A REVIEW PAPER ON CRYPTOGRAPHY

Author: Imran M. Modi

Email: imranmodi.it@gmail.com

Assistant Professor - Smt. Chandramaniben Zaverchand Meghji Gosrani BCA College

ABSTRACT – In the modern era of digitalization, Networking & Wireless networks come in ICT (Information and Communication Technology), Wireless communication is open and insecure and it's very hard to keep our data confidential from intruders but this problem can be resolved by using strong cryptosystems. Cryptosystems are very useful to protect information. Cryptography plays an important role to provide different kinds of security to the user.

OBJECTIVE - The main objective of this paper is awareness of security and its requirements to the common computer users and study of number of cryptographic techniques are developed for data transmission.

Keyword - Cryptography, Cryptology, Encryption, Decryption

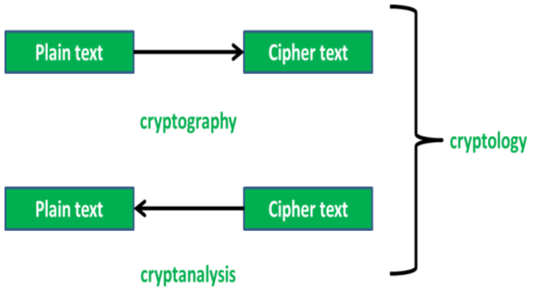
I. INTRODUCTION

Today’s our entire globe is depending on the internet and its application for every part of life. There are so many things that give facility to deal with this technology. In wireless communication we transmit our data anywhere and anytime, so it is required to secure our data with cryptography, which makes data not only unintelligible to an unauthorized person but also confidential to genuine recipients. Cryptography is the art of protecting information by sending to unauthorized malicious computer programs and applications. It provides a different kind of security goals to ensure privacy of data and data alteration on regular basis.

Some important word:

- ***Cryptography***: The Methods of making ciphers.
- ***Cryptanalysis***: The Methods of breaking ciphers.
- ***Cryptology***: The combine study of cryptography and cryptanalysis.

- ***Cryptosystem*:** A stack of algorithms and protocols for encryption, decryption, and key generation.
- ***Cryptographic System***: Any kind of system that uses cryptography.
- ***Cipher***: A Program of an algorithm that is used in a cryptosystem.



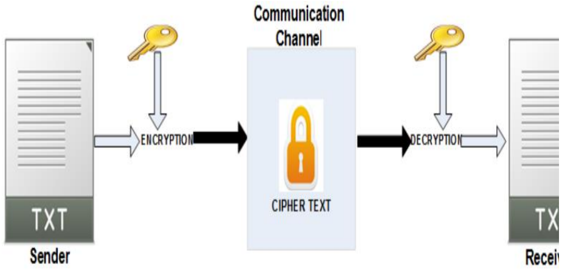


Fig. 1 represents the cryptology

Fig. 2 represents the cryptosystem

II. SECURITY OF THE DATA

Security for the data is very important during the transmission process. It is provided by cryptographic technique. It has become highly important since the selling and buying of products over the open network occur very frequently. In this paper it has been surveyed about the existing works on the encryption techniques.

III. LITERATURE REVIEW

Encryption:

Process of convert the original message or data (i.e. Plain text) into coded form (i.e. Cipher text) which cannot be accessible by third person in the absence of key information.

Decryption:

Reverse process of encryption that converts the encrypted information (i.e. Cipher text) in original form (i.e. Plain text) with the help of key information.

Purpose of Cryptography:

1) *Authentication*: To ensure that message is established with genuine sender.
2) *Confidentiality*: To ensure that message is received to genuine recipient.

