IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

Comparative Study on Various Cryptanalysis Attacks in Cryptography

G. Kishore Kumar[1], Dr. M. Gobi[2]

Research Scholar, Department of Computer Science, Chikkanna Government Arts College, Tiruppur, India[1]

Assistant Professor, Department of Computer Science, Chikkanna Government Arts College, Tiruppur, India[2]

Abstract: Security is the major concern in the modern era in all areas of applications and has become more challenging issue in many areas like computers, communications etc. The data protection is one of the critical/important nowadays, as guaranteed data, protection is required and there are still a lot of challenges in this area even though many techniques are proposed/recommended for Security. Cryptography is a most prevalent technique, that can ensure of integrity, availability and identification, confidentiality, authentication of user and as well as security and privacy of data can be provided to the user. Cryptanalysis is known as breaking the cipher, ciphertext, or cryptosystem. This paper enlightens the various attacks in Cryptanalysis and how they can be addressed that would helpful in addressing the security issues, in which our research would be focusing.

Keywords: Cryptography, Algorithms, Cryptanalysis, Public Key, Private Key, Symmetric, Asymmetric, Ciphers, Attacks.

I. CONCENPT OF CRYPTOGRAPHY

A. Introduction

Cryptography term is originally from the Greek words κρυπτο, means hidden/Secret and γραφη means writing. Its history periods are back to about 2000 B.C and it's about the study of secret writing scientifically. Cryptography is one of the ancient/olden methods engaged by ancient civilizations for secret method of communications. Particularly the Egyptians are known to have used cryptography on the tombs of deceased kings and rulers. Julius Caesar invented a process called as CAESAR CIPHER for sending secret/confidential messages to his generals during wars. This was one of the prominent methods in the history of Cryptography, which was very easy and fast. This was implemented by the substitution cipher method with alphabet shifts of 3, which would for example shift an "A" to "D" or a "B" to "E".[6]
Nowadays Cryptography uses intricate scientific approaches and the algorithms are designed for cryptosystems based on computational resistance/stability due to which the hackers/challenger will not be able to break into the system. In addition, a modern cryptosystem talks about the design and analysis of various procedures/techniques, which are interrelated, to various aspects such as authentication, data security and integrity. [5]

The encryption algorithms play vital role and acting as necessary tool for data protection and secured network communication. The encryption algorithms convert the data into jumbled form by using the "key" and the user only using the same key can do the decryption.[4]

The following diagram explains the working principle of cryptography/crypto-system in general:

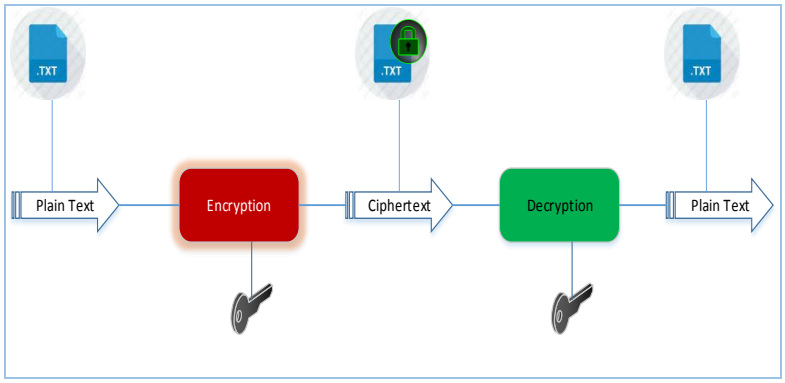

Fig. 1 Cryptography

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

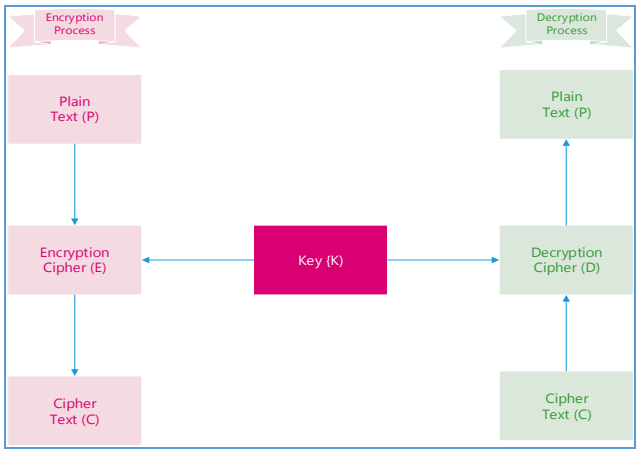

Fig. 2 Cryptography working principle

To ensure that a particular system is secure, the cryptanalysts will try to break the ways/techniques used to build that particular system.

