VOLUMINOUS AMOUNT OF CRYPTOGRAPHIC METHODS AND CRYPTOGRAPHIC ATTACKS

Taranjit Kaur[1], Reecha Sharma[2]
[1]M.Tech Student, Punjabi University, UCoE, Patiala, Punjab, India
taranjit1988@gmail.com
[2]Assistant Professor, Punjabi University, UCoE, Patiala, Punjab, India
richa_gemini@yahoo.com

ABSTRACT

Today the main concern is the protection of information and it is done with encryption. It is used in almost every field of communication such as military, medical, video conferencing, broadcasting and internet communication. A cryptographed image becomes so unreadable that human eyes cannot decrypt any part of the image. Cryptography of images as compared to text is difficult due to high correlation among pixels and bulk information capacity. Cryptographic algorithm is a procedure to encrypt-decrypt message (either text or multimedia message) and to protect the encrypted message from various types of attacks. Cryptography can be done in various ways. A little knowledge is a dangerous thing, Very true in cryptography .Various cryptographic attacks are also discussed.

KEYWORDS: *Block cipher, confusion, cryptographic attacks, cryptographic methods, diffusion, stream cipher.*

I. INTRODUCTION

Communication is a spine of today's world and security of data in communication is another big necessity to be achieved. Cryptography has proved to be a boon for people in the field of communication. Cryptography is the science of hiding the data or making the data secret and secure when data is sent from one side to another over insecure channel. If encryption is done properly, it leads to approximately no leakage of information while travelling over a wireless channel. Cryptography has proved beneficial for internet communication as the whole world depends on internet for faster information transfer. A plaintext is converted to ciphertext via encryption process by applying key. Key is a secret, like a password, which is used to encrypt and decrypt information. And ciphertext is converted to plain mage by decryption process by applying same or different key [1]. If intruders are successful in decrypting the message, then inevitable situation may occurs. The main purposes of cryptography are: Authentication, Access Control, Data Confidentiality, Data Integrity, and Non-Repudiation [2].

In this paper, sections are divided as, in section 1, introduction. In section 2, various ways to do cryptography is described. Characteristics of strong encryption is discussed in section 3. In section 4, various cryptographic attacks are mentioned. In section 5, conclusion is discussed.

II. CRYPTOGRAPHIC METHODS

Cryptographic methods can be categorised into the following ways:

2.1. Operation based algorithm cryptographic methods:

Cryptographic techniques need an algorithm for encryption and decryption of images. Based on this we have:

2.1.1 Pixel position permutation based algorithm: in this algorithm, pixel positions are altered by applying certain logic [3, 4,15].
2.1.2 Value transformation based algorithm: in this, pixel intensity is changed [3,4,15].
2.1.3 Visual transformation based algorithm: by using this algorithm, the image is made so non readable that even human eyes can't decrypt any part of the image [3,4,15].
2.1.4 Monopixel Cipher: Algorithm that substitutes one number (pixel value) in the ciphertext pixel for one in the plaintext pixel.
2.1.5 Polypixel Cipher: Algorithm that substitutes a number from two or more ciphertext pixel for each plaintext pixel number based on position in the image message.
2.1.6 Modular Mathematics: also known as clock arithmetic, computes operations over a given range of values from 0 to 255. Referred to as modulo 256.
2.1.7 One-time Pads: Offer perfect secrecy if a true source of randomness is used, but is very difficult to use in practice.

2.2. On the basis of type of decryption, cryptographic algorithms can be classified as:

2.2.1 Lossy algorithm: in this the decrypted image, contains small amount of distortion, which are acceptable [5].
2.2.2 Lossless algorithm: in this decrypted image is exact replica of original image. The decrypted image is used in applications where high image quality and fine details in image are required [5].

2.3. Cryptography done on the basis of number of keys used:

2.3.1 Symmetric or private key cryptography: in such cryptography, a single key is used to encrypt and decrypt the image. Symmetric algorithms are used for maintain the confidentiality and data integrity. Even if an intruder captures the data, the intruder will not be able to manipulate it in any meaningful way [3, 5].