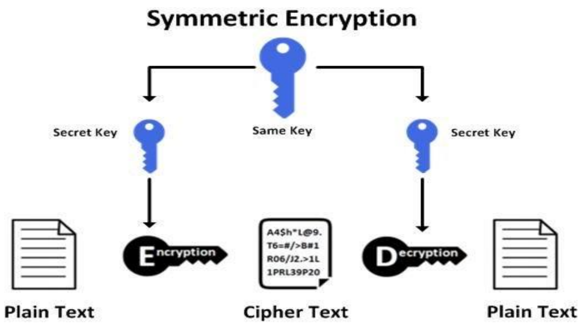
3) *Availability*: To ensure that resources should be available to authorized sender / receiver.
4) *Integrity*: To ensure that the contents of the message is unchanged during transmission.
5) *Access Control*: It specifies that who has access right to the data or resources Ex. Password, PIN.
6) *Quality of Service*: To ensures that data delivery is done in timely and accurate manner.

Types of Cryptography:-

Cryptography is being used by mankind in order to successfully transmit secret message without being caught by the enemies.

Secret Key Cryptography:

When sender and receiver uses the **same key** for both encryption / decryption. Such type of encryption mechanism is known as **Secret Key Cryptography** or **Private Key Encryption**. It is also known as **Symmetric Encryption.**



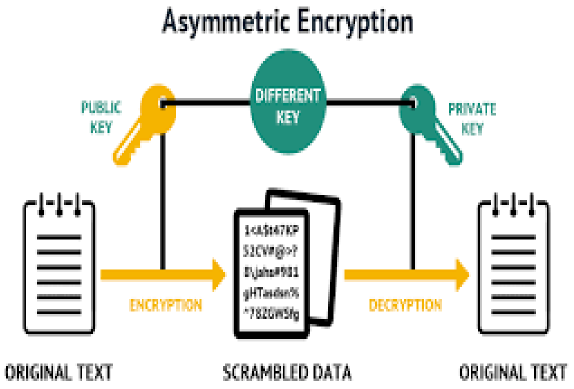
The most popular symmetric key cryptography system is Data Encryption System (DES).

Other examples are Triple DES, AES, RC5.

Fig. 4 Private Key Cryptography

Public Key Cryptography:

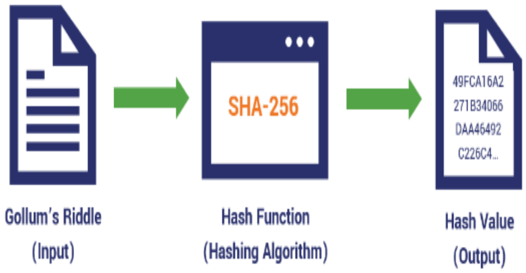
When sender and receiver uses the **two** different keys, **one key for encryption** & **another key for decryption** for example, RSA, Elliptic Curve. Such type of examples for encryption, then that mechanism is known as public key cryptography or **Asymmetric Encryption**.



If the public key is known by everyone but receiver can only decode it because he/she only knows the private key

Fig. 5 Public Key Cryptography

Hash Function



A hash function usually means a function that compress or shortens the output than the input. It takes a group of characters, which is called a key, maps it to a value of a certain length (called a **hash value** or **hash**). The hash value is represents the original string of characters, but is normally smaller than the original. This also known as a **Hashing Algorithm** or **Message Digest Function**. Many operating systems use hash functions to encrypt passwords.

For example, MD5, SHA-1, SHA-2, NTLM, LANMAN. SHA – 256 is stronger hashing algorithms.

IV. RESEARCH DESIGN

The study of these key management schemes are based on the **primary data collection** of some research papers defining some works done on cryptography for solving security issues on data transmission over the network. From the table. 1 we can analyze that each of the encryption techniques has its own strong and weak points. The scope of study is that knowledge of performance, strength and weakness of the algorithms. From the experimentally results, it is evident that the memory required for implementation is smallest in blowfish whereas it is largest in RSA. DES and AES require medium size of memory.

Comparison between different symmetric algorithms.

