International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-08, Nov 2017

An Approach to Public-Key Cryptography using Diffie - Hellman Key Exchange Algorithm

[1]Dr. S. V. B. Subrahmanyeswara Rao, [2]Mrs. Yalamanchili. Anjani

[1]Assoc. Professor, Ramachandra College of Engineering, Eluru,A.P.India.

[2]Assoc. Professor VKR,VNB& AGK College of Engineering, Gudivada, A.P.India.

Abstract-The ability to distribute cryptographic keys has been a challenge for centuries. The Diffie-Hellman was the first practical solution to the problem. However, if the key exchange takes place in certain mathematical environments, the key exchange become vulnerable to a specific Man-in-Middle attack, first observed by Vanstone. This paper is an effort to solve a serious problem in Diffie-Hellman key exchange, that is, Man-in-Middle attack. 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.

Key Words-Cryptography, Diffie-Hellman, Man-In-Middle Attack, Primality Testing.

I. INTRODUCTION

Cryptography and encryption/decryption methods fall into two broad 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 crypto system 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 gains 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 .

This paper investigates the Diffie-Hellman protocol and the difficulty of the discrete logarithm problem the protocol relies on. We then analyze 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.

II.BACKGROUND AND REVIEW

Modular Arithmetic:

Given any positive integer *n* and any non-negative integer *a*, if we divide *a* by *n*, we get an integer quotient q and an remainder *r* that obey following relationship:

$$a = qn + r, \quad 0 \le r \le n; \quad q = \lfloor a/n \rfloor$$

Where $\lfloor x \rfloor$ is largest integer less than or equal to *x*

FIG shows the relationship $a = qn + r,\ 0 \le r \le n;$

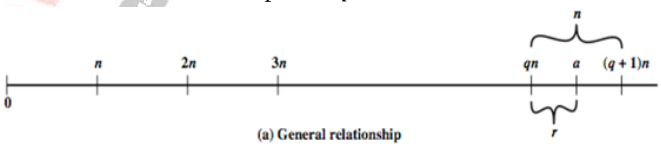

Fig. 1 General Relationship

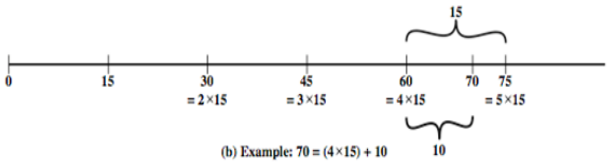

Fig. 2 Example

The Modulus

If *a* is an integer and *n* is a positive integer, we define *a mod n* to be the remainder when *a* is divided by *n*. Integer is called the Modulus.

Thus, for any integer ,

$$a = qn + r, \quad 0 \le r \le n; \quad q = \lfloor a/n \rfloor$$
$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

Ex: 11 mod 7 = 4;

- 11 mod 7 = 3

$a = -11\ n = 7$

 DOI : 10.18231/2454-9150.2017.0044

$a = qn + r\,, \quad 0 \le r \le n; \quad q = \lfloor a/n \rfloor$
$q = \lfloor a/n \rfloor = \lfloor -11/7 \rfloor = -2$
$a = qn + r$
$-11 = -2.7 + r$
$-11 + 14 = r$
$r = 3$

Note: Two integers and are said to be C*ongruent modulo n*, if $(a \bmod n) = (b \bmod n)$.This is written as $a \equiv b \pmod n$.
Ex:
$73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$
Note: If $a \equiv 0 \pmod n$, then n/a.

Properties of Congruences
Congruences have the following properties:
1. $a \equiv b \pmod n$, then $n/(a-b)$.
2. $a \equiv b \pmod n$ implies b $\equiv a \pmod n$.
3. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$.
Ex:
$23 \equiv 8 \pmod 5$; $a = 23, b = 8, n = 5$ *and*
$a - b = 23 - 8 = 15 = 5 * 3 = n * 3$
$-11 \equiv 5 \pmod 8$;
$-11 - 5 = -16 = 8 * (-2)$
$81 \equiv 0 \pmod{27}$; $81 - 0 = 81 = 27 * 3$

Modular Arithmetic Operations
(mod n) operator maps all integers into the set of integers $\{0, 1, - - -, (n-1)\}$.
Can we perform arithmetic operations within the confines of this set?
It turns out that we can; this technique is known as *Modular arithmetic*.