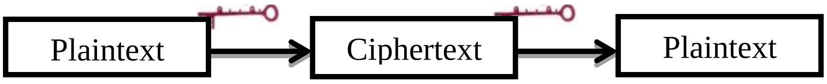


Figure 1: Symmetric key cryptography

2.3.2 Asymmetric or public key cryptography: in this cryptography, two keys are used. One key is used for encryption while other key is used for decryption [3,5].

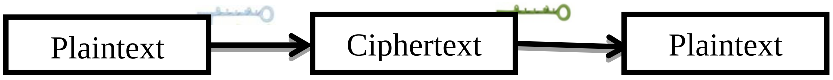


Figure 2: Asymmetric key cryptography

2.3.3 Hybrid or session key cryptography: Combines strengths of both methods symmetric and asymmetric cryptography. Asymmetric distributes symmetric key and Symmetric provides bulk encryption.

2.3.4 Hash function cryptography: it is one way cryptography. Hash functions have no key since the plaintext is not recoverable from the ciphertext. Cryptographic hashing functions are used to ensure the integrity of data. They are also known as cryptographic checksums or integrity checksums 6].

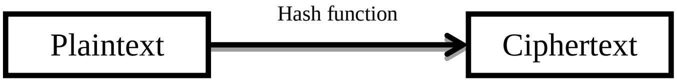


Figure 3: Hash function cryptography

2.4. On the basis of processing of original image:

2.4.1 Block cipher algorithm: a block ciphertext is a type of symmetric key encryption algorithm that transforms a fixed length block of plaintext into a block of ciphertext of same length. They are suitable for parallel processing. This processes the input one block of pixels at a time producing an output block for each input block [7]. This algorithm can be done further in two ways:

- Electronic code book (ECB): this encrypts each partitioned block independently.
- Cipher feedback chaining (CBC): in this type of encryption, ciphered block of the previous block is XORed to the next current block and then encryption is done to that block. CBC increases the security strength as all the blocks can be bonded together.

2.4.2 Stream ciphers algorithm: stream ciphertext typically operate on smaller units of plaintext, usually bits. It is much faster than a block ciphertext. This processes the input pixels continuously producing output one pixel at a time [5,7].
cipher feedback (CFB) , output feedback (OFB) , counter mode(CM) (also known as integer counter mode (ICM) and segmented integer counter (SIC) mode) are used to convert block cipher to stream cipher.

III. CHARACTERISTICS OF STRONG ENCRYPTION

The following two factors make image encryption extremely good. These are:

3.1 Confusion

It is done by changing the pixels intensities. It changes key values each round. It also complicates plaintext-key relationship [7-9].

3.2 Diffusion

It is done through shuffling of pixel. It changes the position of pixels of plaintext in ciphertext [7-9].

IV. VARIOUS TYPES OF ATTACKS

According to the Kerckhoff's Principle, key of the encryption process should be kept secret, even though everything about the encryption process is publically known. It is very difficult to decrypt the encrypted images but intruders keep on trying to crack such encryption algorithms, these efforts are known as cryptographic attacks. Cryptographic attacks destroy the security of cryptographic algorithms. They decrypt the image without prior access to a key. An intruder who has gained access to data paths decrypt (read) the message from the channel. When an intruder is eavesdropping the communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to analyse the network is generally the biggest security problem that the communicating world is facing. If encryption not done, sniffer Attack can take place. A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If packets are not encrypted properly, sniffer is used to get whole knowledge of the information. Even encapsulated packets can be broken open and read unless they are encrypted and the attacker does not have access to the key. By using a sniffer, intruder analyse the communication channel or network and gathers information or can crash or corrupt the channel [10]. So encryption has also become a necessity. Also Without strong encryption data can be read by others as it traverses the network.

4.1 Known plaintext attack:

The main task of the opponent in such attack is to find the cipher key on the basis of the obtained ciphertext segments and associated piece of plaintext [11].

