or H=K.

Field Theory

A field $<F, +, .>$, is a set *F* together with two binary operations, which we
will call addition and multiplication, defined on *F* such that the following axioms are satisfied:

Addition: $<F, +>$is an abelian group.
Multiplication: $<F^*, .>$is an abelian group.
Distributive: For all $a,b, c \in F$, $a . (b + c) = (a . b) + (a . c)$.

A field *F* is said to be a ***finite field***, if the set *F* has a finite number of elements.
If *F* is a finite field, then the multiplicative group is cyclic.

PRIMALITY TESTING

A ***primality test*** is an algorithm used for determining whether an input number is prime. Primality tests can be divided into two main groups: deterministic and probabilistic. Deterministic primality tests prove with certainty whether a number is prime or composite. Probabilistic primality tests tell us a number is composite or *probably* prime.

Miller-Rabin Primality Test

The Miller-Rabin Primality Test is an efficient probabilistic algorithmto test for primality based on the idea of strong pseudoprimes. Consider an odd composite number *n* and $n - 1 = d \cdot 2^s$with *d* odd. *n* is a ***strong pseudoprime*** if either
$a^d \equiv 1 \pmod{n}$ or $a^{d.2r} \equiv -1 \pmod{n}$ with $r = 0,1,\ldots s - 1$. The Carmichael numbers are Fermat pseudoprimes for every base. However, a composite number can only be a strong pseudoprime to at most one quarter of all bases.

The algorithm is as follows:
Choose a random integer $a \in [2, n - 2]$. If $a^d \neq 1 \pmod{n}$ and $a^{d.2r} \neq -1 \pmod{n}$ for all
$r = 0,1,\ldots s - 1$, then *a is called a witness and n is composite*. Otherwise, *n* is a strong probable prime to

base *a*.If *n* >9 and is odd composite, the probability that the algorithm will fail to produce a witness for *n* is <1/ 4. The probability that we fail to find a witness after *k* iterations is <1/ 4^k. We can make this probability as small as we desire with a large number of iterations. For instance, if we wanted to ensure the probability of calling a composite number a prime is less than 10^{-6}, we must compute 10 iterations or more.
The Miller-Rabin test is very fast and has a complexity of$O((\log n)^3)$. Of course, because it is probabilistic, there is a chance of the test returning a number as prime when it is in fact composite. The Miller-Rabintest offers us both speed, as compared to other primality tests, and the ability to control the probability of error and will be our tool of choice.

DIFFIE-HELLMAN PROTOCOL

The parameters of the protocol are: *p*, a large prime and *g*, a primitive element of Z_n. This means that all numbers n=1, ... , p-1 can be represented as $n = g^i$. These two numbers do not need to be kept secret. For example, Alice could send them to Bob in the open. The protocol runs as follows:

1. Alice choses a large random integer *x* and sends Bob
$X=g^x \bmod p$
2. Bob choses a large random integer *y* and sends Alice
$Y=g^y \bmod p$
3. Alice computes
$k=Y^x \bmod p$
4. Bob computes
$k=X^y \bmod p$

k is the key. *k* is equal to $g^{xy} \bmod p$.

Both Alice and Bob have arrived at the same value, because $(g^a)^b$ and $(g^b)^a$ are equal mod *p*. Note that only *a*, *b*, and *($g^{ab} \bmod p = g^{ba} \bmod p$)* are kept secret. All the other values – *p*, *g*, $g^a \bmod p$, and $g^b \bmod p$ – are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel.

Example 1.1
A simple example of Diffie-Hellman Key Exchange Protocol is as follows:

1. Alice and Bob agree to use a prime number *p* = 23 and base *g* = 5.
2. Alice chooses a secret integer $\boldsymbol{a} = \mathbf{6}$, then sends Bob $A = g^{\boldsymbol{a}} \bmod p$
   - $A = 5^{\mathbf{6}} \bmod 23 = 8$
3. Bob chooses a secret integer $\boldsymbol{b} = \mathbf{15}$, then sends Alice $B = g^{\boldsymbol{b}} \bmod p$
   - $B = 5^{\mathbf{15}} \bmod 23 = 19$
4. Alice computes $\boldsymbol{s} = B^{\boldsymbol{a}} \bmod p$
   - $\boldsymbol{s} = 19^{\mathbf{6}} \bmod 23 = \mathbf{2}$
5. Bob computes $\boldsymbol{s} = A^{\boldsymbol{b}} \bmod p$
   - $\boldsymbol{s} = 8^{\mathbf{15}} \bmod 23 = \mathbf{2}$
6. Alice and Bob now share a secret (the number **2**).