Modular arithmetic exhibits the following properties:
1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
Examples of the three properties:
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = (3+7) \bmod 8$
$= 2$ *or*
$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$
$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8$
$= -4 \bmod 8 = 4\,(11 - 15) \bmod 8 = -4 \bmod 8 = 4$
$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8$
$= 21 \bmod 8 = 5\,(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$
Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.
To find 11^7 mod 13, we can proceed as follows:
$11^2 = 121 \equiv 4 \pmod{13}$
$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
$11^7 \equiv 11 \times 4 \times 3 \equiv 121 \equiv 2 \pmod{13}$

Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

W	-	w^{-1}
0	**0**	**0**
1	**7**	**1**
2	**6**	-
3	**5**	**3**
4	**4**	-
5	**3**	**5**
6	**2**	-
7	**1**	**7**

Table. 1 Additive and multiplicative inverses modulo 8

In this case(Table.1), the negative of an integer *x* is the integer *y* such that $(x + y) \bmod 8 = 0$.
To find Additive inverse of an integer in the left-hand column, scan across the corresponding row of the matrix to find the value 0; the integer at the top of that column is additive inverse; $(2 + 6) \bmod 8 = 0$.
Now, to find the multiplicative inverse of an integer from the multiplication table, scan across the matrix in the row for that integer to find the value 1; the integer at the top of that column is the multiplicative inverse; thus, $(3 \times 3) \bmod 8 = 0$. Note that not all integers mod 8 have a multiplicative inverse; more about that later.

Properties of Modular Arithmetic
Define the set Z_n as the set of nonnegative integers less than *n*:
$Z_n = \{0, 1, - - -, (n-1)\}$
This is referred to as the Set of residues or Residue classes*(mod n)*.
Each integer in Z_n represents a residue class.
We can label the residue classes*(mod n)* as $[0], [1], - - -, [n-1]$
Where $[r] = \{a: a \text{ is an integer}, a \equiv r \pmod n\}$

Residues classes(mod 4) are

[0] = {…,-16,-12,-8,-4,0,4,8,12,16,….}

[1] = {…,-15,-11,-7,-3,1,5,9,13,17,….}

[2] = {…,-14,-10,-6,-2,2,6,10,14,18,….}

[3] = {…,-13,-9,-5,-1,3,7,11,15,19,….}

Of all the integers in a residue class, the smallest nonnegative integer is the one used to represent the residue class.

 DOI : 10.18231/2454-9150.2017.0044

Finding the smallest nonnegative integer to which is congruent modulo is called Reducing *k* modulo *n*.

If we perform modular arithmetic with in Z_n, the properties shown in Table below hold for integers in Z_n

Property	Expression
Commutative laws	$(w+x) \bmod n = (x+w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x+y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$
Identities	$(0+w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse (−w)	For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$

Table.2 Congruence properties

Z_n is a commutative ring with a multiplicative identity element.

There is one peculiarity of modular arithmetic that sets it apart from ordinary arithmetic.

First, observe that (as in ordinary arithmetic) we can write the following:

$$\text{If } (a + b) \equiv (a + c) \pmod{n} \text{ then } b \equiv c \pmod{n}) \rightarrow (1)$$

Ex: $(5 + 23) \equiv (5 + 7) \pmod 8;\ 23 \equiv 7 \pmod 8)$

Equation (1) is consistent with the existence of an additive inverse.

Adding the additive inverse of a to both sides of Equation (1), we have

$$((-a) + a + b) \equiv ((-a) + a + c) \pmod{n}$$
$$b \equiv c \pmod{n})$$

However, the following statement is true only with the attached condition:

$$\text{If } (a \times b) \equiv (a \times c) \pmod{n} \text{ then } b \equiv c \pmod{n}) \text{ if a is relative prime to n} \rightarrow (2)$$

Two integers are relatively prime if their only common positive integer factor is 1.

