© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 05 | July - September 2017

REVIEW OF CRYPTOGRAPHY AND KEY EXCHANGE

[1]Ishu Saini,

AbstractCryptography is the science of converting the simple text into cipher text using various methods. The basic requirement of cryptography is need of secure data which satisfy the main principles like confidentiality, integrity, non-repudiationetc.We will study the basics of cryptography and its type's symmetric and asymmetric cryptography along with the key exchange problem with the conventional methods. We will also review the work related to the key exchange based on private key method in our paper.

Keywords: Key Exchange, Protocol, Cryptography, Authentication, Confidential.

I. INTRODUCTION

Cryptography is the science of information security. The meaning ofCryptography is "hidden" derived from the Greek kryptos. Cryptography means hide information in storage or transit including techniques such as microdots, merging words with image. Cryptography is the process of converting plaintext (ordinary text, just as message) using process encryption into cipher text using process decryption. This technique is used for secure communication between two parties in the presence of third party.There are four objectives for the Modern cryptography:

- **Confidentiality** (It specifies that only the participants (Sender & Receiver) should be able to access the message.)
- **Integrity** (The content of message should not be altered. If it is altered, then it is called type of modification attack)
- **Non-repudiation** (There are situation where a sender transform the content of message and after that he refuses that he had not sent the message)
- **Authentication** (The sender and receiver have to prove the identification to each other)

In recent times, cryptography is the basic requirement of the computer scientists for security purposes so that two parties can send data to each other without any alteration and confidently. So the sender and receiver can authenticate to each other for secure communication so that the information can be safely send to each other.[1]

Cryptosystem: Cryptography is the process of converting plaintext (ordinary text, just as message) using process encryption into cipher text using process decryption.Encryption is a method of transforming original data, called **plaintext** or **cleartext**, intoa form that appears to be random and unreadable, which is called **ciphertext**. That text can be understoodby a personby a computer(executable code) is called Plain text or clear text.After transformation into ciphertext, then it is impossible to process this text by human as well as machine until it is decrypted. So we can say this process is very secure due to encryption and decryption method. To protect the message from attack i.e. private and public attack, the cryptography is the basic requirement. A **cryptosystem**isthe studyof encryption and decryption techniques and this technique can be made successfulby hardware devices/program or software code in an application. Theencryption algorithms are used by cryptosystem, which describes how the process will be done or execute. Most algorithms use complex mathematical formulas for secure communication so that the third party can't calculate or find the password easily. The secret key i.e. long string of bits is used by mostly encryption methods algorithm toencrypt and decrypt the text or content of message. The set of mathematical rules or set of procedures is called algorithm. There are two types of algorithms are used for enciphering and deciphering the content of message. Many algorithms are publicly known and are not the secret part ofthe encryption process.

The way that encryption algorithms work can be kept secretfrom the public, but many of them are publicly known and well understood. The key is the secret piece for encryption and decryption algorithm. The **key** can be the long sequence of strings of bits that should be confidential between two participating parties. It should be large, complex and combination of digits, alphabets, special characters, symbols etc. so that no one excluding sender & receiver can crack it. Is it possible to crack the lengthy, complex string of bits? Not really. A **key space**is used by an algorithm, which is arange of values that can be used to construct a key.The more and more available values can beused to show different keys, when the larger the keyspace is present and it is clear that when lots of random the keys will be there, then it is very difficult forintruders to crack that. It is necessary that the entire keyspace should be used by encryption algorithm and select all the key as random as possible. This makes more possibilities for attackersto decipher the protected information. So the size of key space should be long such that the intruder cannot easily intercept the message. The protection of message depends on the secret key that will be shared between sender and receiver for secure communication in the presence of third party [2, 3].

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 05 | July - September 2017

II. TYPES OF CRYPTOGRAPHY

Thereare following type of cryptography:

Symmetric Cryptography: In a cryptosystem that uses symmetric cryptography, samekey or secret key will be used for encryption and decryption, as shown in Figure 2. This provides dual functionality. It is called same key cryptography because only one key is used or shared between two parties or participants for communication to protect the content of message. If this key is theft by attacker, then the attackercan decrypt any message with this key due to same key. It means if A (sender) and B (receiver) want to communicate to each other securely, then both have to obtain a copy of the same key. If A (sender) also wants to communicate using symmetric encryption with C and B,then A have to kept three individual keys, one for each friend. When A wants to communicate only with B, then only one lock and one key pair is required for secure communication between sender and receiver. Two lock and one key pair will be required if A wants to communicate with B and C. If B wants to communicate with other than A then B require another lock and key for secure communication.