B. Terminologies used

- *Plaintext*: The original data is known as plaintext
- *Cipher text*: The Encryption data or un understandable data is called cipher text
- *Encryption*: The process of converting plaintext to ciphertext
- *Decryption*: The Process of Converting Cipher text to plaintext.
- *Key*: In cryptography keys are two types on Conventional key or Symmetric key or private key and Asymmetric key or public key
- *Encryption algorithm*: A plain text is encrypted using an algorithm.
- *Decryption algorithm*: A cipher text is decrypted using an algorithm.
- *Key space or Key length (size of key)*: The security level of cryptography is determined by this.
- *Block cipher*: The data is in the form of Blocks.
- *Stream Cipher*: The data is in the form of streams.
- *Symmetric key*: Both sides of Sender and receiver use the same key.
- *Asymmetric key*: Two keys one is public key and private key.
- *Cryptanalysis*: The study of ciphertext in an attempt to restore the message to plain text.

C. Types of Cryptography[6]

The Crypto-System is defined as any system, which comprises cryptography. The security of such system majorly depends upon the below given factors:

- Type of algorithms used
- Number of keys in the algorithm
- Number of rounds Etc.

1) **Symmetric Key Cryptography**

The following diagram explains about the Symmetric key cryptography where in the same key will be used for both encryption and decryption, which will be shared with the received for decryption. Both the sender & receiver agree for the same key usage.

There are main services provided by Symmetric Cryptography that deal with storing/transmitting the data. The following are the services in this:

- *Confidentiality*: keeping the data secret.
- *Integrity*: keeping the data unaltered.
- *Authentication*: to be certain where the data came from.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

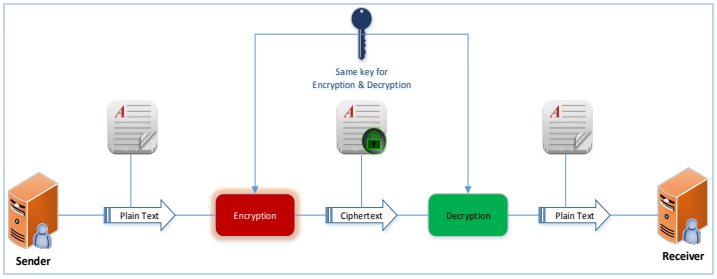

Fig. 3 Symmetric Key Cryptography

2) **Asymmetric Key Cryptography**

The following diagram illustrates about asymmetric key cryptography in which two different keys will be used for encryption and decryption. The sender uses a key to encrypt the plaintext, and another one to decrypt the cipher text. One of these keys is distributed or public and the other one is kept as private key.

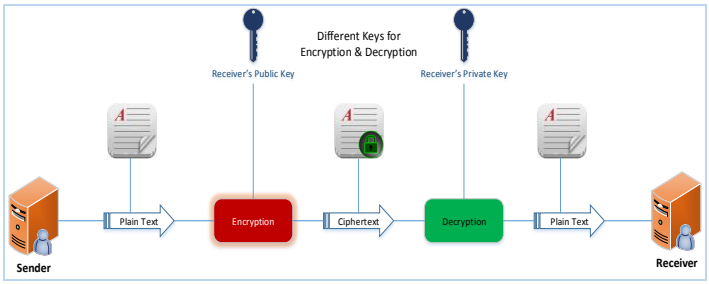

Fig. 4 Asymmetric Key Cryptography

D. Classification of Ciphers

Based on input data, ciphers are classified as follows:

- Block ciphers, which encrypt block of data of fixed size
- Stream ciphers, which encrypt continuous streams of data.