Similar to the case of Equation (1), we can say that Equation (2) is consistent with the existence of a multiplicative inverse.

Applying the multiplicative inverse of to both sides of Equation (2), we have

$$((a^{-1})ab) \equiv ((a^{-1})ac) \ (mod\ n)$$
$$b \equiv c \ (mod\ n))$$

Ex: Consider an example in which the condition of equation(2) does not hold.

Integers 6 and 8 are not relatively prime, since they have the common factor 2

$$6 \times 3 = 18 = 2(mod\ 8)$$
$$6 \times 7 = 42 = 2(mod\ 8)$$
$$Yet\ 3 \neq 7(mod\ 8)$$

III. Diffie Hellman Key Exchange

Purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. Algorithm itself is limited to the exchange of secret values.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

a)Discrete Logarithm

We can define a primitive root of a prime number p as one whose powers modulo generate all the integers from 1 to p.

That is, if 'a' is a primitive root of the prime number , then the numbers

$$a\ mod\ p, a^2\ mod\ p - - - - a^{p-1}\ mod\ p$$

are distinct and consist of the integers from 1 through *p-1* in some permutation.

For any integer *b* and a primitive root *a* of prime number *p*, we can find a unique exponent *i* such that

$$b \equiv a^i\ (mod\ p\ ) where\ 0 \leq i \leq (p-1)$$

The exponent *i* is referred to as the *Discrete Logarithm* of *b* for the base *a*, *mod p*.We express this value as $d\ log_{a,p}\ (b)$.

b)The Algorithm

Two publicly known numbers:

- a prime number q and
- an integer α that is a primitive root of q.

Suppose the users A and B wish to exchange a key.

User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A}\ mod\ q$

Similarly, User B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B}\ mod\ q$

Each side keeps the X value private and makes the Y value available publicly to the other side.

User A computes the key as $K = {Y_B}^{X_A}\ mod\ q$ and

User B computes the key as $K = {Y_A}^{X_B}\ mod\ q$

These two calculations produce identical results:

$$K = {Y_B}^{X_A}\ mod\ q$$
$$= (Y_B)^{X_A}\ mod\ q$$
$$= (\propto^{X_B}\ mod\ q)^{X_A}\ mod\ q$$
$$= (\propto^{X_B})^{X_A}\ mod\ q$$

By the rules of Modular Arithmetic

$$K = (\propto^{X_A})^{X_B}\ mod\ q$$
$$= (\propto^{X_A}\ mod\ q)^{X_B}\ mod\ q$$
$$= {Y_A}^{X_B}\ mod\ q$$

Result is that the two sides have exchanged a secret value.

 DOI : 10.18231/2454-9150.2017.0044

Because X_A and X_B are private, an adversary only has the following ingredients to
work with: q, α ,Y_A and Y_B .
Thus, the adversary is forced to take a discrete logarithm to determine the key.
Ex: To determine the private key of user B, an adversary must compute
$X_B = \text{dlog}_{a,q}(Y_B)$

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_B} \bmod q$

User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_A = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A
$K = (Y_B)^{X_A} \bmod q$

Calculation of Secret Key by User B
$K = (Y_A)^{X_B} \bmod q$

Security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms.
For large primes, the latter task is considered infeasible.

c)Testing for Primality

An attractive and popular algorithm ,it can yield a number that is almost certainly a prime.

