ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 5; Issue 2; March-April: 2017; Page No. 15-18

Introduction of Cryptography

Megha Chhabra[1], Vineet Chhabra[2]

[1] Assistant Professor, Computer Science department, S.S jain subhod PG college jaipur

meghaagarwal108@gmail.com

[2] Assistant Professor, Electronic and Communication department, Anand International college of Engineering kanota

vineetchhabra1986@gmail.com

Abstract

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties. Cryptography is about constructing and analyzing protocols that prevent third parties or from the public to access private messages various aspects in information security such as data confidentiality, data integrityand authentication. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and digital communication engineering. Applications of cryptography include ATM cards, military encryptions, computer passwords, and electronic commerce.

Keywords: cryptography; Symmetric Key; Asymmetric Key; Encryption and decryption; hash function; Public key; Enigma Machine.

I. Introduction

Human being had two inherent needs: (i) to communicate and share information and (ii) communicate selectively. These needs rise the ways to encrypt the messages in such a way that only the intended people can access the information. Unauthorized people never extract any information, even if the scrambled (encrypted) messages fell in their hand.

The art or science of concealing the messages/information to introduce secrecy in information security is known as cryptography.

The word 'cryptography' was combination of two Greek words, 'Krypto' and 'graphene' meaning hidden writing.

II. History of Cryptography

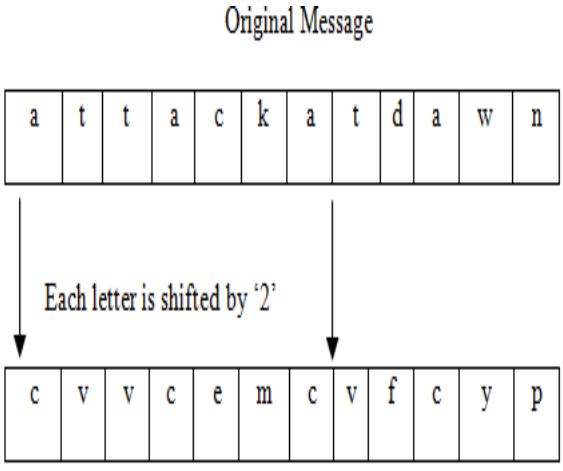
The art of cryptography is born with the knwoledge of writing. As civilizations evolved, human led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography.

The roots of cryptography are found in Roman and Egyptian civilizations.

Hieroglyph – The Oldest Cryptographic Technique

The first evidence of cryptography can be traced some 4000 years ago, the Egyptians used to communicate by messages which are written in hieroglyph. This codes was the secret known only to the scribes who used to transmit messages on behalf of the kings.

Later, during the 500 to 600 BC the scholars moved on to using simple mono-alphabetic substitution ciphers. This secret rule involved replacing alphabets of message with other alphabets. This secret **rule** became a **key** to retrieve the secret message back from the garbled message.



Corresponding author: Megha Chhabra

The Romans popularly known cryptography method Caesar Shift Cipher, relies on shifting the letters of the message by number (common choice was three), the recipient of this message would then shift the letters back by the same number to obtain the original message.
Secret Message

Steganography

Steganography adds another dimension in the world of cryptograph. In steganography, peoples not only want to protect or hide the important data by concealing it, they also want to make sure any unknown person never gets any evidence that the information was ever exists.

Examples are **invisible watermarking**.

The uses of steganography cryptography can be traced in 440 BC.

Evolution of Cryptography

After the European Renaissance, various Italian and Papal states led the rapid proliferation of cryptographic techniques. Various analysis and attack techniques were researched in this era to break the secret coded information.

- In the 15th century improved advanced coding techniques such as **Vigenere Coding** came into existence, which offered moving letters in the message with a number of variable places instead of moving them the same number of places.

- Only after the 19th century, cryptography evolved from the ad hoc approaches to encryption to the more sophisticated art and science of information security.

- In the early 20th century, during the world wars the invention of mechanical and electromechanical machines, such as the **Enigma rotor machine**, provided more advanced and efficient means of coding the information.

- During the period of World War II, both **cryptography** and **cryptanalysis** became excessively mathematical.

With the advances taking place in this field, government organizations, military units, and some corporate houses started adopting the applications of cryptography to guard their security systems.

III. MODERN CRYPTOGRAPHY

Modern cryptography is focused on the computers and communications security. The foundation of modern cryptography is based on various concepts of mathematics e.g. number theory, computational-complexity theory, and probability and statistics theory.

Encryption and decryption

Data or any information that can be read and understood without any special information is called plaintext or clear text. The method of disguising clear text in such a way to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to ensure that information is hidden from peoples for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption.

