Volume 3, No. 9, September 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

ON A KEY EXCHANGE TECHNIQUE, AVOIDING MAN-IN-THE-MIDDLE-ATTACK

Barun Biswas[1#], Krishnendu Basuli[2*], Samar Sen Sarma[2*]
[#1]Dept. of Computer Science, West Bengal State University, India
barunbiswas9u6@gmail.com
[*2]Dept. of Computer Science, West Bengal State University, India
krishnendu.basuli@gmail.com
[*2]Department of Computer Science and Engineering, University of Calcutta, 92, A.P.C. Road, Kolkata – 700 009, India.
sssarma2001@yahoo.com

***Abstract*—** Cryptography is a technique in which a data is transmitted through the medium without being hampered. It is not new subject. It was used far ago. This technique deals with many steps, such as: key generation, key transmission, key storage and key deletion. The most difficult part of the cryptography is the design of cipher; i.e. designing of the algorithm used to encrypt and decrypt plain text and cipher text respectively. A problem generally noticed is man-in-the-middle attack. We will try to eliminate or reduce the chance to occur this problem.

***Keywords*—** Diffie-Hellman cypher, Plaintext, Cyphertext, symetric kry, Man-in-the-middle Attack.

INTRODUCTION

Today Information is as important as any other assets in our daily life. Like any other assets information must be keep secure from unauthorised access and attack from other. To be secured, information need to be hidden from unauthorised access (confidentiality), protected from unauthorised access (integrity) and available to authorised entity when needed (availability)[2][3].

So maintain confidentiality we can use many process which can protect the information from unauthorised access. In this paper we will introduce some of the techniques for maintaining confidentiality.

Motivation:

The basic motivation of this discussion is avoid unauthorised access. While sender sends any information or data to any receiver, the receiver can receive the original data or information without any distortion or any unexpected change made to the original data. For this purpose we will use some secret key to encrypt the original data. In the time of transmission if any unauthorised media access the encrypted data or cipher text so that it can't be understood by the middle parson or media.

Some basic definition:

In the following there are some basic definition for the easy understanding of the discussion and term used in this paper.

- ***a. Plain Text:*[2]]3][6]** Plain text is the text which the sender wants to send to the receiver.
- ***b. Cipher text:*[2][3][6]** Cipher text is the text that is sent through the media. It is not in the original form of the data or information. It is the form after the cipher is applied on the data.
- ***c. Cryptography:*[2][3][6]** Cryptography, a word with Greek origin, means "secret writing." However we use the term to refer to the science and art of transforming message to make them secure and immune to attack. Although in the past cryptography refers only to the encryption and decryption of messages using secret keys. Today it is defined involving three distinct mechanisms: symmetric key encipherment, asymmetric key encipherment and hashing.
- ***d. Symmetric Key Encipherment:*[2][3][6]** In the symmetric key encipherment sender can send a message to the receiver over an insecure channel with the assumption that the adversary can't understand the massage by sampling eavesdropping the channel. In this process the sender and the receiver use the same algorithm (cipher) to encrypt and decrypt the data.
- ***e. Asymmetric Key Encipherment:*[2][3][6]** In asymmetric key cipherment the situation same as symmetric key cipherment, with a few exceptions. First there two keys instead of one : one public key and other private key
- ***f. Cipher:*[2][3][6]** Cipher is the algorithm used to encrypt or decrypt the plain text and cipher text respectively.

PREVIOUS WORK

About 1900 BC An Egyptian scribe used non-standard hieroglyphs in an inscription. Kahn lists this as the first documented example of written cryptography [history of encryption 730]

The history of cryptography can be broadly divided into three phases: [4]

a. From ancient civilizations to the nineteenth century and the first part of the twentieth century,
b. With relatively simple algorithms that were designed and implemented by hand.
c. Extensive use of encrypting electro-mechanical machines, around the period of the Second World War.
d. Ever more pervasive use of computers, about in the last fifty years, supported by solid
Mathematical basis.

Diffie–Hellman key exchange (**D–H)** [1][2] is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

The scheme was first published by Whitfield Diffie and Martin Hellman in 1976, although it was later alleged that it had been separately invented a few years earlier within GCHQ, the British signals intelligence agency, by Malcolm J. Williamson but was kept classified. In 2002, Hellman suggested the algorithm be called **Diffie–Hellman–Merkle key exchange** in recognition of Ralph Merkle's contribution to the invention of public-key cryptography (Hellman, 2002).

