ISSN 2278-7763

A novel process for key exchange avoiding man-in-middle attack

Subtitle as needed

Barun Biswas*[1], Krishnendu Basuli+[2]

*1Dept. of Computer Science, West Bengal State University, India
barunbiswas9u6@gmail.com
+2Dept. of Computer Science, West Bengal State University, India
krishnendu.basuli@gmail.com

Abstract- For the security porpoise in the internet cryptography is one of the most important subjects nowadays. Designing a cypher for data exchange between two nodes or receiver and sender deals with one of the troubleshoot jobs. In our proposed algorithm we try to introduce a new technique in the field of cryptography. We are hopeful that this new technique will sure reduces the overhead of data or key exchange between nodes. Here we will discuss the symmetric key exchange between nodes.

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

I. INTRODUCTION

In cryptography key exchange is one of the most important aspects. While transmitting data between two hosts we use some keys to encrypt data from plain text to cypher text. We use the same key to decrypt the data from cypher text to plain text. The process where same key is used to encrypt or decrypt data in cryptography is called symmetric key cryptography [1]. While using symmetric key in cryptography the sender and receiver may use the same key by some previous agreement or they may send the key one another. While sending key one another the security aspect might be maintained.

In the following process of key exchange we will try to introduce a new process in which a key can be send safely and the probability of being hacked the key can be reduced. Our process is inspired by Diffie-Hellman technique [10][11].

II. BASIC DEFINITION

A. Cryptography:

An **Cryptography** (or cryptology; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively)[1] is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).[2] More generally, it is about constructing and analysing protocols that overcome the influence of adversaries[3] and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication.[4] Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

B. Cypher:

In cryptography, a **cipher** (or **cypher**)[5] is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information from plain text into code or cipher. In non-technical usage, a "cipher" is the same thing as a "code"; however, the concepts are distinct in cryptography..

C. Cypher text:[6]

ISSN 2278-7763

In cryptography, **cipher text** (or **cypher text**) is the result of encryption performed on plaintext using an algorithm, called a cipher.

D. **Plain text:[6]**

In cryptography, **plaintext** is information a sender wishes to transmit to a receiver.

E. **Symmetric key cryptography*:***

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976[7].

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

F. **Asymmetric key cryptography:**

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used—a public key and a private key[8]. A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair[8]. The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance"[9].

III. PREVIOUS WORKS

Diffie–Hellman key exchange (**D–H)** [10] 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[11].

Next comes **Secure Socket Layer (SSL)** [12] involves negotiating and establishing secure connections, and securing the data transmission. SSL handshake uses certificates and PKI [13] for mutual authentication and key exchange. PKI binds public keys with particular user identities by means of a certificate authority (CA).

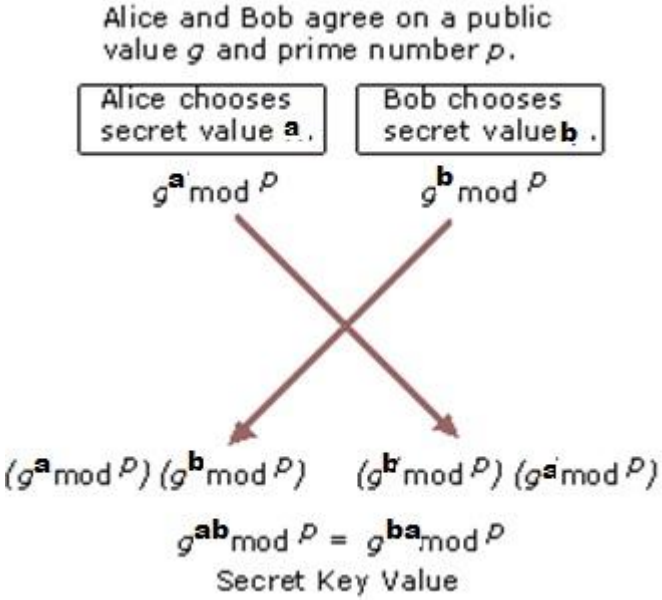
More than these there are many more researches have been done in this field. They all are significant.