4.2 Ciphertext only attack:

In this type of attack the opponent has to disclose as much plaintext as possible and even to find out the cipher key. Opponent goes to a certain channel and by a certain channel and by a certain key can decrypt some segments of the ciphertext [11].

4.3 Chosen plaintext attack:

Unlike above two attacks the opponent not only has access to some segments of the cipher and plaintext but can also choose a plaintext to encrypt and accordingly gets corresponding ciphertext that he wanted for comparison. This attack is more vigorous than the known plaintext attack [11].

4.4 Chosen ciphertext attack:

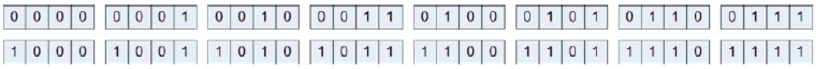
In such attack opponent chooses different parts of the ciphertext and accordingly gets its equivalent plaintext [11].

4.5 Adaptive chosen plaintext and adaptive chosen ciphertext attack:

In both these adaptive attacks the opponent or cryptanalyst chosen further plaintext or ciphertext based on previous results [11].

4.6 Brute force attack:

This type of attack is mostly used in known plaintext or ciphertext only attack. A brute force attack systematically attempts every possible key. A brute force attack on a 4-bit key. Here is an example of brute force attack on a 4-bit key [11].



0 0 0 0	0 0 0 1	0 0 1 0	0 0 1 1	0 1 0 0	0 1 0 1	0 1 1 0	0 1 1 1
1 0 0 0	1 0 0 1	1 0 1 0	1 0 1 1	1 1 0 0	1 1 0 1	1 1 1 0	1 1 1 1

Figure 4: combinations of 4 bits [11].

4.7 Compromised-Key Attack:

A key is a secret part of the encryption process. It is a secret code or number necessary to interpret secured information. To have access over the key is a tedious and resource-forcible process for an intruder. After an intruder seizes a key, that key is referred to as a compromised key. An intruder uses the compromised key to retrieve the information or can modify the information and try to use the compromised key to compute additional keys, which might allow the intruders to have access of whole communication. It is unlike brute force attack, as in brute force attack specific key size is taken and all its combination is taken to decrypt the information [10].

4.8 Man-in-the-Middle Attack:

This attack occurs when third party between two communication parties is actively monitoring, capturing, and controlling their communication transparently. In this, intruder can purposely re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. [10].

4.9 Side Channel Attack:

Side channel attacks hostility takeover additional information based on the physical implementation of a cryptographic algorithm, including the hardware used to encrypt or decrypt data. The cryptographic attack methods previously described assume that a cryptanalyst has access to the plaintext or ciphertext (sometimes both) and possibly the cryptographic algorithm. But side channel attack clouts additional information, such as time taken (or CPU cycles used), to perform a calculation, voltage used, and so on [11].

4.10 Linear Cryptanalysis:

Linear cryptanalysis is a known plaintext attack but uses large amounts of plaintext (some part of plain image) and ciphertext (some part of cipher image) pairs encrypted with an unknown key. The cryptanalyst decrypts each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext to seek the least random result. A subkey that produces the least random intermediate cipher for all ciphertexts becomes a candidate key (the most likely subkey) [11].

4.11 Birthday Attack:

It comes under the class of brute force attack. The birthday attack is an attack that can discover collisions (means same values) in hashing algorithms. It is based on the Birthday Paradox, which states that if there are 23 people in a room, the odds are slightly greater than 50% that two will share the same birthday.The odds might appear counter intuitive. The key to understanding the attack is

Remembering that it is the odds of any two people (out of the 23) sharing a birthday and it is not the odds of sharing a birthday with a specific person. Alice is in a room with 23 people and has 22 chances to share a birthday with anyone else (there are 22 pairs of people). If she fails to match, she leaves, and Bob has 21 chances to share a birthday with anyone else. If he fails to match, Carol has 20 chances, and so on. Twenty-two pairs, plus 21 pairs, plus 20… plus one pair equals 253 pairs. Each pair has a 1/365 chance of having a matching birthday, and the odds of a match cross 50% at 253 pairs. The birthday attack is most often used to attempt discover collisions in hash functions [11].