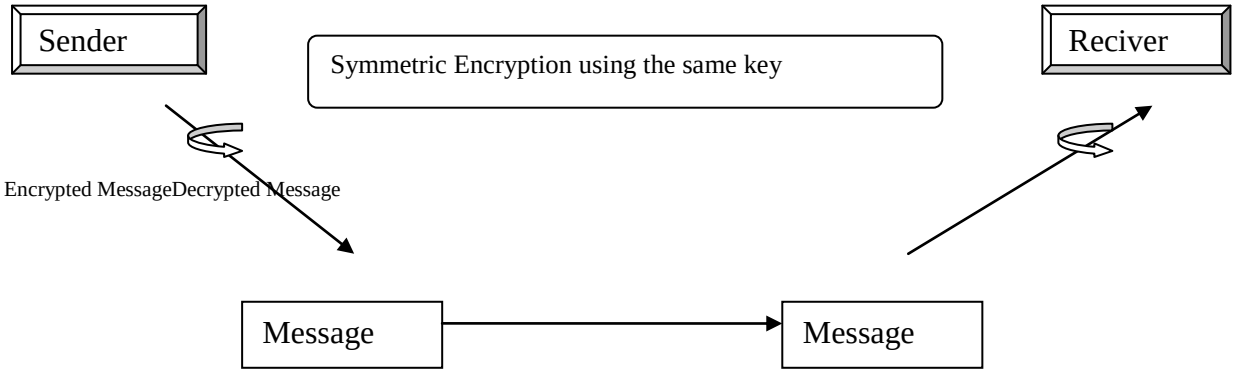

Figure 2 Symmetric Cryptosystem

B. Asymmetric Cryptography: Only a single secret key is used between two participants in symmetric key cryptography.But on the other hand in public key cryptography, each and every participant has different keys, or two keys for communication or authentication to each other. One key is used for encrypt the content of message; the other key is required to decrypt the message. In a public key cryptography or asymmetric key cryptography, the pair of keys is used: one as public key and other one as private key.

The public keycan be known to everyone, and the private keymust only be known to the owner. Figure 3illustrates an asymmetric cryptosystem. This means that if an evildoer gets a copy of Bob's public key, it does not mean he can now use some mathematical magic and find out Bob's private key. So we can say that in Asymmetric Cryptography, it provides one key pair in which one key can be used for locking and the other key is used for unlocking means fir decryption the cipher text from the original text. In this mechanism, one key will be kept as private and another one is kept as public for secure communication between sender and receiver. In this mechanism, if sender and receiver wants to communicate or authenticate to each other for the protection of content of message from third party, then receiver have to send the lock and own public key to sender. Then the sender encrypt the message to receiver with this public key and then send the message to receiver, then receiver decrypt the content of message by own private key. In this technology, only the receiver has to provide the private key for secure communication between two parties. The secure communication depends on the size of secret key, encryption/decryption algorithm and the encrypted message.

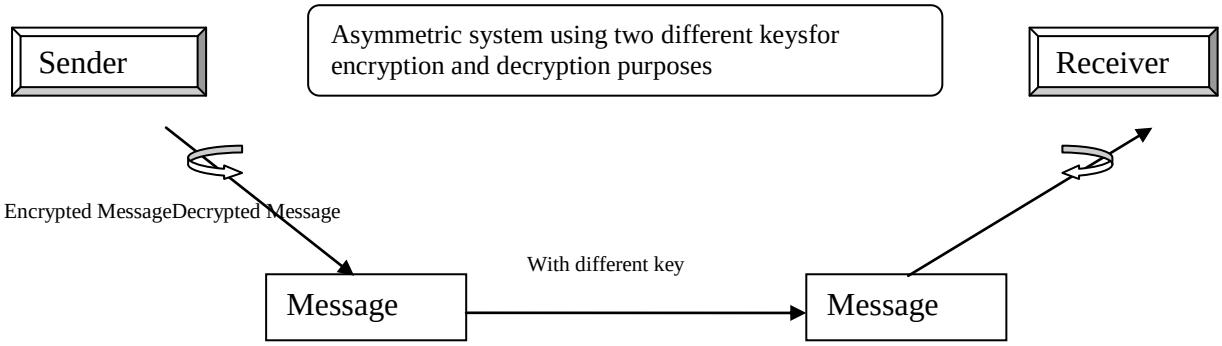

Figure 3 Asymmetric Cryptosystem[3, 4]

If B (receiver) wants to encrypt the content of message with his private key, then the decryption can be take place by copy of B's public key for transformation of cipher text into original text (plain text). It is impossible in asymmetric key cryptography to encipher and decipher of message using the exact same key. So we can conclude that asymmetric key cryptography is more secure than symmetric keycryptography.

III. POSSIBLE SENDING MODES

If we consider, the sender (A) wants to send some confidential message or information to his friend i.e. receiver (B) in the same city, but due to some circumstances they cannot approach to each other, then they can opt listed following modes:-

First Mode: The sender(A) puts the content of message in an envelope, seals it and send it by post.This is not a secure way. In this mechanism, any third person can intercept the message or open the letter before it reaches to B. This problem can be solved by courier facility. The sender can send the letter by courier. But the problem is that it is not guarantee thatthe letter is delivered to original destination (B).

