ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Literature Review: Cryptology and Cryptosystem

Akanksha Srivastava

Assistant Professor, Dept.of EEE, Lingayas University, Haryana, India.

ABSTRACT: The world is changed from sending data through written letters on paper via post office to instant communication via chat, email, video calls and social networking sites like Facebook, twitter and Google+ etc. Most of the data communication is via electronic system, now-a day. Communication system needs to be fully secure to avoid crook and tricky activities. Nowadays, secure programming is important and still becomes more essential. It is important to keep our data secure from adversaries. Cryptology is the method of communicate which makes data transmission secure and secret. Cryptology is required for data security or confidentiality and data integrity. This paper also represents different types of cryptanalyst attacks on cipher.

KEYWORDS: Cryptology, cryptosystem, cipher, cryptanalyst attack, symmetric key.

I. INTRODUCTION

Cryptology is the method of communicate which makes data transmission secure and secret form. The branch of the science which deals with secure communication on presence of adversaries is Cryptography. The branch of science which deals with making algorithm and codes is Cryptography and the branch of science which deals with of breaking codes or extracting the meaning is called cryptanalysis [1]. The whole system which combines cryptography and cryptanalysis is called Cryptosystem.

II. COMMUNICATION MODEL

The basic communication model which is used in cryptography depicted in Figure 1. Two parties, which are general, referred to as Alice and Bob. Alice is sender which sends data, Bob is receiver which receives data and Eve is a third person which tries to use that data. The data is sent by transferring message over an insecure channel. The channel is called insecure, because the communications happens in the presence of adversaries, or malicious adversary called Eve, whose objective is the defeat of the security services provided by Alice and Bob to secure the communication.

The first task of Eve is to detect the encrypted message, also called ciphertext, and to recover the original message, called plaintext. In addition, Eve could also try to effect Alice and to communicate to Bob a false or modified message.

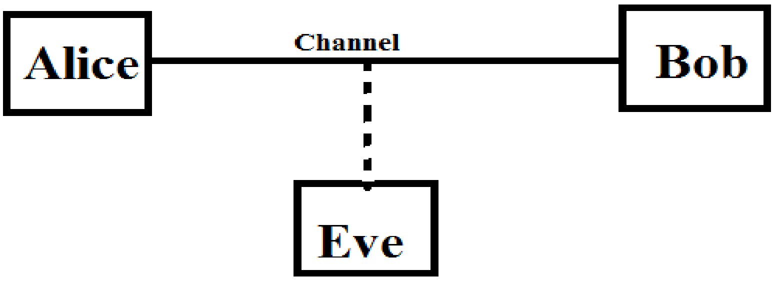

Figure 1: Basic Communication Model in Cryptography.

The main objective of the cryptographer is to find approach to secure and authenticate message. The original text is called plain text and encrypted text is called ciphertext. To generate the ciphertext from plain text a Key is used.

DOI: 10.15680/ijircce.2015.0305076

Encryption is a process which converts data plaintext to ciphertext and decryption is vice versa process. The motive of the cryptographer is to hide message from the intruder [2].

A cryptosystem is shown in figure 2. Cryptosystem is basically a network communication system which consist a message data source, an encryptor process, an insecure channel, a decryptor process, a message data destination and a secure key transfer mechanism. The motive of the cryptanalyst is to find the data and make the efforts of the cryptographer useless by breaking the cipher. To break the cryptographic scheme the person should have powerful knowledge of cipher and algebraic algorithm. A cryptanalytic attach is a procedure through which cryptanalyst gains information about the secret key.

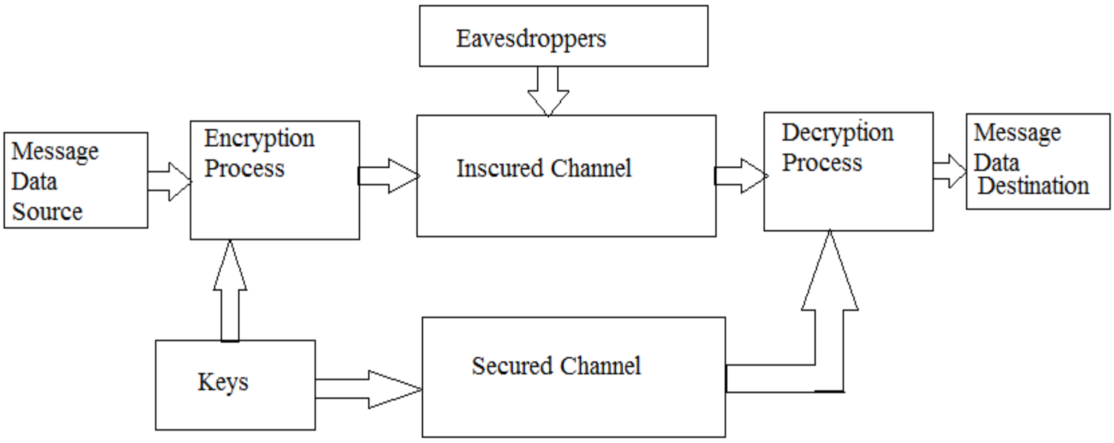

Figure 2 Secret Key Cryptography Models

III. SECURITY GOALS

The major goals that can be established in a secure communication are:

- **Privacy,** or **confidentiality**, is the process of keeping the information confidential. No other person who is not an authorized entity cannot access on it.
- **Data integrity** assures that the information has not been manipulated by unauthorized entities. Manipulation is insertion, deletion, and substitution of data.