Miller-Rabin Algorithm

This algorithm is typically used to test a large number for primality.
Any positive odd integer $n \geq 3$ can be expressed as $n - 1 = 2^k q \; with \; k > 0, q \; odd$. Here $(n-1)$ is an even integer.
Then, divide $(n-1)$ by 2 until the result is an odd number , for a total of n divisions.

a) Two Properties Of Prime Numbers:

The First Property is stated as follows:
If p is prime and a is a positive integer less than p, then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1 \; or \; a \bmod p = -1 \bmod p = p - 1$
By the rules of modular arithmetic $(a \bmod p)(a \bmod p) = a^2 \bmod p = 1$ which is true only for $a \bmod p = 1 \; or \; a \bmod p = -1$

The Second Property is stated as follows:

Let p be a prime number greater than 2.
We can then write
$$p - 1 = 2^k q \; with \; k > 0, q \; odd$$
Let a be any integer in the range $1 < a < (p-1)$.
Then one of the two following conditions is true.
1. a^q is congruent to 1 $modulo \; p$.
That is $a^q \bmod p = 1 \; or \; a^q \equiv 1 \; (mod \; p)$
2. One of the numbers a^q , a^{2q} , $a^{4q} - - - a^{2^{k-1}q}$ is congruent to $-1 \; modulo \; p$.

That is, there is some number j in the range $(1 \leq j \leq k)$ such that
$a^{2^{(j-1)}q} \bmod p = -1 \bmod p = p - 1$ or
$a^{2^{(j-1)}q} \equiv -1 \bmod p$
Proof:
Making use of Fermat's theorem

Fermat's theorem states that if n is prime.
We have $p - 1 = 2^k \; q$
Thus, we know that $a^{p-1} mod \; p = a^{2^k q} = 1$
Thus, the sequence of numbers are $a^q \bmod p$, $a^{2q} \bmod p$, $a^{4q} \bmod p - - - a^{2^k q} \bmod p$
we know that the last number in the list has value 1.

Each number in the list is the square of the previous number.

Therefore, one of the following possibilities must be true.
1. The first number on the list, and therefore all subsequent numbers on the list, equals 1.
2. Some number on the list does not equal 1, but its $square \bmod p$ does equal 1.

b)Details of the Algorithm

If n is prime, then either the first element in list of element in list of residues or remainders $\left(a^q, a^{2q}, - - - - a^{2^{k-1}q}, a^{2^k q}\right) modulo \; n$ equals 1 ; or some element in the list equals $(n-1)$; otherwise n is Composite (Not a Prime)
Even though the condition has been met, it doesn't mean n is prime

TEST(n)
1. $Find \; integers \; k, q, with \; k > 0, q \; odd \; so \; that \; (n - 1 = 2^k q)$
2. $Select \; a \; random \; integer \; a, 1 < a < n - 1$
3. $if \; a^q \bmod n = 1 \; then \; return \; "Inconclusive";$
4. $for \; j = 0 \; to \; (k-1) do$
5. $if \; a^{2^j q} \bmod n = n - 1 \; then \; return \; "Inconclusive";$
6. $return \; "Composite";$

Test for the Prime number $n = 29$
$Find \; integers \; k, q, with \; k > 0, q \; odd \; so \; that$

 DOI : 10.18231/2454-9150.2017.0044

$(n-1 = 2^k q)$
$29-1 = 2^2.7$
$k = 2$ and $q = 7$
Case 1:
Let us try for $a = 10$
$a^q \bmod n = 1$
$10^7 \bmod 29 = 1$
$17 \neq 1$
$a^{2^j q} \bmod n = n-1$
$j = 1\ a^{2^j q} \bmod n = n-1$
$10^{2^1.7} \bmod 29 = 29-1$
$(10^7)^2 \bmod 29 = 28$
$28 = 28$
Inconclusive
29 *may be prime*
Case 2:
Let us try for $a = 2$
$a^q \bmod n = 1$
$2^7 \bmod 29 = 1$
$12 \neq 1$
$a^{2^j q} \bmod n = n-1$
$j = 1\ a^{2^j q} \bmod n = n-1$
$2^{2^1.7} \bmod 29 = 29-1$
$(2^7)^2 \bmod 29 = 28$
$28 = 28$
Inconclusive
2 *may be prime*