RSA Algorithm

The most famous of the public key cryptosystem is RSA which is named after its three developers Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA cryptosystem is a public-key cryptosystem, widely used for secure communication and e-commerce applications. It is often used to encrypt messages sent between two communicating parties so that an eavesdropper who overhears the conversation cannot decode them easily. It also enables a party to append an unforgeable signature to the end of a message. This signature cannot be easily forged and can be checked by anyone.
The basic RSA cryptosystem is completely specified by the following sequence of steps.

1. Alice selects at random two large primes p and q.
2. Alice computes n = pq.
3. Alice selects a small odd integer e that is relatively prime to
(p – 1)(q – 1).
4. Alice sets d so that de mod (p – 1)(q – 1) equals 1.
5. Alice publish the pair (e, n) as the public key, with $P_A(M) = M^e \bmod n$.
6. Alice stores the pair (d, n) as the secret key, with $S_A(E) = E^d \bmod n$.

In order to send message M in {0, 1, . . . , n–1}, Bob sends $P_A(M) = M^e \bmod n$. On receiving the encrypted message Alice computes $S_A(P_A(M)) = M^{de} \bmod n$. Our choices of d, e, and n ensure that $M^{de} \bmod n$ equals M.

THE DISCRETE LOGARITHM
Eve can have more information than just the fact that the key resides in the interval
(1, *p* -1). Because the exchange occurs over an open channel, Eve knows α^x and α^y as well. If $\beta \equiv \alpha^x \pmod p$ and $\gamma \equiv \alpha^y \pmod p$, then *p* ,α ,β and γ are known. All Eve has to do is solve $\alpha^x \equiv \beta \pmod p$for *x* or $\alpha^y \equiv \gamma \pmod p$ for *y*. Once *x* or *y* are known, Eve simply raises α^x to *y* or α^y to *x* and arrives at the secret key *K* . However, if *p* is large, solving $\alpha^x \equiv \beta \pmod p$ for *x* in general is considered difficult. The problem of finding *x* if α^x is known as the ***discrete logarithm problem*** (DLP), often abbreviated $x=L_\alpha(\beta)$.

Diffie-Hellman Problem
The Diffie-Hellman Problem is of two types, the computational and the decisional. The ***Computational Diffie-Hellman Problem*** is defined as follows: Let *p* be

a prime and let α be a primitive root mod p . Given $\alpha^x \pmod p$ and $\alpha^y \pmod p$, find $\alpha^{xy} \equiv \beta \pmod p$. Recall that Eve has access to both α^x and α^y as they are both made public during the exchange. It is not currently known whether or not this problem is easier than computing discrete logs A related problem, known as the ***Decisional Diffie-Hellman Problem***, is defined as follows: Let p be a prime and let α be a primitive root mod p . Given $\alpha^x \pmod p$ and $\alpha^y \pmod p$, and $\beta \neq 0 \pmod p$, decide whether or not $K \equiv \alpha^{xy} \pmod p$. In other words, if someone offers a number to Eve and claims it is K, can Eve decide whether or not that person is telling the truth with the information captured in the open channel?

Solving these problems Eve can attack the Diffie-Hellman Key Exchange protocol. It may either pretend to be sender or it may alter the messages between the two clients also, it may simply hear to the conversation and compromise the privacy of the communication.

