Number Theory and related Algorithms in Cryptography

Alireza Nemaney Pour (010003)

School of Information Science,
Japan Advanced Institute of Science and Technology

August 15, 2002

Keywords: Diffie-Hellman, MTI, Active Attack, Key Verification.

1 Introduction

Cryptography has a long and fascinating history. The most striking development in the history of cryptography came in 1976 when **Diffie** and **Hellman** published "*New Directions in Cryptography* "[3]. This paper introduced the revolutionary concept of public-key cryptography and also provided a new and ingenious method for key exchange, the security of which is based on the intractability of the discrete logarithm problem.

In many cryptographical protocols two parties wish to begin communicating. However, assume they do not initially possess any common secret key and thus cannot use secret key cryptosystems. The key exchange by Diffie-Hellman protocol remedies this situation by allowing the construction of a common secret key over an insecure communication channel.

The objective of a key distribution or key agreement protocol is that, at the end of the protocol, the two parties involved both have possession of the same key K, and the value of K is not known to any other party.

Attacks against Diffie-Hellman include the *man-in-the-middle attack*. It is in practice very easy if the protocol doesn't use countermeasures such as authentication. An *active attack* involves an *active adversary* who modifies or injects messages. The objective of an active adversary might be " to fool the users into accepting an "invalid " key as valid " or " to make the users believe that they have exchanged a key with each other when they have not ".

2 The Goals

In most of the Key-Exchange Algorithms a *trusted authority* is responsible for verifying the identities of users, choosing and transmitting keys to users, etc. This is something that this research follows to avoid it because there are cases that users want to communicate directly.

As a fundamental goal, the objective of this research is on developing a secure key distribution protocol aiming at achieving the following goals :

1. secure against the man-in-the-middle attack
2. security based on intractability of Diffie-Hellman problem
3. capable to key authentication, to provide assurance for the recipient whether he or she has computed the valid key

This research will focus on the development of a protocol by which users can authenticate each other in an insecure network without a central authority. Using such a protocol, users will be able to correctly identify the origin of a message, with an assurance that the identity is not false.

There are many algorithms based on the hardness of Discrete Logarithm Problem which most of them such as MTI and ElGamal are insecure against the man-in-the-middle attack. We will consider MTI and ElGamal protocls in this research and try to rectify certain problems in MTI and ElGamal with proposing an efficient public key distribution protocol.

3 An Overview

3.1 Diffie-Hellman Protocol

Diffie-Hellman key agreement provided the first practical solution to the key distribution problem, allowing two parties, never having met in advance or shared keying material, to establish a shared secret by exchanging messages over an open channel.

Both users Alice and Bob first agree on a prime p and a primitive root $g \in \mathbb{Z}_p^*$.

1. Alice chooses r at random such that $1 \leq x \leq p-2$, computes $X \equiv g^x \ (mod\ p)$ and sends it to Bob.
2. Bob chooses r' at random such that $1 \leq y \leq p-2$, computes $Y \equiv g^y \ (mod\ p)$ and sends it to Alice..
3. Alice computes
$$K \equiv Y^x = (g^y)^x = g^{xy} \ (mod\ p).$$
4. Bob computes
$$K' \equiv X^y = (g^x)^y = g^{xy} \ (mod\ p).$$

Unfortunately, the protocol is vulnerable to an active adversary who uses a *man-in-the-midle attack*. An active adversary like Lucy will intercept messages between Alice and Bob and substitute her own messages, as indicated in the following diagram :

$$Alice \ \underset{g^{y'}}{\overset{g^x}{\rightleftarrows}} \ Lucy \ \underset{g^{y}}{\overset{g^{x'}}{\rightleftarrows}} \ Bob$$

At the end of the protocol, Alice has actually established the secret key $g^{xy'}$ with Lucy, and Bob has established a secret key $g^{x'y}$ with Lucy. When Alice tries to encrypt a message to send to Bob, Lucy will be able to decrypt it but Bob will not. (A similar situation holds if Bob sends a message to Alice.)

3.2 MTI/C1 Protocol

1. Alice chooses a random secret r such that $1 \leq r \leq p-2$, computes $Z \equiv Y^{rx} = g^{rxy} \ (mod\ p)$ and sends it to Bob.