Second Mode: The other method to send the messageby via hand delivery system. In this mechanism, the envelope is handed over by third person P who personally hand-over the envelope to B. This will be a better solution as compared to first mode. But it totally depend upon the trustworthiness of third party i.e. P. It is possible; P may act as intruder for A and B. If P open the envelope before it reaches to B, then the confidently message will be intercepted by P.

Third mode: A comes with a new idea. The envelope is put inside the box by Sender A, put seal on the box with a highly secure lock and then sends the box to the receiver B. Due to highly secure lock on the box, it is expected that nobody can open the box even B also.Other possibility is that the sender A can also sends the key of the lock along with the box, then the receiver B can obtain the key and open the lock and then read the content of message. But this is not very secure as if key is transformed or send with the box, then it is possible that anybody or third party can access the letter very easily.

Key Exchange Problem: In this chapter, we have studied different mode of sending the message between sender and receiver and also discussed their problems, and found that they are not complete acceptable and secure. So these problems can be solved by key exchange problem. Since the sender and the receiver will use the same key to lock and unlock, this is called as symmetric key cryptography. But due to same secret key, the problem of key distribution is arises [4].

IV. PROPOSED SOLUTIONS

Based upon symmetric key algorithm

Diffie-Hellman Key Exchange/Agreement Whitefield Diffie and Martin Hellman in 1976 had proposed key exchange or agreement algorithm. In this algorithm, the participants i.e. the

sender and receiver have to agree on a symmetric key i.e. the same key or single key can be used for encryption as well as decryption. The key is only used for key agreement purpose, not for enciphering and deciphering the message.Once the agreement of key has been taken place between participants on key, then the key can be used for encryption as well as decryption. This is the main fundamental of key exchange for secure communication over insecure medium [5].

Seo and Sweeney Key Agreement Protocolthe other algorithm is proposed by Seo and Sweeney for a simple authenticated key agreement protocol that sender and receiver (two participants) share a common password *P* before the protocol begins and uses the same public values of gand nas the original Diffie-Hellman. This algorithm purposes some solution over the provisoalgorithm [7].

Tseng's Modified Key Agreement Protocol By using a pre-shared password technique, Seo and Sweeney proposed a simple key agreement protocol which was intended to act as a Diffie-Hellman scheme with user authentication. In the Seo-Sweeney protocol, two parties who have shared a common password can establish a session key by exchanging two messages. The authors also claimed that key validation can be achieved by exchanging two more messages. Later, Tseng addressed a weakness in the key validation steps of the Seo-Sweeney protocol. By replying to the message sent from the honest party, the adversary can fool the honest party into believing a wrong session key. Tseng modified the key validation steps of the Seo-Sweeney protocol and claimed that key validation can be achieved in the modified protocol. In the Tseng's modified protocol, as in the original Diffie-Hellman scheme, the system possesses two public values n and g, where n is a large prime number and g is a generator with order n-1 in GF(n). Let Alice and Bob denote the two parties who have shared a common password P. The protocol has two phases, the key establishment phase and key validation phase[6].

Based upon Asymmetric key algorithm thereis no need of key agreement.It uses lesser number of key keys as compared to private key cryptography.It uses large keys i.e. the size of key is largeand it is slow as compared to private key cryptography. VariouskeyexchangealgorithmsuchasRSA are used and other new techniques like Idea, DES and AES are also very efficient methods of data hiding.

V.CONCLUSIONANDFUTURE SCOPE

Inthispaper, wereviewedthebasicsofcryptography along with the study of symmetric and asymmetric algorithm. We then studied the key exchange problem in detail and for both and studied the proposed methodologies with their features based on whether it is private key or public key based one. More study can be carried out on comparison of both on key exchange methods. Also studying various methods of key exchange like RSA etc. in public key cryptography and review of various transposition methods and attacks like brute force attack, dictionary attack, and replay attack can be carried out.

VI. REFERENCES

1. Cryptography concepts, URL: http://en.wikipedia.org/wiki/private_key_crptography.
2. Key exchange problem, URL: http://en.wikipedia.org/wiki/keyagreement.
3. William Stalling, "Network security and cryptography ", secondedition, PHI publications, page 25-58, 2007.
4. Atul Kahate, "Cryptography and network security" second edition, Tata McGraw-Hill, page 21-103, 2009.
5. Diffie, W., Oorschot, P.C.V., Wiener, M.J., 1992, Authentication and authenticated key exchanges, *Des. Codes Cryptography*, 2, pp. 107-125.
6. [14] Tseng, Y.M., 2005, Weakness in simple authenticated key agreement scheme, *Electronics. Letters* 36 (1) pp. 48–49.
7. Seo, D.H., Sweeney, P., 1999, Simple authenticated key agreement algorithm, *Electronics. Letters* 35 (13) pp. 1073–1079.