Bits	**Digits(approximate)**	**PC Time (approximate)**	**SC Time (approximate)**
64	19	317,098 years	115 days
128	39	3 x 10^(25) years	3 x 10^(19) years
256	77	3 x 10^(63) years	3 x 10^(57) years
512	154	3 x 10^(140) years	3 x 10^(134) years
1024	308	3 x 10^(294) years	3 x 10^(288) years
2048	616	3 x 10^(602) years	3 x 10^(596) years

Table 2. Times to Exhaust Key Space

MAN-IN-THE-MIDDLE ATTACK

THEORY BEHIND THE ATTACK

Wiener and Van Orschot noted that, if certain primes are used, a potentially fatal protocol attack on the Diffie-Hellman key exchange protocol becomes possible. The idea is based on forcing the parties to agree on a shared key that resides in a subgroup of the cyclic group Z^*_p. If the order of the subgroup is small enough, an adversary can exhaustively search the subgroup, retrieve the secret key, and eavesdrop on the communication of Alice and Bob.

For instance, consider the case when the prime used for the key exchange is of the form $p = 2q + 1$, where q is a prime. Then, $\alpha^q = \alpha^{(p-1)/2}$.

We now generalize the situation if Alice and Bob use a prime number of the form

$p = Rq + 1$, where R is a small integer and q is again a large prime.

Claim: $\alpha^{(p-1)/R}$ *is an element of order R.*

Proof: Raising $\alpha^{(p-1)/R}$ to consecutive powers, starting with 0, we get:

$(\alpha^{(p-1)/R}) = 1, (\alpha^{(p-1)/R})^2, (\alpha^{(p-1)/R})^3, \ldots, (\alpha^{(p-1)/R}) = \alpha^{p-1} = 1$

This produces a list of R different values. Continuing after R ,

$(\alpha^{(p-1)/R})^{(R+1)} = (\alpha^{(p-1)/R})^R . (\alpha^{(p-1)/R}) = 1.(\alpha^{(p-1)/R})$,

$(\alpha^{(p-1)/R})^{(R+2)} = (\alpha^{(p-1)/R})^R . (\alpha^{(p-1)/R})^2 = 1. (\alpha^{(p-1)/R})^2, \ldots\ldots$,

$(\alpha^{(p-1)/R})^{(R+n)} = (\alpha^{(p-1)/R})^R . (\alpha^{(p-1)/R})^n = 1.(\alpha^{(p-1)/R})^n$

For $n < R$, the results are in the original list.

For $n \geq R$, we can write $R + n = R + kR + m$ *with* $0 \leq m \leq R - 1$ *and* $m, k \in \mathbf{Z}$.

$(\alpha^{(p-1)/R})^{(R+n)} = (\alpha^{(p-1)/R})^{(R+kR+m)} = (\alpha^{(p-1)/R})^R . (\alpha^{(p-1)/R})^{kR} . (\alpha^{(p-1)/R})^m =$

$1.1^k . (\alpha^{(p-1)/R})^m = (\alpha^{(p-1)/R})^m$

Because $0 \leq m \leq R - 1$, this is in our original list and $\alpha^{(p-1)/R}$ is of order R .

So, if the prime Alice and Bob agree to use is of the form $p = Rq + 1$, Evecan force them to agree on a key in a subgroup of Z^*_p of order R by replacing α^x and α^y with $(\alpha^x)^q$ and $(\alpha^y)^q$. Even if Alice and Bob are vigilant, the key can take any of R values and the generalized attack poses a significant threat to an unauthenticated key exchange using the Diffie-Hellman protocol.

COUNTERMEASURES AGAINST THE ATTACK

To prevent this potentially fatal protocol attack, several options can be chosen. The easy and efficient method is to force authentication prior to the key exchange.

Authentication

The attack we have discussed is not the only man-in-the-middle attack Diffie -Hellman is vulnerable to. To combat this attack, a variation of Diffie-Hellman that

ensures authentication can be used. Diffie-Hellman protocol that allows the establishment of a shared secret key between two parties with mutual authentication. The method employs digital signatures. A digital signature of a message is a number dependent on some secret known only to the signer; and, additionally, on the content of the message being signed. The STS protocol is frequently employed with the RSA signature scheme.
To employ an RSA signature scheme, public and private key pairs must first be generated.