IV. CRYPTOGRAPHY IN SOFTWARE

The great advantage of software realizations of cryptographic protocols is that they are portable to multiple platforms. Software realizations of cryptographic protocols have a fast time to market factor, but they can be applied in systems having limited traffic at low encryption rates.

- Authentication, or authenticity, is the general term for the process of corroborating the source of data (data origin authentication) and the identity of the parties (entity authentication).

- Non-repudiation is the service that prevents the denial of previous commitments or actions by an entity. In other words, the author of the message cannot deny crating or transmitting the message. With the combination of these four cryptographic goals, it is possible to derive other security objectives as access control, validation, signature, or authorization. In general, cryptography deals with the design of algorithms and protocols that are able to guarantee one or more of these security goals.

V. CRYPTANALYST ATTACK

As the level of a-prior information available to the cryptanalyst attacks are classified-

DOI: 10.15680/ijircce.2015.0305076

A **ciphertext-only attack** is an effort of the cryptanalyst to fetch original data when he has a given key, it can access cipher text, but has no access on plaintext or key.

A **known plaintext attack** is an effort of the cryptanalyst to fetch original data when he can access both plaintext and corresponding ciphertext, but not the key.

A **chosen-plaintext attack** is an effort of the cryptanalyst to fetch original data when he can choose plaintext which is to be encrypted and can access the ciphertext, but no access on the key.

A **chosen ciphertext attack** is an effort of the cryptanalyst to fetch original data when he can choose ciphertext and can fetch the corresponding plaintext. The attacker has to access the decryption device only [3,4,5].

There are two types of ciphers-

- Private-key (or secret key) used ciphers
- Public-key used ciphers

In both ciphers key is shared in different manner. In private or secret key cryptographer uses same key in encryption and decryption process. So the exchange process of key from encryptor to decryptor should be very careful. In public key cryptography the decryption process uses different key from encryption process key to decrypt the data

Public and private keys algorithm both has complementary advantages and disadvantages. Both the keys have their own specific application area. Private-key ciphers have high range throughput, but it is difficult to keep key secret at both the ends. Sound cryptographic says that for best secure communication keys should be changed frequently. In public keys algorithm the throughput is low but no need to change keys very frequently.

Practically private key cryptography is used for bulk data encryption while private key algorithm is required for efficient key management system.

VI. SYMMETRIC KEY CRYPTOGRAPHY

There are two types of symmetric key algorithms:

- Block cipher
- Stream Cipher

According to the kerckhoff's principle [5] as the key size increases the probability of success of adversary effect reduces. So as the size of key increases, the level of the security also increases.

Basically Block Cipher works on plaintext and ciphertext blocks. For a known key the plaintext block is encrypted in same cipher key block. For example, DES algorithm uses block size of 64 bit and Rijndael algorithm uses block size of 128 bit. Security level of encrypted data is mainly depends on data and key size.

The traditional **block cipher** which is used in constrained devices is DES (Data encryption standard).Other examples of block cipher is DESX, DESL, DESXL etc.

Stream Cipher is a type of symmetric key algorithm in which individual characters of plaintext are encrypted simultaneously. Stream Cipher is inferior to lightweight block ciphers. The major draw-back of stream cipher is its lengthy initialization phase in first usage. Communication protocols do not identify stream cipher. Stream cipher has simple structure and speedy hardware [5]. They are basically used in applications where the size of the plaintext is unknown. Examples of stream ciphers are RC4, E0, and AES etc.

Verman cipher is a type of stream cipher in which the length of the key is equal to message length. The encrypted text is generated by adding the message with key digit by digit.

VII. CONCLUSION

In this paper basic of cryptology and cryptosystem is introduced. There are different types of attacks on cipher that could be happened is studied. Symmetric key cryptography and block and stream ciphers are reviewed.

REFERENCES

1. A. Poschmann, "Lightweight Cryptography - Cryptographic Engineering for a Pervasive
2. World", Ph.D. Thesis, Department of Electrical Engineering and Information Sciences, Ruhr-University at Bochum, Bochum, Germany, 2009.

DOI: 10.15680/ijircce.2015.0305076

3. B.Schneier, Applied Cryptography: Protocols,Algorithm and Source Code in C, John Wiley & Sons,2001.
4. LUCA HENZEN, VLSI Circuits for Cryptographic Authentication, Diss. ETH No. 19351, 2010.
5. Debdeep Mukhopadhyay, "Design and analysis of cellular Automata Based Cryptographic Algorithm", Ph.D. dissertation, Dept Computer science and engineering. IIT Kharagpur, 2007.

BIOGRAPHY

Akanksha Srivastava is an Assistant professor in the Electrical and Electronics Department, Lingayas University, Haryana, India. She received Master of Technology (M.tech) degree in VLSI, 2014 from Amity University, Noida, India. Her research area is VLSI, cryptology etc.

DOI: 10.15680/ijircce.2015.0305076