As we are considering Diffie-Hellman algorithm of symmetric key exchange let us first discuss the process and point out the drawback of the process.

A. **Diffie–Hellman key exchange** (**D–H)**

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.

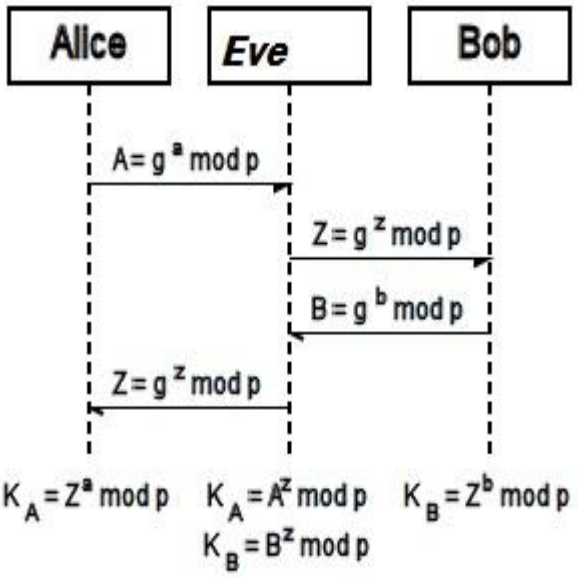
ISSN 2278-7763



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 the 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.

B. **Man-in-the-Middle Attack**

We everyone knows about the Man-in-the-Middle Attack. 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.



1. Alice choose a, calculate A=g^a mod p
2. Eve, the intruder, interpret A, she chooses z, calculate Z=g^z mod p, and sends Z to both Alice and Bob.
3. Bob choose b, calculate B=g^b mod p, and sends B to Alice; B is interpreted by Eve and never reaches Alice.
4. 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.
5. 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.

ISSN 2278-7763

=1.54406804435

IV. PROPOSED PROCESS

In our proposed process we try to eliminate the man-in-the-middle attack, so our approach would be such that the middle man could not change the key. For his porpoise we introduce some techniques. The proposed technique is as follows:

A. Algorithm

Suppose Barun(B) wants to exchange key with Krishnendu(K). Both B and K use e as a secret number as the base of log.

Step 1: B chooses a large prime number M and calculate K1=log e (M).

Step 2: K chooses a large prime number N and calculate K2=log e (N).

Step 3: B sends K1 to K, note that N is not known to B.

Step 4: K sends K2 to B, note that M is not known to K.

Step 5: B calculates Key=K1+K2=log e (M) + log e (N) = log e (MN).

Step 6: K calculates Key=K1+K2=log e (N) + log e (M) = log e (NM) = log e (MN).

Step 7: Both B and K can check whether the key is being attacked or not by calculating as follows: e^log e (MN)=MN.