Modern Symmetric Key Encryption

Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert in to another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified in to :

1. Block Ciphers
2. Stream Ciphers.

The primary objective of using cryptography is to provide the following four fundamental information security services

1. Confidentiality
2. Data Integrity
3. Authentication
4. Non-repudiation

Characteristics of Modern Cryptography

There are 3 major characteristics that separate modern cryptography from the classical cryptography.

Table 1:

Classic Cryptography	Modern Cryptography
It manipulates traditional characters, i.e., letters and digits directly.	It operates on binary bit sequences.
It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
It requires the entire cryptosystem for communicating confidentially.	Modern cryptography requires parties interested in secure communication to possess the secret key only.

CRYPTOSYSTEMS

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.

Types of Cryptosystems

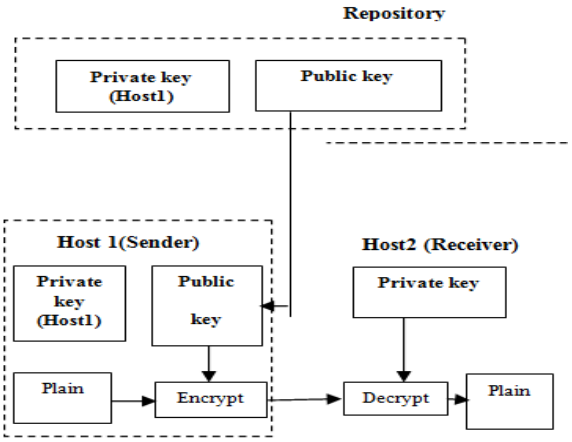
Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system:

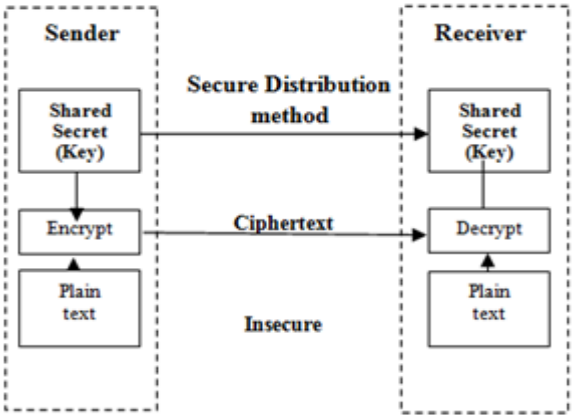
- Symmetric Key Encryption
- Asymmetric Key Encryption

Difference between these systems is the relationship between the keys used (encryption and the decryption keys). Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information or message is known as Symmetric Key Encryption.





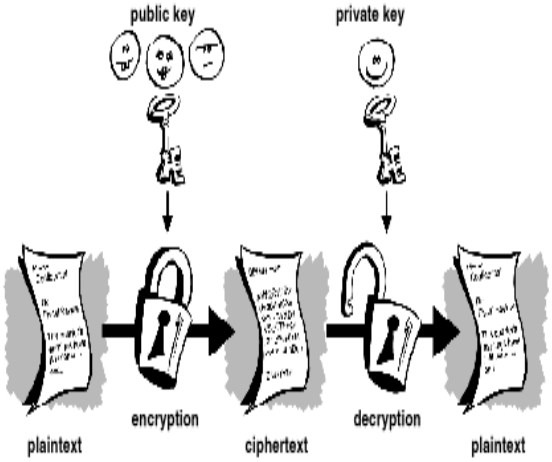
Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. The keys are different, but they are mathematically related and retrieving the plain text by decrypting ciphertext is feasible.

Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons.

Public key cryptography

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.



The primary benefits of public key cryptography are that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named, you guessed it, for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz).

Cryptography Hash functions

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values.

The ideal hash function has three main properties:

a) It is extremely easy to calculate a hash for any given data.

b) It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.

c) It is extremely unlikely that two slightly different messages will have the same hash.

THE ENIGMA MACHINE

The Enigma machine is a piece of spook hardware invented by a German and used by Britain's codebreakers as a way of deciphering German signals traffic during World War Two. The Germans were using an encryption code called Enigma – which was basically an encryption machine that encrypted messages for transmission. Most communications were sent via radio, which means that allied forces could listen in on their communications – hence the need for encryption. The German's encryption scheme however, was much stronger than older methods. It has been claimed that as a result of the information gained through this device, hostilities between Germany and the Allied forces were curtailed by two years.

Future of Cryptography

Elliptic Curve Cryptography (ECC) has already been invented but its advantages and disadvantages are not yet fully understood. ECC allows to perform encryption and decryption in a drastically lesser time, thus allowing a higher amount of data to be passed with equal security. However, as other methods of encryption, ECC must also be tested and proven secure before it is accepted for governmental, commercial, and private use.

Quantum computation is the new phenomenon chapter in the World of modern cryptography. While modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored; a quantum computer stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" also know as "qubits". This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

Modern cryptography will have to look for computationally harder problems or devise completely new techniques of archiving the goals presently served by modern cryptography.