RSA signature scheme key generation steps:
1. Generate two large distinct random primes p and q, each roughly of the same size
2. Compute $n = pq$ and $\Box = (p-1)(q-1)$
3. Select a random integer $e, 1 < e < \Box$, such that $\gcd(e, \Box) = 1$
4. Use the extended Euclidean algorithm to compute the unique integer $d, 1 < d < \Box$ such that $ed = 1 \pmod{\Box}$
5. The user's public key is (n, e) and the user's private key is d

It is important to note that each user should generate a public and private key
let E denote a symmetric encryption
algorithm, and $S_A(m)$ denote Alice's signature on m, the protocol is as follows

Set up:
a. A prime number p and generator α of $Z^*_p (2 \le \alpha \le p-2)$ are selected and published
b. Alice selects RSA public and private signature keys (n_A, e_A) *and* d_A (Bob selects analogous keys). Assume each party has access to authentic copies of the other's public key.

Actions:
a. Alice generates a secret random $x, 1 \le x \le p-2$, encrypts the message with its signatures and sends to Bob $E_{SA}(a^x \bmod p)$.
$A \rightarrow B$: $E_{SA}(a^x \bmod p)$.
b. Bob decryptes message using public key of Alice.
c. Bob generates a secret random $y, 1 \le y \le p-2$, and computes the shared key $K = (a^x)^y \bmod p$. Bob encrypts the message using its signatures and sends to Alice $E_{SB}(a^y \bmod p)$.
$B \rightarrow A$: $E_{SB}(a^y \bmod p)$
d. Alice computes the shared key $k = (a^y)^x \bmod p$, decrypts the encrypted data, and uses Bob's public key to verify the received value as the signature on the hash of the cleartext

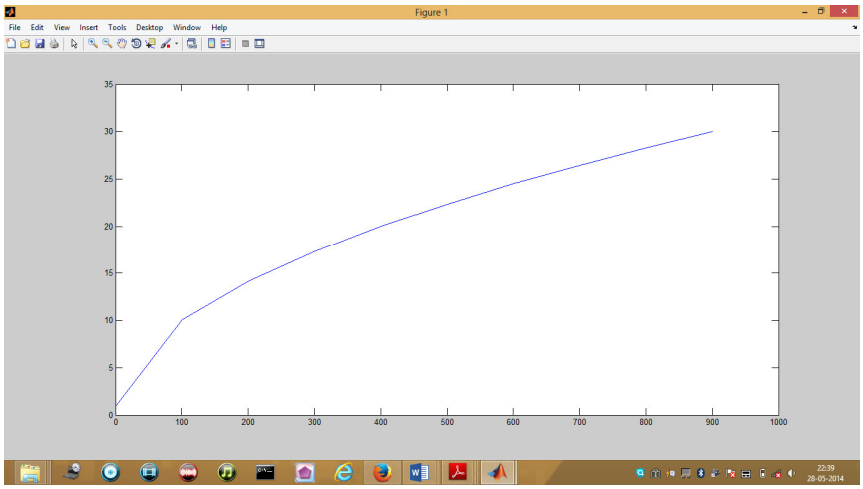
Upon successful verification, Alice and Bob accepts k that is actually shared with Bob, and sends Bob an analogous message.

Eve cannot alter the original exponentials without triggering a failure during Alice and Bob's key agreement. This precludes the man-in-middle attack we have focused on and defends Alice and Bob's key exchange against several other possible active man-in-middle attacks.

Results and Conclusions
Here we have investigated and analysed man-in-the-middle attack on the Diffie-Hellman key exchange protocol. In particular, if the Miller-Rabin primality test is used, for attack the algorithm's complexity is $O((\log N)^3)$ with N being the input prime number.. We demonstrated a technique, authentication that can prevent the attack. In fact, it appears industry has begun to adopt the prime order subgroup technique to defend against the attack. It is possible that analysing the given prime number, capturing the required messages, altering those messages, and forwarding the messages to the intended recipients will be too time-consuming. This would obviously alert the parties of possible compromise.

For example eve can try man in middle attack in 2 ways.
1. He can try to send messages to bob pretending that the message is sent by the alice but, he will fail because bob can easily know that the message is not being sent by alice.
2. He can try to manipulate the message and send the manipulated message to bob, when bob recieves the method he will find that this is not the true message because signature of the message do not match with the signature of alice.
In this way we can make the key exhange free from man-in-middle attack.