Classical ciphers used substitution and transposition for encryption and decryption. The rotor machine is a device that is used to encrypt and decrypt secret messages. It is a stream cipher device and electro-mechanical in nature. The following diagram illustrates the classification of ciphers:

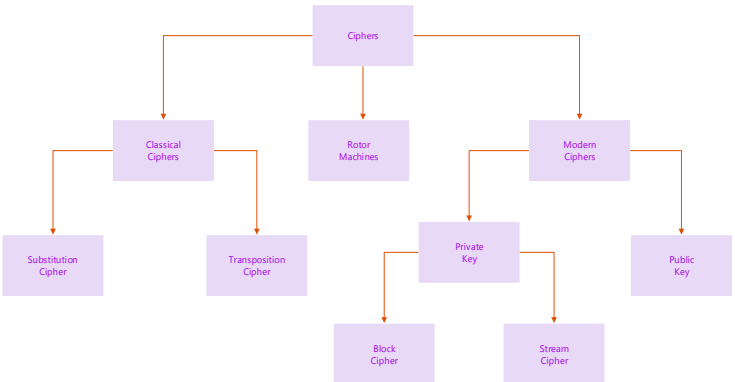

Fig. 5 Classification of Ciphers

E. Main Objectives of Cryptography

The following are the main goals/objectives of Encryption/Cryptography that needs to be achieved for user benefits:

- *Confidentiality*: The information cannot be understood by anyone for whom it was unintended.
- *Integrity*: Either in storage or in transit between sender and the anticipated receiver, the information cannot be altered by without the alteration being detected.
- *Non-repudiation*: The information creator or sender cannot disagree at a later stage the intentions in the creation/transmission of the information.
- *Authentication*: Both the sender and receiver can confirm on each other's identity and on the information's origin/destination.
- *Access Control*: To avoid unauthorized user access, the data be accessed only by authorized users.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

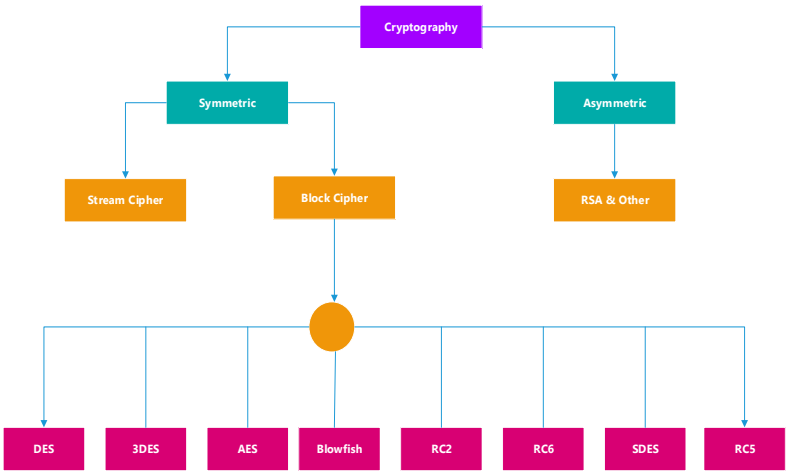

Fig. 6 Objectives of Cryptography

II. CRYPTANALYSIS

A. Introduction

The study of ciphers/ciphertext or cryptosystems is called as Cryptanalysis wherein the way of finding weakness in them by which the retrieval of plaintext from ciphertext, and the key or the algorithm also will not be known/visible. This is otherwise popularly known as breaking the cipher/ciphertext or cryptosystem.
The science of cracking codes and decoding secrets is called as cryptanalysis, which is used to disrupt authentications schemes. In addition, this is used to break cryptographic protocols, moreover to discover and correct weakness in the encryption algorithms. Sometimes breaking is used interchangeably with weakening which refers to a property finding (fault) in the design/implementation of the cipher. This will reduce the number of keys required in a brute-force attack, which is nothing other than trying every possible key till the correct one is found. For example, assume that a symmetric cipher implementation uses a key length of 2^128 bits (2 to the power of 128): this means that a brute force attack would be trying up to all 2^128 all possible combinations/rounds to find a certain the correct key, otherwise on an average of 2^127 combinations for converting the ciphertext to plaintext, which is impossible in the given present and near future computing capabilities. However, the cipher which is weaker and the plaintext can be found with moderate computing resources when not completely broken, wherein a technique that allows a plaintext would be found in 2^40 rounds.