3.Test for the Prime number $n = 221$
Find integers $k, q,$ *with* $k > 0, q$ *odd so that* $(n-1 = 2^k q)$
$221-1 = 2^2.55$
$k = 2$ and $q = 55$
Let us try for $a = 5$
$a^q \bmod n = 1$
$5^{55} \bmod 221 = 1$
Solving $5^{55} \bmod 221$
In Binary, 55 is represented as 110111

32	16	8	4	2	1
1	1	0	1	1	1

Table.3 Binary, 55 is represented as 110111

$5^1 \equiv 5 (mod\ 221)$
$5^2 \equiv 25 (mod\ 221)$
$5^4 \equiv (5^2)^2 = 25^2 (mod\ 221) = 625\ (mod\ 221)$
$= 183\ (mod\ 221)$
$5^8 \equiv (5^4)^2 = 183^2 (mod\ 221) = 33489\ (mod\ 221)$
$= 118\ (mod\ 221)$
$5^{16} \equiv (5^8)^2 = 118^2 (mod\ 221) = 13924\ (mod\ 221)$
$= 1\ (mod\ 221)$
$5^{32} \equiv (5^{16})^2 = 1^2 (mod\ 221) = 1\ (mod\ 221)$
$= 1\ (mod\ 221)$
$5^{55} \equiv 5^1 \times 5^2 \times 5^4 \times 5^8 \times 5^{16} \times 5^{32} = 22875\ (mod\ 221)$
$= 112 (mod\ 221)$
$112 \neq 1$
$a^{2^j q} \bmod n = n-1$
$j = 1\ a^{2^j q} \bmod n = n-1$
$5^{2^1.55} \bmod 221 = 221-1$
$(5^{55})^2 \bmod 221 = 220$
$112^2 \bmod 221 = 220$
$168 \neq 220$
Return Composite
Since $221 = 13\ X\ 17$

(c)In our Diffie-Hellman Key Exchange lets consider an example
Key exchange is based on the use of the prime number q = 353 and a primitive root of 353, in this case α = 3.
User A and User B select secret keys $X_A = 97$ and $X_B = 233$ respectively.
Each computes its public key:
User A computes $Y_A = \alpha^{X_A} \bmod q = 3^{97} \bmod 353 = 40$
User B computes $Y_B = \alpha^{X_B} \bmod q = 3^{233} \bmod 353 = 248$
After they exchange public keys, each can compute the common secret key:
User A computes the key as $K = {Y_B}^{X_A} \bmod q = 248^{97} \bmod 353 = 160$ and
User B computes the key as $K = {Y_A}^{X_B} \bmod q = 40^{233} \bmod 353 = 160$
We assume an attacker would have available the following information:
q = 353; a = 3; Y_A = 40; Y_B = 248
In this simple example, it would be possible by brute force to determine the secret key 160. In particular, an attacker E can determine the common key by discovering a solution to the equations:
User A computes $Y_A = \alpha^{X_A} \bmod q$
$\Rightarrow 40 = 3^a \bmod 353$
User B computes $Y_B = \alpha^{X_B} \bmod q$
$\Rightarrow 248 = 3^b \bmod 353$
Brute-force approach is to calculate powers of 3 modulo 353, stopping when the result equals either 40 or 248. The desired answer is reached with the exponent value of 97, which provides $3^{97} mod\ 353 = 40$.
With larger numbers, the problem becomes impractical.

d)Key Exchange Protocols
Figure shows a simple protocol that makes use of the Diffie-Hellman calculation.

 DOI : 10.18231/2454-9150.2017.0044

Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection.
User A can generate a one-time private key X_A, calculate Y_A, and send that to user B.
User B responds by generating a private value X_B, calculating Y_B, and sending to user A.
Both users can now calculate the key. Necessary public values q and α would need to be known ahead of time.
Alternatively, user A could pick values for q and α and include those in the first message.

As an example of another use of the Diffie-Hellman algorithm, suppose that a group of users (e.g., all users on a LAN) each generate a long-lasting private value X_i (for user) and calculate a public value Y_i .