4.12 Differential cryptanalysis:

It is a chosen plaintext attack that finds a relationship between ciphertexts produced by two related plaintexts it focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm [11].

4.13 Dictionary attack:

In this attack, intruder uses dictionary containing common words to find out the password for the encryption algorithm. Words are used in their upper or lower case to create password. There are many softwares which makes dictionary attack feasible [11].

4.14 Frequency Analysis attack:

It guess values based on frequency of occurrence.

4.15 Replay Attack:

It repeats or delays the previous known values of transmitted information.

4.16 Factoring Attacks:

This attack finds keys through prime factorization [16].

4.17 Social Engineering:

In this attack humans themselves manipulates the cipher text to get plain text by frauds[17].

4.18 RNG Attack:

This attack try to Predict IV (initialization vector) used in algorithm [18].

4.19 Denial-of-Service Attack:

The denial-of-service attack inhibits the use of the processor or network by intended users. After gaining access to over the network, the intruder can do any of the below mentioned attacks [10]. Basic model of communication is:

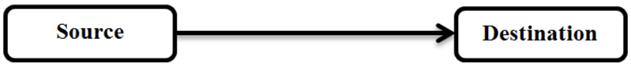


Figure 5: basic model of communication

4.19.1 Interruption attack:

In such type of attack the availability of the information is interrupted. The sender or the receiver is not allowed to send the information to the desired destination. It is so because the information is interrupted in between the transmission.

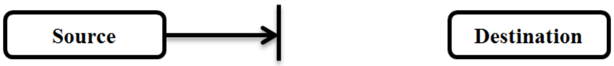


Figure 6: Interruption attack

4.19.2 Interception attack:

Interception attack is an attack on the confidentiality of the information. In this the intruder reads the information which is send from source to destination. The information is read through the routers in between the path.

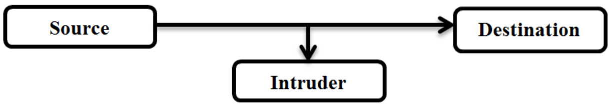


Figure 7: Interception attack

4.19.3 Modification attack:

This attack is on integrity of information. Intruder is reading packets sent by sender and making modification and sending modified information to destination or receiver.

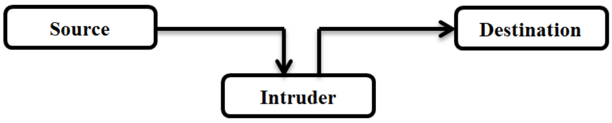


Figure 8: Modification attack

4.19.4 Fabrication attack:

This attack is on the authenticity of information. Intruder watching communication and intruder fabricate itself new packets send to destination and destination or receiver get satisfied that the packets or information is sent from the source only.

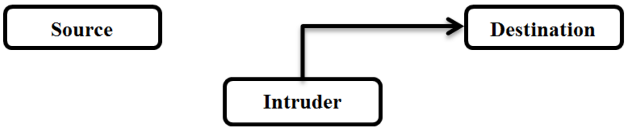


Figure 9: Fabrication attack

4.20 Application Layer Attack:

An application-layer attack points application servers by purposely causing a flaw in a server's operating system or applications. This results that intruder gaining the ability to bypass normal access controls. The intruder can read, add, delete, or modify the encryption algorithm or plain image or abnormally terminate your data applications or operating systems or introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt the systems and network or introduce a virus program that uses computers and software applications to copy viruses throughout the communication channel or disable other security controls to enable future attacks [10].

V. CONCLUSIONS

In this paper, various cryptographic methods and cryptographic attacks are discussed. Always a fast and secure conventional cryptosystem should be chosen to have high security communication.

