Evolution of Encryption Techniques and Data Security Mechanisms

K. John Singh and R. Manimegalai

School of Information Technology and Engineering, VIT University Vellore, Tamil Nadu, India
Department of Computer Science and Engineering, Park College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract: Rapid advancements in information technology world resulted in the drastic growth in the amount of data transferred through the network. Networks used for multimedia communication do not provide much security for data transfer as well as digital communication. Billions of people use internet options for essential communication and as a tool for commercial interests. Therefore, security is an enormously important issue to deal with. As web services also have data storage and data communication, we need to protect and provide confidentiality. There is a need to recognize the different aspects of security and their applications. This paper provides a comprehensive overview of evolution of encryption algorithms right from ancient cryptography techniques to modern encryption algorithms.

Keywords: Confidentiality · Authentication · Substitution Cipher · Enigma Rotor · Hash Function

INTRODUCTION

Before taking a deep dive into the ocean of cryptography. The cryptosystem or a cipher system conceals information from unintentional user [1]. Cryptography is the science of creating that kind of cryptosystem where as cryptanalysis is the scientific art of unravelling these cryptosystem when it is read by any pirate. Both cryptography and cryptanalysis encompass by the term cryptography. In cryptography, encryption and decryption are the two major processes. Encryption is the process of renovating plain text into cipher text. Here plain text is the original form of message while cipher text is the unrecognizable form of information [1]. The typical reverse process of encryption is called as decryption. Algorithms that are used to encrypt and decrypt the information are called as encryption algorithms and decryption algorithms respectively.

History of Cryptography and Cryptanalysis: The word Cryptography is coined from the following two Greek words: krypto="hidden” and grafo="to write” i.e. “hidden writing”. Cryptography is being used since ancient times in order to hide the original message during data transfer. As we know, cryptography plays an important role in providing information security is the major aspect of security. More generally, cryptography is the science of privacy and is an ancient art. It is about constructing and analysing the protocols that overcomes the authority of adversary and which are correlated with various aspects of information security such as data integrity, non-repudiation and confidentiality and authentication [2].

Integrity: It is the conception of stability methods, values, actions, principles and expectations. We can test the integrity of the system either objectively or subjectively.

Non-Repudiation: It refers to the status of affairs where the self-styled creator of the statement will not be able to effectively test the validity of the contract.

Confidentiality: It is the ethical standard of caution associated with the profession such as law, medicine etc. It is preferably needed in all the fields it is related to the secrecy of the data and more precise, the secrecy tone of a voice.

Authentication: It is the act of confirming the reality of an aspect of an entity. This might grip confirming the uniqueness of a person, software programs etc.
In ancient era of cryptography, message confidentiality solely depends on cryptographic methods [3]. Communication of messages from graspable form into an impenetrable one and acknowledgement back again from the other end without interpreting by pirates. To ensure secrecy in communication, encryption is worn up in the communication among leaders, diplomats and those of spies. Encryption and cryptography are two synonyms in this era [3]. Mainly, encryption and decryption are used for privacy. Encryption algorithms are supported in achieving this privacy on each transmission over a network.

The earliest cryptography was the form of writing simple messages, as most of the people could not read. It was solely concerned about the converting messages into the written manner of figures to protect the message during transmission of messages from place to place [4]. The need of cryptography arose because of the technological advances in our life style. As we know, necessitate to obscure message has been with us when humans moved out of caves, started living in groups and decided to seize this civilization scheme sincerely. As soon as there were different groups or tribes, the basic idea was that we had to work against each other along with the terms of secrecy, crowd management and level of aggression. The most basic forms of cryptography were established in the crib of civilization including the region encompassed by Egypt, Greece and Rome. We have the history of cryptography at least 4000 years earlier [4]. The history of cryptography can be discussed in the three titles are; (i) Classical cryptography, (ii) medieval cryptography and (iii) modern cryptography. Cryptography techniques developed so far can be divided into the following three eras:

- **Techniques developed from ancient civilization to first part of nineteenth century (4000 BC – 400 AD).** These techniques are simple algorithms designed and implemented manually.
- **Classical techniques that are implemented using electro-mechanical machines (1000 AD - 1948).** These algorithms were developed during world war times, especially for secret communications between Presidents and Heads of allied nations.
- **Techniques that are developed during modern computing era i.e. after the release of microprocessors (1949 - till date).** These techniques are developed based on solid mathematical background.

The history and timeline of cryptography algorithms is shown in Table 1. It is interesting to note that beside researchers and academicians, other communities such as military persons, diarists and diplomatic personals have also contributed several techniques in cryptography. For brevity, only limited details such as name(s) of the invention and inventors are given in Table 1. More details on some of the popular inventions are given subsequently after Table 1.

It is believed that Egyptians used a symbolic representation called Hieroglyphic symbol for recording and transferring religious, secret and mystical knowledge to next generation around 4000 BC. Hieroglyphs are figurative, stylized symbols representing real or illusional objects. Though numerous failed attempts were made to decipher the hidden meaning of hieroglyphic symbols, real breakthrough came during Napoleon’s Egyptian invasion. Napoleon’s troops discovered a stone called Rosetta stone which contains a hieroglyphic and a demotic version of the same text in parallel with a Greek translation. A complete decipherment was made by Jean-François Champollion during 1820 [5]. Egyptian Hieroglyphs have been added to the Unicode Standard Version 5.2 in October, 2009.

