Cryptographic Technique
for Communication System

Synopsis

Shivam Vatshayan

Admission No.: 16SCSE101566

Under the Supervision of

Dr. Raza Abbas Haidri

GALGOTIAS
UNIVERSITY

School of Computing Science and Engineering
Greater Noida, Uttar Pradesh
Winter 2019-2020

TABLE OF CONTENTS

Abstract

In today's world Sensitive data are increasingly used in communication over the internet. Thus Security of data is the biggest concern of internet users. Best solution is use of some cryptography algorithm which encrypts data in some cipher and transfers it over the internet and again decrypted to original data. The field of cryptography deals with the procedure for conveying information securely. The goal is to allow the intended recipients of a message to receive the message properly while interrupt eaves-droppers from understanding the message. Key arrangement schema allows communicating parties to establish a shared cipher key. This paper provides a survey to data security problem through Cryptography technique. Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data classified and for verifying data indignity. While our conventional cryptography methods, such for AES (encryption), SHA-256 (hashing) and RSA/Elliptic Curve (signing), work well on systems which have reasonable processing power and memory capabilities, these do not scale well into a world with embedded systems and sensor networks. Thus, lightweight cryptography methods combined to form Complex and secure Hybrid Cipher is proposed to overcome many of the problems of conventional cryptography. This includes constraints related to physical size, processing requirements, memory limitation and energy drain.

1. Introduction

Information security can be summed up to info, a group of steps, procedures, and strategies that are used to stop and observe illegal access, trouble-shooting, revelation, perturbation and adjustment of computer network sources. Enhancing the privacy, eligibility and reliability of the work requires a lot work to strengthen the current methods from constant trials to break them and to improve new ways that are resistant to most kinds of attacks if not all. Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since the ancient days of the Romans who used similar methods to enable security on their valued information and documents. Data encoding is the process of changing the form of the data into certain symbols through the use of meaningless codes.

Cryptography is the art of creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it.

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

1.1 Overall Description:

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today's age of computers, cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

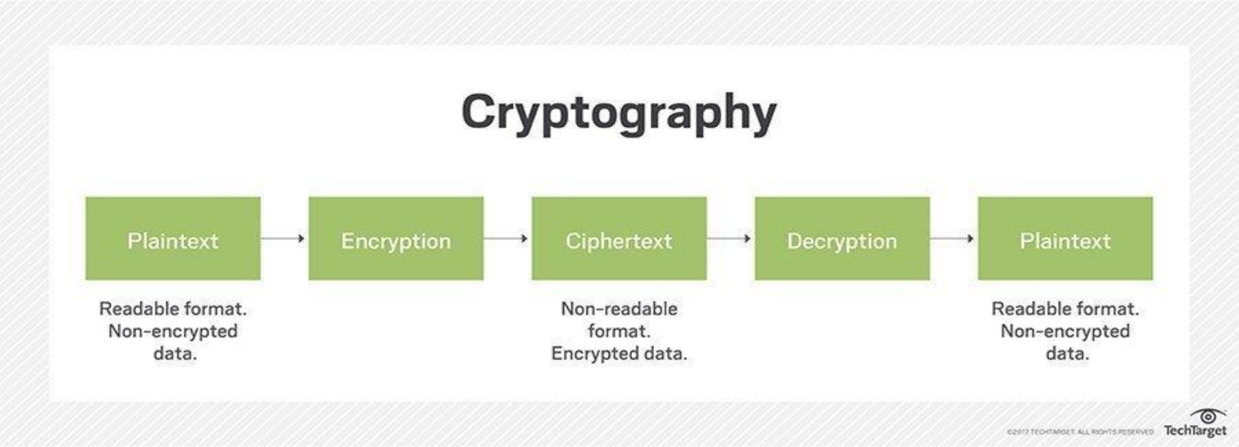
Features of Cryptography: These are mentioned below.

- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types of Cryptography: In general there are three types of cryptography which are explained as follows.

- **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

- **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
- **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
©2017 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Components of a Cryptosystem: The various components of a basic cryptosystem are as follows:

- **Plaintext.** It is the original data to be protected during transmission.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on

public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**. An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

1.2 Purpose: In digital world cyber-attacks are very frequent. Any social networking site, web application, etc are more prone to attacks. Some of the attacks are given as follows.

Cryptographic Attacks: The basic intention of an attacker is to break a cryptosystem and to find the plaintext from the ciphertext. To obtain the plaintext, the attacker only needs to find out the secret decryption key, as the algorithm is already in public domain.

Hence, he applies maximum effort towards finding out the secret key used in the cryptosystem. Once the attacker is able to determine the key, the attacked system is considered as broken or compromised.

Based on the methodology used, attacks on cryptosystems are categorized as follows −

- **Ciphertext Only Attacks (COA)** − In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.
- **Known Plaintext Attack (KPA)** − In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.
- **Chosen Plaintext Attack (CPA)** − In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions. A popular public key cryptosystem, RSA is also vulnerable to chosen-plaintext attacks.

- **Dictionary Attack** − This attack has many variants, all of which involve compiling a ‘dictionary’. In simplest method of this attack, attacker builds a dictionary of ciphertextsand corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.