These public values, together with global public values for q and α, are stored in some central directory. At any time, user *j* can access user 's i public value, calculate a secret key, and use that to send an encrypted message to user A.

If the central directory is trusted, then this form of communication provides both confidentiality and a degree of authentication.

Because only *i* and *j* can determine the key,
No other user can read the message (confidentiality).
Recipient knows that only user could have created a message using this key (authentication). However, the technique does not protect against replay attacks.

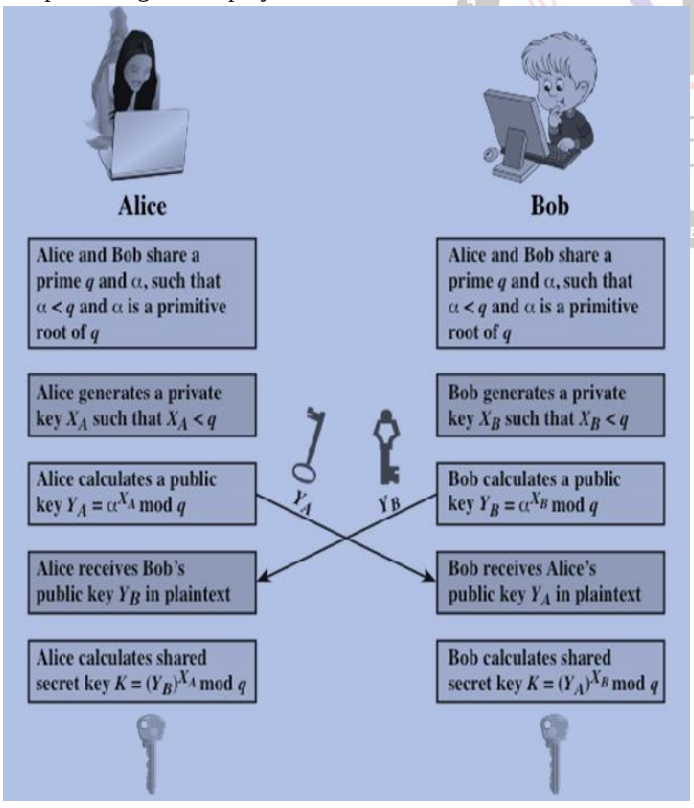

Fig.4: User A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection.

e) Man-in-the-Middle Attack

The protocol depicted in below Figure is insecure against a Man-in-the-Middle attack.
Suppose Alice and Bob wish to exchange keys, and Darth is the adversary.

The attack proceeds as follows.
1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2} .
2. Alice transmits to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K2 = (Y_{D1})^{X_{D2}} mod\ q$
4. Bob receives Y_{D1} and calculates
$K1 = (Y_{D1})^{X_B} mod\ q.$
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates $K1 = (Y_B)^{X_{D1}} mod\ q$
7. Alice receives and calculates $K2 = (Y_{D2})^{X_A} mod\ q.$