This may be used in information welfare applications, for example forging an encrypted signal to be accepted as authentic. Challengers/Competitors, who will be able to discover the key, now will send fake/bogus encrypted messages to use this as advantage. Also this could be used to pretend that this message has come from official source.
According to Diffie and Hellman, Skill in the production of cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from amateurs. [7]

B. Types of Attacks

There are various technical and non-technical cryptography attacks for which the systems are victim/target. The cryptanalytic attacks can be involved beside any encryption algorithms, but also with various other algorithms like MACing algorithms, digital signature algorithms and pseudo-random number generators.[8]

The attacks are categorized into two major parts based on the action performed by the attacker as given below:

1) **Passive Attacks**
The core objective of a passive attack is to acquire unauthorized access to the information, such as actions like intercepting/interrupting and eavesdropping on the communication channel that is being regarded.
These are passive in nature, as they never affect information and the communication channel as well. A passive attack is commonly referred as stealing information, wherein the only difference between stealing physical goods and information is stealing of data still lies with the owner who possess the data. Moreover, this attack is considered as more dangerous as the information owner will not be able to notice the theft.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

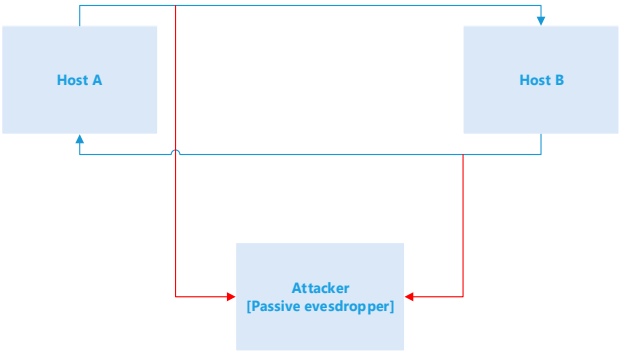

Fig. 7 Passive Attacks

2) **Active Attacks**

An active attack is considered as when any information is changed by conducting some process on it, such as modification is done in an unauthorized manner, unintended/unauthorized transmission of information, alteration of authentication data like originator name/associated timestamp with data deletion & denial of service for data access.

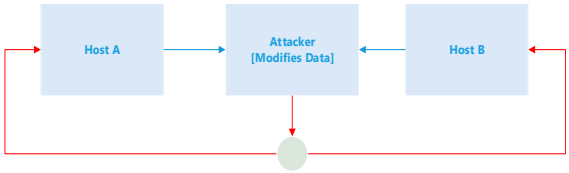

Fig. 8 Active Attacks

There are many tools/techniques proposed by cryptography in the area of carrying-out cryptosystems implementation that are proficient in inhibiting most of the attacks given above. It is very much essential to know about the concerned environment when the cryptosystems attacks are considered wherein the assumptions and knowledge about the environment decides the proficiencies. The following describes about the above said details: [8]

- Details of the Encryption Scheme
- Availability of Ciphertext
- Availability of Plaintext and Ciphertext

C. Cryptographic Attacks [8][9]

The aim of an attacker is to break & find-out a plaintext out of a ciphertext in a cryptosystem. For attaining the plaintext, the attacker needs to find out the secret decryption key wherein the algorithm is already in the public domain. Hence, the attacker applies his maximum effort to find-out the secret key applied in the concerned cryptosystem. The attacked system is considered as broken/compromised when the attacker is able to define the key.

The following are the various types of attacks in cryptanalysis:

- Ciphertext Only Attacks - COA
- Known Plaintext Attack - KPA
- Chosen Plaintext Attack - CPA
- Dictionary Attack
- Brute Force Attack - BFA
- Birthday Attack
- Man in Middle Attack - MIM
- Side Channel Attack - SCA
- Timing Attacks
- Power Analysis Attacks
- Fault analysis Attacks

a) Ciphertext Only Attacks [COA]

The attacker will have access to a set of ciphertexts, wherein there will be no access to corresponding plaintext in this method. This method becomes success when the relevant plaintext can be derived from the available ciphertexts. The encryption key will be determined occasionally in this attack. The latest cryptosystems are secured against these attacks.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

b) Known Plaintext Attack [KPA]

The attacker will be familiar with the plaintext on some parts of the ciphertext. The objective is to decrypt the remaining ciphertext by using this information, wherein this would be done by determining the key or by some other method. Linear cryptanalysis is the finest example of this attack against block ciphers.

c) Chosen Plaintext Attack [CPA]

The attacker has the text of his own encrypted, as he would be having the ciphertext-plaintext pair of his own which makes his task simpler in determining the encryption key. The differential cryptanalysis applied against block ciphers and hash functions as well is an example of this attack. The RSA, which is a popular public key cryptosystem, is also vulnerable to this attack.

d) Dictionary Attack

This attack involves compilation of a 'dictionary', wherein this is a simplest method of attack. Here the attacker generates a dictionary of ciphertexts with corresponding plaintexts based on his experience over a period of time. Whenever any ciphertext is received, he tries to find out the relevant plaintext from the dictionary.