- **Brute Force Attack (BFA)** − In this method, the attacker tries to determine the key by attempting all possible keys. If the key is 8 bits long, then the number of possible keys is 2^8 = 256. The attacker knows the ciphertext and the algorithm, now he attempts all the 256 keys one by one for decryption. The time to complete the attack would be very high if the key is long.

- **Man in Middle Attack (MIM)** − The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.
    - Host *A* wants to communicate to host *B*, hence requests public key of *B*.
    - An attacker intercepts this request and sends his public key instead.
    - Thus, whatever host *A* sends to host *B*, the attacker is able to read.
    - In order to maintain communication, the attacker re-encrypts the data after readingwith his public key and sends to *B*.
    - The attacker sends his public key as *A*’s public key so that *B* takes it as if it is taking it from *A*.

- **Side Channel Attack (SCA)** − This type of attack is not against any particular type of cryptosystem or algorithm. Instead, it is launched to exploit the weakness in physical implementation of the cryptosystem.

- **Timing Attacks** − They exploit the fact that different computations take different times to compute on processor. By measuring such timings, it is be possible to know about a particular computation the processor is carrying out. For example, if the encryption takes a longer time, it indicates that the secret key is long.
- **Power Analysis Attacks**: These attacks are similar to timing attacks except that the amount of power consumption is used to obtain information about the nature of the underlying computations.

- **Fault analysis Attacks**: In these attacks, errors are induced in the cryptosystem and the attacker studies the resulting output for useful information.

1.3 Motivation: Inorder to tackle above mentioned attacks, we need a very sound communication system. This system ensures the security parameters such as Confidentiality, Integrity and Authentication.

3. Literature Survey

Many Cryptographic Algorithms such as RSA, AES, DSA and EWS as Symmetric and asymmetric are commonly used in security of message. But Now a days many attacks are defined which occur as breaking of security protocol that result in huge data stealing and replication. This threats and attacks are getting stronger So, There is need of Manipulative defined hard string algorithms that will acts are wall for stoppage and ban of several threats and attacks. RSA algorithms are based on prime number that are very large (100 or more digits)[1][2]. There are basically three steps in RSA algorithms like selection and generation of the public and private keys, encryption and decryption process[1][2] But still it get penetrated and broken. AES goes through different rounds as 10 rounds for 128 bit, 12 rounds for 192 bits[3] but still get saturated at one point. Bluetooth uses E0 Algorithm for communication transmission but it is still vulnerable as threats in between replicate the copy of messages.[3]. So, After Research on this sole cryptographic algorithms I came to know If we have to Increase the Strength of System then must try on Hybrid and ciphers algorithms that can be used to for different purposes and for proper protection of system.

4. Problem Statement

Cryptographic System had formatted, design, generated and implemented new version of secure Ciphers for encapsulating message and data from time to time with few or more changes. But Every Single New ciphers goes in two scales such as –

- Simple or Complicating: This Cipher are made for sub small system for less value security purpose but ciphers formation in any part as direct simple or complicating with use of many subsystem inside it.
- Time or Cost Consuming: This Cipheris made and then result in time consuming logic for Ciphers as execution of process of decoding.
- Independent Ciphers Demerits are-
    - Easy to Attack
    - New ways formation to tackle the line of security
    - Fault evolution
    - Key can be obtained through sub manual process
    - Easy trapping & Jamming of system

So, we can get to know that different cipher and algorithm if It is used then It can be broken or a change unknowingly with different types of attacks in system during communication.

5. Proposed Model

Cryptographic Model will be build using Hybrid Algorithm that will act like giant soldier to protect the data Integrity, Confidentiality and uniqueness from or In during transmission and communication of messages from sender to receiver or vice-versa.

It will work as in 2 Phases:

- 1st Phases- Running & Implementing sole Ciphers
- 2nd Phases- Combination of more than 2 Ciphers for Hybrid Algorithm

References

1. Chowdhury, Z.J., Pishva, D. and Nishantha, G.G.D. (2010) AES and Con - dentiality from the Inside Out. The 12th International Conference on Advanced Communication Technology (ICACT), 2, 1587-1591.

2. Rege, K., Goenka, N., Bhutada, P. and Mane, S. (2013) Bluetooth Commu-nication Using Hybrid Encryption Algorithm Based on AES and RSA. Interna-tional Journal of Computer Applications, 71, 10-13.

3. Bluetooth Security White Paper. Bluetooth SIG Security Expert Group.Downloadable from: (last visited: May 26, 2017) http://grouper.ieee.org/groups/1451/5/Comparis on

4. https://en.wikipedia.org/wiki/Cryptography

5. http://ijcsn.org/IJCSN-2017/6-3/A-Literature-Survey-on-Efficiency-and-Security-of-Symmetric-Cryptography.pdf

6. http://www.ijsrp.org/research-paper-0718/ijsrp-p7978.pdf

7. https://www.ijcsmc.com/docs/papers/August2016/V5I8201615.pdf

8. https://www.tutorialspoint.com/cryptography/attacks_on_cryptosystems.htm

9. https://www.geeksforgeeks.org/custom-building-cryptography-algorithms-hybrid-cryptography/

10. https://www.ripublication.com/ijaer17/ijaerv12n19_104.pdf

11. https://searchsecurity.techtarget.com/definition/cryptography