B calculates R1=MN/M

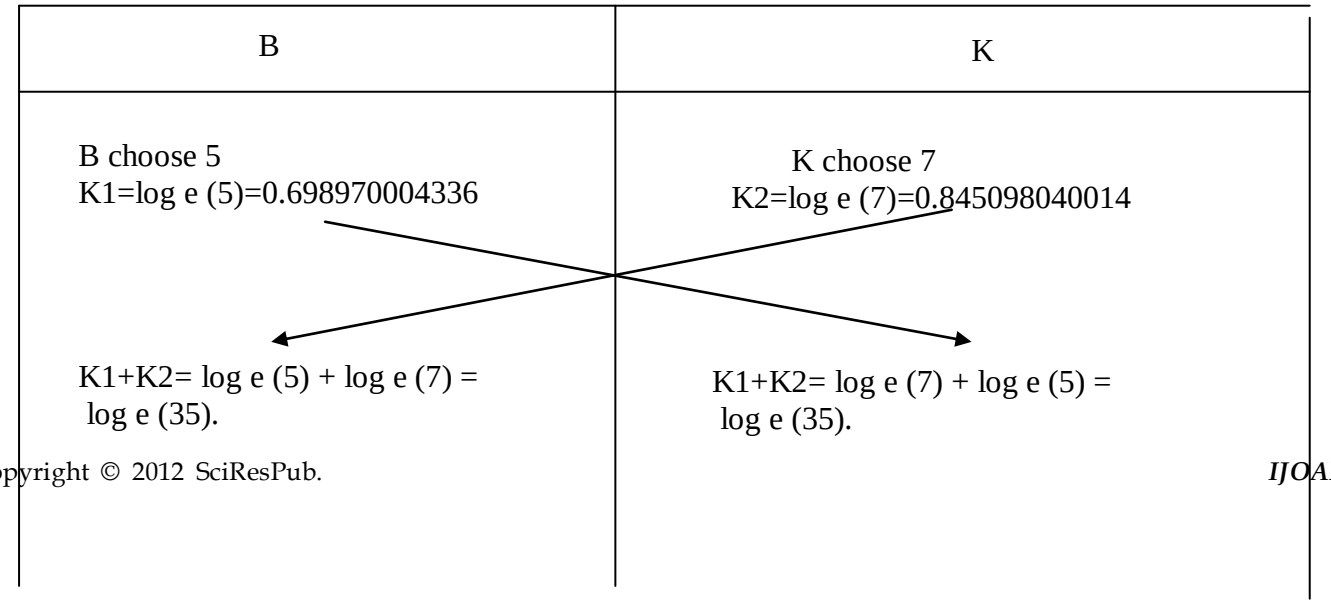
If R1 is a prime number then key is not attacked.

Similarly K calculate R2=MN/N.

If R1 is a prime number then key is not attacked.

B. Example:

e = 10



=1.54406804435

In the above example we take only twelve digits after the decimal point for the simplicity of the calculation.

C. How Man-in-the-Middle attack can be eliminate.

Note that both B and K use a secret number e as the base of the log. If in the middle the key is attacked and the key is changed not necessarily the base will be e. As we can calculate R1=MN/M and R2=MN/N so we can easily catch the error.

V. CONCLUSION

Design of algorithm on cryptographic field is one of the most challenging aspects. Actually exchanging it on internet without hampered is such a big deal. While designing the algorithm we keep in mind the man-in-the-middle attack. In this cypher we tried our best to maintain that security aspect. However we can't say that man-in-the-middle attack can be fully eliminate because the base selected by the middle man can be same as e unfortunately. More over Diffie-Hellman cypher is a great algorithm and our cypher is encouraged by Diffie-Hellman algorithm.

VI. REFERENCES

[1] Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984)
[2] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. *Handbook of Theoretical Computer Science*. **1**. Elsevier.
[3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.
[4] Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-8523-7.
[5] Behour A. Forouzan, Sophia Chung Fegan "Data Communication and Networking", Fourth Edition 2009.
[6] Berti, Hansche, Hare (2003). *Official (ISC)² Guide to the CISSP Exam*. Auerbach Publications. pp. 379. ISBN 0-8493-1707-X.
[7] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644–654
[8]Whitfield Diffie and Martin Hellman, "Multi-user cryptographic techniques",[Diffie and Hellman, AFIPS Proceedings 45, pp109–112, June 8, 1976].
[9] David Kahn, "Cryptology Goes Public", 58 *Foreign Affairs* 141, 151 (fall 1979), p. 153.
[10] Dieter Gollmann "*Computer Security Second Edition"* West Sussex, England: John Wiley & Sons, Ltd. 2006.
[11] Diffie, W., Van Oorschot, P.C., Wiener, M.J. Authentication and authenticated key exchanges. Des. Codes Cryptography 2(2), 107-125, 1992.
[12] Frier, A., K.P., Kocher, P.. The secure socket layer. Technical report, Netscape Communications Corp,1996.
[13] Younglove, R.. Public key infrastructure. how it works. Computing & Control Engineering Journal 12, 99-102, 2001.