e) Brute Force Attack [BFA]

The attacker attempts to define the key by attempting all probable keys. The number of possible keys is 28=256 when the key is 8 bits long. The time required to complete the attack would be very long as the attacker tries to find the decryption text with all the possible 256 keys.

f) Birthday Attack

This attack is considered as a variant of brute-force technique as this is used against the cryptographic hash function. The reply would the one of the possible 365 dates when any student in a class is asked about the birthday. For example, if the first student's birthday is 17th Oct., then we need to enquire $1.25^* \sqrt{365} \approx 25$ students to find the next student whose birthday is 17th Oct.

g) Man in Middle Attack [MIM]

The aim of this attack is mostly on the public key cryptosystems wherein the key exchange is involved before the communication happens. For example, A wants to communicate with B & requests public key of B, wherein an attacker intercepts this and sends his public key instead. Hence, the attacker is able to read whatever A sends to B. The attacker re-encrypts the data after reading with his own public and sends to B. The attacker shares his public key as A's.

h) Side Channel Attack [SCA]

This attack is used to exploit the weakness in cryptosystem's physical implementation and this is not against any particular cryptosystem/algorithm.

i) Timing Attacks

This attack exploit about the timings on the computations that varies from processor to processor, by which the particular computation carried out by a processor will be known. For example, if a secret key is long then it indicates that encryption takes a longer time.

j) Power Analysis Attacks

This attack is similar to timing attacks, only the difference is on the amount of power consumption is used which is used to obtain the information on the underlying computations.

k) Fault analysis Attacks

In this attack, the attacker analyses the resulting output from the errors induced in the cryptosystem for any kind of useful information.

l) Chosen Ciphertext attack [9]

The attacker has the able to select any ciphertext and study the plaintext produced by decrypting them.

m) Implementation Attacks [9]

These attacks have a different approach in discovering the secret key, wherein the physical phenomena in hardware is considered than attacking the mathematical properties of the algorithm.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 1, January 2018

III. CONCLUSION / FUTURE RESEARCH DIRECTIONS

Encryption algorithms play vital role in overcoming the security issues by use of various cryptographic techniques available. Our future research would be focusing on enhancement of any of the cryptographic techniques for highly secured data, which is practical. This paper has highlighted about various types of cryptanalysis attacks available. Based on this, in future, we aim to conduct various experiments to evaluate the performances of few algorithms, which would help in ensuring high-level security.

REFERENCES

[1] Contel Bradford, "Common Encryption Algorithms and the Unbreakables of the Future"
[2] Rajdeep Bhanot, Rahul Hans,"A Review and Comparative Analysis of Various Encryption Algorithms",International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306
[3] Nigel Smart,"Cryptography: An Introduction (3rd Edition)"
[4] Dr. M.Gobi,Kishore Kumar G," Comparative Study on Blowfish & Twofish Algorithms for Cloud Security", International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 3 Issue 9, September 2017 pp. 1 – 11
[5] Jyotirmoy Das,"A Study on Modern Cryptography and their Security Issues",International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 10, October 2014
[6] G.Kishore Kumar, Dr.M.Gobi,"Role of Cryptography & its Related Techniques in Cloud Computing Security",International Journal for Research in Applied Science and Engineering Technology,IJRASET,Volume 5 Issue VIII (August 2017)
[7] Neha Tirthani & Dr.Ganesan R,"Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography"
[8] "ATTACKS ON CRYPTOSYSTEMS", www.tutorialspoint.com
[9] Dr. S.B. Sadkhan, "Security of Networks",2011-12
[10] Kalyani P. Karule, Neha V. Nagrale,"Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security",International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016
[11] Rajdeep Bhanot, Rahul Hans,"A Review and Comparative Analysis of Various Encryption Algorithms",International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306
[12] Contel Bradford, "Common Encryption Algorithms and the Unbreakables of the Future"

BIOGRAPHIES

G. Kishore Kumar – Research scholar in Department of Computer Science, Chikkanna Government Arts College, Tirupur, India. He has completed Master of Computer Applications [MCA] in Alagappa University, Karaikudi, India. His major field of study in Network Security and Cryptography.

Dr. M.Gobi – Associate Professor in Department of Computer Science in Chikkanna Government Arts College, Tirupur, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Cryptography, Java, Software Engineering and Information Systems Security.