To prevent man-in-the-middle attack the Station-To-Station (STS) protocol was proposed[].

Diffie-Hellman[5]:

Public key cryptography was first publicly proposed in 1975 by Stanford University researchers Whitfield Diffie and Martin Hellman to provide a secure solution for confidentially exchanging information online. The following figure shows the basic Diffie-Hellman Key Agreement process.

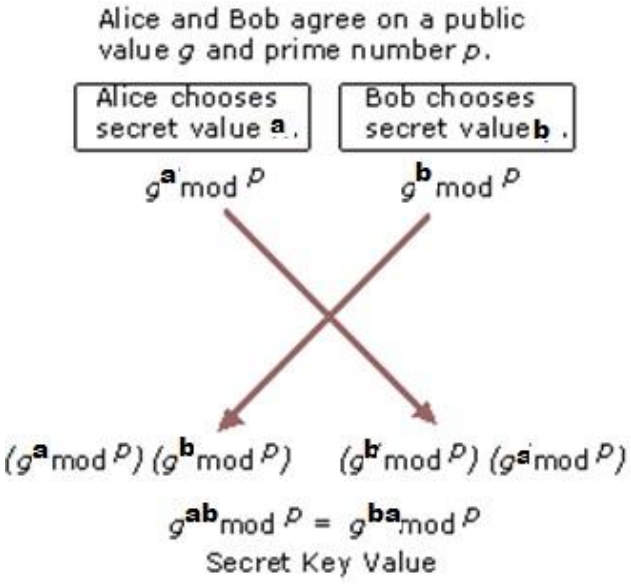


Figure: 1

Diffie-Hellman key agreement is not based on encryption and decryption, but instead relies on mathematical functions that enable two parties to generate a shared secret key for exchanging information confidentially online. Essentially, each party agrees on a public value *g* and a large prime number *p*. Next, one party chooses a secret value a and the other party chooses a secret value b. Both parties use their secret values to derive public values, *g*^a mod *p* and *g*^b mod *p*, and they exchange the public values. Each party then uses the other party's public value to calculate the shared secret key that is used by both parties for confidential communications. A third party cannot derive the shared secret key because they do not know either of the secret values, a or *b* . For example, Alice chooses secret value a and sends the public value *g*^a mod *p* to Bob. Bob chooses secret value b and sends the public value *g*^b mod *p* to Alice. Alice uses the value *g*^ab mod *p* as her secret key for confidential communications with Bob. Bob uses the value *g*^ba mod *p* as his secret key. Because *g*^ab mod *p* equals *g*^ba mod *p*, Alice and Bob can use their secret keys with a symmetric key algorithm to conduct confidential online communications. The use of modulo function ensures that both parties can calculate the same secret key value, but an eavesdropper cannot. An eavesdropper can intercept the values of *g* and *p* , but because of the extremely difficult mathematical problem created by the use of a large prime number in mod *p*, the eavesdropper cannot feasibly calculate either secret value *a* or secret value b . The secret key is known only to each party and is never visible on the network.

Man-in-the-middle Attack [2]:

Let us take the example illustrated by Diffie-Hellman to discuss the Man-in-the-Middle Attack. Let us that Eve is in the middle of Alice and Bob. Eve does not need the value of x or y to attack the protocol. She can fool both Alice and Bob by the following process.

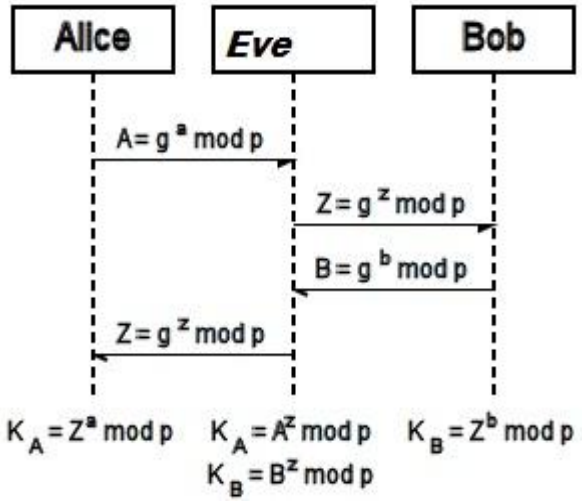


Figure: 2

a. Alice choose a, calculate A=g^a mod p
b. Eve, the intruder, interpret A, she chooses z, calculate Z=g^z mod p, and sends Z to both Alice and Bob.
c. Bob choose b, calculate B=g^b mod p, and sends B to Alice; B is interpreted by Eve and never reaches Alice.
d. Alice and Eve calculate the same key g^az mod p, which become a shared key between Alice and Eve. Alice however think that it is a key shared between Bob and herself.
e. Eve and Bob calculate the same key g^bz mod p, which become a shared key between Eve and Bob. Bob, however, thinks that it is a key shared between Alice and himself.