REFERENCES

[1] Keerti Kushwaha and Sini Sibu, “ PROPOSED MODEL OF IMAGE CRYPTOGRAPHY (A DESIGNING APPROACH FOR IMAGES SECURITY)”, International Journal of Emerging Technology and advanced engineering, ISSN 2250-2459, ISO 9001:2008 certified journal, Volume 3, Issue 1, January 2013 , Page no : 144-149.

[2] Behrouz A. Forouzan, “Data Communication and Networking”, Genuine Tata McGraw-Hill 2nd edition.

[3]. Komal D Patel and Sonal Belani, “IMAGE ENCRYPTION USING DIFFERENT TECHNIQUES : A REVIEW” , International Journal of Emerging Technology and advanced Engineering , ISSN 2250-2459, Volume 1, Issue 1, November 2011 ,pp. 30-34.

[4]. Somdip dey, “SD-AEI: AN ADVANCED ENCRYPTION TECHNIQUE FOR IMAGES” , An Advanced Combined Encryption Technique For Encrypting Images Using Randomized Byte Manipulation , pp. 68-73 , 2012.

[5] Hiral Rathod , Mahendra Singh Sisodia, Sanjay Kumar Sharma, “A REVIEW AND COMPARATIVE STUDY OF BLOCK BASED SYMMETRIC TRANSFORMATION ALGORITHM FOR IMAGE ENCRYPTION”, International Journal of computer technology and electronics engineering (IJCTEE) Volume 1, issue 2, ISSN 2249-6343 ,page no : 23-30.

[6] Bart PRENEEL, “Analysis and Design of Cryptographic Hash Functions”, pdf, February 2003.
[7] Yaobin Mao and Guanrong chen, “CHAOS-BASED IMAGE ENCRYPTION”.
[8] Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine 1(3):6 – 21.
[9] Kocarev L, Jakimovski G (2001) Chaos and cryptography: From chaotic maps to encryption algorithms. IEEE Trans Circuits and Systems-I 48(2):163 – 169.
[10] Microsoft technet, library, “Common Types of Network Attacks”.
[11] Eric Conrad, “Types of Cryptographic Attacks”.
[12] Taranjit Kaur and Reecha Sharma, “TJ-ACA: An Advanced Cryptographic Algorithm forColor Images using Ikeda Mapping”, International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013, page no: 1295-1300.
[13] Taranjit Kaur and Reecha Sharma, “Security Definitive Parameters for Image Encryption Techniques”, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 5, May 2013, page no: 109-112.
[14] Taranjit Kaur and Reecha Sharma, “Image Cryptography by TJ-SCA: Supplementary Cryptographic Algorithm for Color Images”, International Journal of Scientific & Engineering Research (IJSER) Volume 4, Issue 7–July 2013.
[15] Somdip Dey, “An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2): 82-88.
[16] S. A. Danilov, I. A. Popovyan, “Factorization of RSA-180”, Moscow State University, Russia, page no: 1-5.
[17] Harley, David. 1998 Re-Floating the Titanic: Dealing with Social Engineering Attacks EICAR Conference.
[18] Leo Dorrendorf, Zvi Gutterman, Benny Pinkas, “Cryptanalysis of the Random Number Generator of the Windows Operating System”, Israel Science Foundation, page no: 1-24.

Authors

Taranjit Kaur received the Btech. degree in Electronics and Communication Engineering from the Punjab Technical University (PTU), Jalandhar, India in 2011, and pursuing her M.Tech. Degree in Electronics and Communication Engineering in Punjabi University, Patiala, India. Her research interests include cryptography, Image Processing.

Reecha Sharma did her B.tech in electronics and instrumentation engg.from MMEC Mullana, Ambala, india in 2003.M.E in Electronics, instrumentation and control Engg. From Thapar University Patiala,india in 2005.She has seven year of teaching experience. She has guided three M.tech students. At present she is working as assistant professor (ECE) University College of engg. Punjabi university Patiala, India.