	DES	**AES**	**Blowfish**
Developed	1977	2000	1993

Key length	56 bit	128, 192, 256 bit	64 bit
Cipher type	Symmetrical	Symmetrical	Symmetrical
Block size	64 bit	128 bit	32 – 448 bit
Security	not good enough	Considered secure	Not so good

Table. 1

Symmetric-key cryptography is very good in providing security, but it suffers with key distribution. The confidentiality and integrity of message is most requirement for devices like mobile phone with android, windows and iPhone system, desktop or palmtop PC, Tablet and kindle.

APPLICATIONS OF CRYPTOGRAPHY:

a) Database encryption
b) Authentication/Authorization
c) Secure Network Communication
d) Banking Transactions

V. PREVIOUS PAPERS STUDY

[1] In general there are three types of cryptography. Symmetric Key Cryptography, Asymmetric Key Cryptography and Hash Function. It covers integrity, authentication and key management. Network security and system security.

[2] Author described about ciphers, service mechanism and attacks, email security, web security, system security, standard setting organizations.

[3] This author gives detail study of about classification of cryptography, Certificate-less Public Key Cryptography, awareness of email security and its requirements to the common computer users. A number of cryptographic techniques are developed for achieving secure communication. He proposed mailing system which is secure against standard security model.

[4] This paper is about comprehensive evaluation of based on different parameter. Like, cost, strengths, weakness, performance. User can choose cryptographic algorithms

based on the requirement. He had implemented and analyzed in detail cost and performance of popularly used cryptographic algorithms DES, 3DES, AES, RSA and blowfish to show an overall performance analysis & theoretical comparisons.

[5] This paper is also details study of comparative analysis for modern techniques for cryptography. Researchers contributed towards identifying best cryptography mechanisms in terms of their performance results. It measures the computational time of cryptography techniques and is further classified as encryption/decryption time, key generation, and key exchange time.

[6] This author studied about solution of efficient and reliable security needs and cryptography algorithms provides good solutions. For better security schemes mainly data confidentiality now-a-days key management is used. This paper gives a review over cryptography schemes being used to deal with security issues of wireless networks.

[7] In this paper, security analysis of two popular and practical asymmetric algorithms ECC (Elliptic Curve Cryptography) and RSA (Rivest Shamir Adleman) are done. RSA is considered as the first generation public-key cryptography.

VI. CONCLUSION

Thus concluded information that the symmetrical cryptography is not well suited for wireless network as compared to asymmetrical cryptography. Public key cryptography provides more advantages because of its low memory usage, low CPU consumption, and shorter key size. The future scope of study is that we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.

LIMITATION OF STUDY:

I presented here comparison of different symmetric algorithm with their development year, Key length, cipher type, block size and security level parameter only. Other parameters are also available to compare like speed & Elliptic Curve. Also this paper does not cover the comparison of Asymmetric encryption algorithm.

VII. REFERENCE

[1] Behrouz A. Forouzan & Debdeep Mukhopadhyay (2011), "Cryptography and Network Security", 2nd Edition, Tata MacGraw Hill Education Pvt. Ltd.

[2] William Stallings (2003), "Cryptography and Network Security", 3rd Edition, Pearson Education.

[3] A. Joseph Amalraj1, Dr. J. John Raybin Jose, 2016 "A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES", International Journal of Computer Science and Mobile Computing.

[4]Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M, 2015, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", International Conference on Information Security & Privacy (ICISP2015).

[5] Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz, Munam Ali Shah, 2017 "Cryptography: A Comparative Analysis for Modern Techniques", International Journal of Advanced Computer Science and Applications.

[6] Heena Dogra and Jyoti Kohli, 2016, "Secure Data Transmission using Cryptography Techniques", Indian Journal of Science and Technology.

[7] Dindayal Mahto, Danish Ali Khan, and Dilip Kumar Yadav, 2016, "Security Analysis of Elliptic Curve Cryptography and RSA", World Congress on Engineering.

[8] Yogesh Kumar, Rajiv Munjal and Harsh, 2014, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures", (IJAFRC) Volume 1, Issue 6.

[9] Jitendra Singh Chauhan and S. K. Sharma, 2015, "A Comparative Study of Cryptographic Algorithms," International Journal Innovation.