2. Bob chooses a random secret r' such that $1 \leq r' \leq p-2$, computes $Z' \equiv X^{r'y} = g^{r'xy} \ (mod\ p)$ and sends it to Alice.

3. Alice computes

$$K \equiv Z'^{r} = g^{xyrr'} \ (mod\ p).$$

4. Bob computes

$$K' \equiv Z^{r'} = g^{xyrr'} \ (mod\ p).$$

As we discussed before there is no protection against an active adversary in a man-in-the-middle attack. Clearly even with these protocols neither Alice nor Bob cannot confirm whom they have exchanged the keys. The only advantage of these protocols is that an active adversary like Lucy cannot intercept messages with Alice or Bob. But as well as Lucy, none of Alice or Bob can generate a right key to encipher or decipher the messages.

4 A Proposed Public Key Distribution Protocol

This protocol consists of 3 phases; Registration Phase, Transfer Phase, and Key-Generation with Key-Verification Phase for recipient of the message.

4.1 Registration Phase

Each user like Alice and Bob selects a secret data x and y relatively such that $2 \leq x, y \leq p-2$, computes $X \equiv g^x \ (mod\ p)$, and $Y \equiv g^y \ (mod\ p)$ and registers X, and Y to the public file. The prime number p and its primitive root g are public. Clearly, X and Y are public too.
For transferring data and key generating each user, Alice and Bob should do the following:

4.2 Transfer, Key-Generation with Key-Verification Phases

1. Alice chooses a random secret r, $2 \leq r \leq p-2$.

2. Alice computes $K \equiv Y^{rx} = g^{rxy} \ (mod\ p)$ as the shared key.

3. Bob chooses a random secret r', $2 \leq r' \leq p-2$, such that $gcd(r', p-1) = 1$. Again Bob finds $\overline{r'}$ which is the inverse element of r' from $r'\overline{r'} \equiv 1 \ (mod\ p-1)$.

4. Bob computes $Z' \equiv X^{r'y} = g^{r'xy} \ (mod\ p)$, again $v' \equiv g^{r'} \ (mod\ p)$ and sends (Z', v') to Alice.

5. Alice computes $Z \equiv Z'^{r} = g^{rr'xy} \ (mod\ p)$ and again $v \equiv X^{r} \cdot v'^{x} = g^{x(r+r')} \ (mod\ p)$ and sends (Z, v) to Bob.

6. Bob computes

$$K' \equiv Z^{\overline{r'}} = g^{r(r'\overline{r'})xy} = g^{rxy} \ (mod\ p).$$

and

$$K' \equiv v^{y} \cdot X^{-r'y} = g^{rxy} \ (mod\ p).$$

to verify if $Z^{\overline{r'}} = v^{y} \cdot X^{-r'y}$. If the above equation stands up, the generated key is accepted and it means that Bob can be sure that he has a right key.

5 Conclutions and future work

The results of this research are as following:

1. The generated key is secure against the man in the middle attack.
2. The protocol is based on intractability of Diffie-Hellman problem.
3. It is capable for key authentication, it provides assurance for the recipient whether he or she has computed the valid key.
4. Using random numbers for session keys it is non-deterministic.

The other property of this protocol is verification that can be done easily by the recipient of the message. This protocol has been extended from MTI/C1 and ElGamal.

One open problem with this protocols is that it is still unknown whether it can be generalized and extended to be used among 3 or more users. This protocol can be used as a one-pass protocol as well. In this situation it will not be secure against most of the attackes such as man-in-the-middle attack.

References

[1] Neal Koblitz,"*A Course in Number Theory and Cryptogaphy* ", Second Edition, Springer, (1994).

[2] 遠山 啓,"初等整数論 ", 日評数学選書：日本評論社, (1992).

[3] Whitfield Diffie and Martin E. Hellman,"*New Directions in Cryptography* " Invited Paper, (1976).

[4] Tsutomu Matsumoto, Youichi Takashima, and Hideki Imai,"*On seeking Smart Public-Key-Distribution Systems* " The Transactions of the IECE of Japan, Vol. E **69**, No. 2, (1986).

[5] Simon Blake-Wilson, Don Johnson, Alfred Menezes,"*Key Agreement Protocols and their Security Analysis* " (1997).