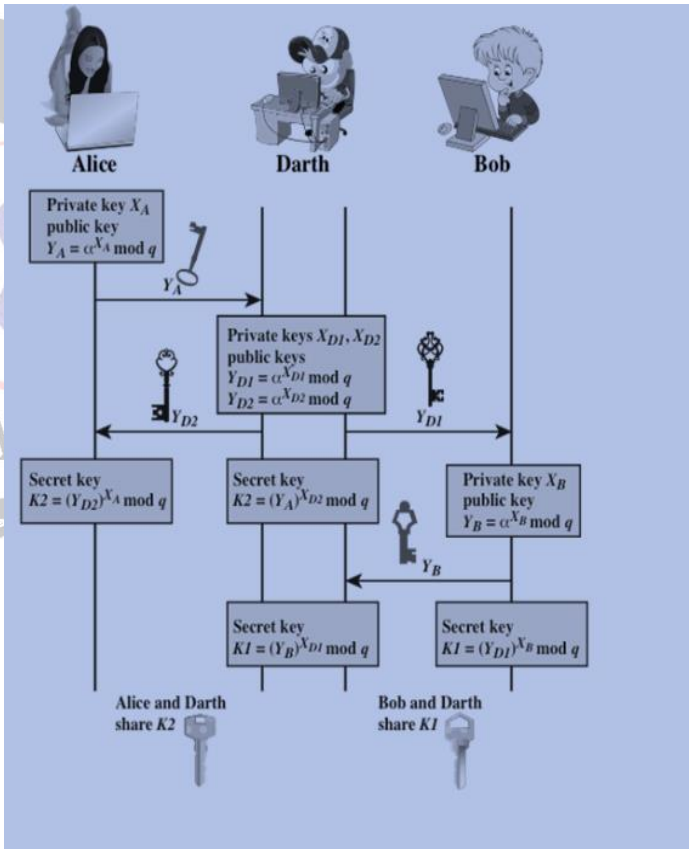

Fig.5: Man-in-the-Middle Attacks

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key K_1 and Alice and Darth share secret key K_2.

All future communication between Bob and Alice is compromised in the following way.
1. Alice sends an encrypted message *M : E (K_2, M).*

 DOI : 10.18231/2454-9150.2017.0044

2. Darth intercepts the encrypted message and decrypts it to recover *M*.
3. Darth sends Bob *E (K_1*, M) or E (K_1, M') where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.

Key exchange protocol is vulnerable to such an attack because it does not authenticate the participants.

IV. CONCLUSIONS AND FUTURE WORK

This thesis investigated and analyzed a particular man-in-the-middle attack on the Diffie-Hellman key exchange protocol. We created an algorithm to carry out the attack and demonstrated how it is constrained by the primality test used by the attacker. In particular, if the Miller-Rabin primality test is used, the algorithm's complexity is $O((\log N)^3)$ with N being the input prime number. We showed that prime numbers of the form $p=Rq+1$ with R bounded are common with small primes but become increasingly rare as larger numbers are considered. In fact, with low bit primes such as 128 bits, a reasonably-sized R will give an attacker a good chance of the prime being of the desired form. However, when large primes such as 1024 and 2048 bits are considered, a very large value of R is required to give an attacker a reasonable chance of conducting the attack. We demonstrated how two techniques, authentication and prime order 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 analyzing 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. In addition, it may be possible to alter the attack to compromise communications that are authenticated and render several Diffie-Hellman variants such as the STS protocol vulnerable.

REFERENCES

[1] J. B. Fraleigh, A First Course in Abstract Algebra. Addison Wesley, San Francisco, CA, 7th Edition, 2002.

[2] K. H. Rosen, Discrete Mathematics and Its Applications. McGraw Hill, San Francisco, CA, 6th Edition, 2007.

[3] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective. Springer, New York, NY, 2001.

[4] A. L. Atkin and F. Morain, Elliptic Curves and Primality Proving. Res. Rep. 1256, INRIA, June 1990.

[5] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P. Annals of Mathematics 160. 2004.

[6] C. Pomerance and H.W. Lenstra, Primality testing with Gaussian periods, preprint.

[7] W. Diffie and M. E. Hellman, New Directions in Cryptography. IEEE IT- 22, 1976, pp. 644–654.

[8] W. Trappe and L. Washington, Introduction to Cryptography with Coding Theory. Pearson, Upper Saddle River, NJ, 2nd Edition, 2006.

[9] 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.

AUTHOR DETAILS

Dr.S.V.B.Subrahmanyeswara Rao has 16 years of teaching experience. He is presently working in Rama Chandra College of Engineering, Eluru in the Department of Mathematics.

His areas of interest are Commutative Algebra and Cryptography.The author would like to thank the Management of RCE for the support.

Mrs.Y.Anjani has 10 years of teaching experience. She is presently working in VKR,VNB& AGK College of Engineering, Gudivada in the Department of Computer Science & Engineering.

Her areas of interest are Cryptography and Network Security, Mobile Computing. The author would like to thank the Management of VKR,VNB& AGK College of Engineering for the support.

 DOI : 10.18231/2454-9150.2017.0044