Below is the graph of complexity of Attack Algorithm. Since we have used the Miller-Rabin Primality test so, the complexity of Attack Algorithm will be $O((\log N)^3)$.
The Complexity of proposed method depends upon the key size used the recommended Key size is of 1024 bits. So that the Key Exchange becomes an extremely secure process and no one can compromise the privacy of the users.



Graph of complexity of Attack Algorithm

Example of the implementation of the proposed method is:

the value of p is: 65537
the value of q is: 1073

The value of (N) is: 70321201
The public key (e) is: 3
The value of (Phi) is: 70254592
The private key (d)is: 46836395

Implementation of Diffie-Hellman algorithm

value of prime number pr is: 65537
primitive root of pr is(α):
3
the value of prime number x: 17

the key value to be send is:
32273

Cipher Text of the entered Message:
15767613

Decrypted Message is:
32273

Another example of implementation can be the following:

the value of p is: 173
the value of q is: 139

The value of (N) is: 24047
The public key (e) is: 5
The value of (Phi) is: 23736
The private key (d)is: 18989

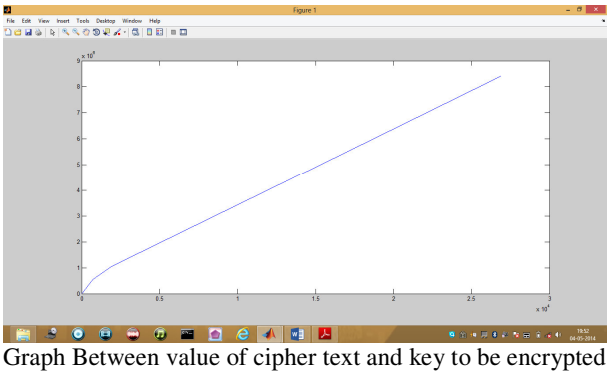
Implementation of Diffie-Hellman algorithm

value of prime number pr: 17
primitive root of pr is:
3

Enter the value of prime number x: 3
the key value to be send is:
10

Cipher Text of the entered Message:
3812

Decrypted Message is:
10



Graph Between value of cipher text and key to be encrypted

LIST OF REFERENCES

[1] A. J. Menezes, P. C. van Oorshot, and S. A Vanstone, *Handbook of Applied Cryptography*. CRC Press, New York, New York, 1997.
[2] P. C. van Oorschot and M. J. Wiener, On Diffie-Hellman Key Agreement with Short Exponents. *EUROCRYPT'96*, LNCS 1070, Springer-Verlag, 1996, pp. 332–343.
[3] S. Singh, *The Code Book*. Doubleday, 1999.
[4] J. B. Fraleigh, *A First Course in Abstract Algebra.* Addison-Wesley, San Francisco, CA, 7th Edition, 2002.
[5] K. H. Rosen, *Discrete Mathematics and Its Applications*. McGraw Hill, San Francisco, CA, 6th Edition, 2007.
[6] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*. Springer, New York, NY, 2001.
[7] A. L. Atkin and F. Morain, Elliptic Curves and Primality Proving. *Res. Rep.* 1256, INRIA, June 1990.
[8] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P. *Annals of Mathematics 160.* 2004.
[9] C. Pomerance and H.W. Lenstra, Primality testing with Gaussian periods, preprint.
[10] W. Diffie and M. E. Hellman, *New Directions in Cryptography*. IEEE IT- 22, 1976, pp. 644–654.
[11] W. Trappe and L. Washington, *Introduction to Cryptography with Coding Theory.* Pearson, Upper Saddle River, NJ, 2nd Edition, 2006.
[12] S. Pohlig and M. Hellman, An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance. *IEEE Transactions on Information Theory,* 24, 1978, pp. 106–110.
[13] T. Agoh, On Sophie Germain Primes. *Tatra Mt. Math.* Publ. 20, 2000.
[14] P. Stanica, private communication, 2009.
[15] Internet Engineering Task Force (IETF) Request for Comment (RFC) 2631, June 1999.