This situation is called man-in-the-middle attack.

PROPOSED PROCESS

In our following process of cryptography we will try to introduce such a process which can avoid man-in-the-middle

attack or try to reduce the chance of occurring man-in-the-middle attack.

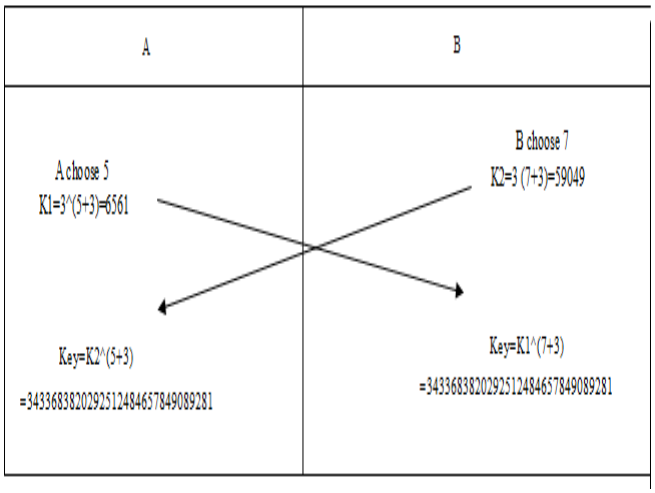
Algorithm:

Suppose A wants to send a message to B. Both A and B use a secret number e

Step 1: A chooses a large prime number M and calculates K1= e^(M+e); say M1=M+e; i.e. K1=E^M1
Step 2: B chooses a large prime number N and calculates K2=e^(N+e); say N1=N+e; i.e. K2=E^N1
Step 3: A sends K1 to B, note that N is not known to A.
Step 4: B sends K2 to A, note that M is not known to B.
Step 5: A calculates Key=(K2)^M1=e^(M1N1)
Step 6: B calculates Key=(K1)^N1=e^(M1N1).
Step 7: Both A and B can check whether the key is being attacked or not by calculating as follows: log e (e^(M1N1))=M1N1.
A calculates R1=(M1N1/M1)-e
If R1 is a prime number then key is not attacked.
Similarly B calculate R2=(M1N1/N1)-e.
If R2 is a prime number then key is not attacked.

Example:

e = 3



How Man-in-the-middle-attack can be reduced:

Suppose the key in the middle is attacked and changed. Say z is the number which is the power of both K1 and K2. So the new key will be K1^z and K2^z. While A and B will check the key by R1=log e (e^key) and R2=log e(e^key) A and B will get (M+e)*z and (N+e)*z. M and e are known to A and similarly N and e are known to B. So they can easily find z. So after subtracting e from z if they get that (z-e) is not a prime number then it can easily be assume the key is attacked. They will discard the key and will resend the key to exchange.

CONCLUSION

This paper introduces a new process for key exchange. In cryptography the most challenging task is to design a cipher. In this sort discussion we tried to implement an easy and simple way to understand cryptographic algorithm. One of the most common problems in data transferring is hacking the data in the middle; i.e. man-in-the-middle attack. In our discussion we introduce such a process where man-in-the-middle-attack can be eliminate, if not it can be reduced to a great percentage. We think that this try will help in the field of secure key transfer between two authorised persons or organisation.

REFERENCES

[1]. Debajit Sensarma, Subhashis Banerjee , Krishnendu Basuli, " A New Scheme for Key Exchange". International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, May-June 2012 pp-864-869

[2]. Behrouz A. Forouzan, "Cryptography & Network Security", Tata McGraw-Hill Publishing Company,2007

[3]. V.K. Pachghare, "Cryptography and Information Security", PHI,2009

[4]. Fron SANS Institution InfoTech Reading room, "History of Cryptography", SANS Institution, 2001

[5]. Dieter Gollmann "Computer Security Second Edition" West Sussex, England: John Wiley & Sons, Ltd. 2006.

[6]. Berti, Hansche, Hare (2003). Official (ISC)² Guide to the CISSP Exam. Auerbach Publications. pp. 379. ISBN 0-8493-1707-X.