**Phaistos Disk:** In 1850 BC, Greeks used a clay disk called Phaistos Disk for secret message sharing which is shown in Figure 1. Size of this disk is about 15 cm in diameter and covered on both sides with a spiral of stamped symbols. Stamping of symbols was done by pressing pre-formed seals into soft clay, in a clockwise sequence spiraling towards the center of the disk. Subsequently, the clay was fired at high temperature. The unique feature of Phaistos Disc is that entire text can be reproduced by inscribing with the help of reusable characters. There are 241 tokens on the disc, comprising 45 unique signs that are easily identifiable. It is believed that Phaistos Disc is the first document of movable type printing. Inspite of several failed attempts to decipher the Disc, symbols in Phaistos Disc are still a mystery. A set of 46 Phaistos Disc characters, comprising 45 signs and one oblique stroke, have been encoded in Unicode version 5.1 since April 2008.

**General Classification of Cryptography Techniques:** In general, cryptographic techniques are classified into three categories, namely, substitution/transposition techniques, key based techniques and hash based techniques. Key based techniques are further classified
Table 1: History and Timeline of Cryptography Techniques

<table>
<thead>
<tr>
<th>Period/Year</th>
<th>Name(s) of Inventors and Description of the Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Before Christ Era (BC)</strong></td>
<td>• Hieroglyphic Symbols used by Egyptians, 4000 BC – AD 400, to transfer religious literature and sacred writing</td>
</tr>
<tr>
<td></td>
<td>• Phaistos Disks made using clay by Greeks, 1800–1600 BC, first movable type printing</td>
</tr>
<tr>
<td></td>
<td>• Substitution Cipher, Steganography, Caesar Cipher by Romans - 600 BC</td>
</tr>
<tr>
<td></td>
<td>• Spartans Skytale Device by Greeks, 500 BC</td>
</tr>
<tr>
<td><strong>1000 AD</strong></td>
<td>• Frequency Analysis by Arabs</td>
</tr>
<tr>
<td><strong>1467</strong></td>
<td>• Cipher Disk</td>
</tr>
<tr>
<td></td>
<td>• Polyalphabetic Cipher by Leon Battista Alberti used in Mechanical Cipher Machines</td>
</tr>
<tr>
<td><strong>1585</strong></td>
<td>• Vigenere by Bellaso</td>
</tr>
<tr>
<td><strong>1795</strong></td>
<td>• Jefferson Disk by Thomas Jefferson used in World War II by US Navy</td>
</tr>
<tr>
<td><strong>1932</strong></td>
<td>• SIGABA used in World War II by USA</td>
</tr>
<tr>
<td></td>
<td>• Typex used in Rotor Machines by British</td>
</tr>
<tr>
<td><strong>1940</strong></td>
<td>• One Time Pad used in Banking initiated by Frank Miller</td>
</tr>
<tr>
<td><strong>1942</strong></td>
<td>• SIGSALY used in World War II</td>
</tr>
<tr>
<td><strong>Medieval Cryptography</strong></td>
<td>• Mathematical Theory of Cryptography published by Shannon</td>
</tr>
<tr>
<td><strong>1949</strong></td>
<td>• Quantum States by Stephen Wiesner</td>
</tr>
<tr>
<td><strong>1970</strong></td>
<td>• Feistel Network Block Cipher Design by Horst Feistel</td>
</tr>
<tr>
<td><strong>1973</strong></td>
<td>• Public-key Cryptography</td>
</tr>
<tr>
<td><strong>1975</strong></td>
<td>• Key Exchange Algorithms by Diffie-Hellman-Merkel</td>
</tr>
<tr>
<td><strong>1976</strong></td>
<td>• Data Encryption Standard (DES) by USA used for enciphering PIN numbers and bank transactions</td>
</tr>
<tr>
<td><strong>1977</strong></td>
<td>• RSA by Ronald Rivest, Adi Shamir and Leonard Adleman, used for Secured Communication</td>
</tr>
<tr>
<td><strong>1990</strong></td>
<td>• Feynman ciphers by Richard Feynman</td>
</tr>
<tr>
<td><strong>1979</strong></td>
<td>• BB84 - First Quantum Cryptography Protocol designed by Charles Bennett and Gilles Brassard</td>
</tr>
<tr>
<td><strong>1994</strong></td>
<td>• Probabilistic Encryption by Shafi Goldwasser and Silvio Micali</td>
</tr>
<tr>
<td></td>
<td>• Chaotic Encryption by Matthews</td>
</tr>
<tr>
<td><strong>1994</strong></td>
<td>• Peter Shor Algorithm</td>
</tr>
<tr>
<td><strong>1995</strong></td>
<td>• Tiny Encryption Algorithm by David J. Wheeler and Roger M. Needham</td>
</tr>
<tr>
<td><strong>1996</strong></td>
<td>• SECMPEG by Jurgen Meyer, Frank Gadegast used for Video Encryption</td>
</tr>
<tr>
<td><strong>1996</strong></td>
<td>• Zig-Zag Permutation Algorithm by Lei B. Y, Lo K. T and Haijun Lei used for Text, Image and Video Encryption</td>
</tr>
<tr>
<td><strong>1998</strong></td>
<td>• Twofish by Bruce Schneider, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson</td>
</tr>
<tr>
<td><strong>1998</strong></td>
<td>• Quantum Cryptography</td>
</tr>
<tr>
<td></td>
<td>• Video Encryption Algorithm (VEA) by Changgui Shi and Bharat Bhargava</td>
</tr>
<tr>
<td><strong>1999</strong></td>
<td>• MPEG Video Encryption Algorithm (MVEA) by Changgui Shi and Bharat Bhargava</td>
</tr>
<tr>
<td><strong>2000</strong></td>
<td>• Real-time Video Encryption Algorithm (RVEA) by Changgui Shi, Wang SY and Bharat Bhargava</td>
</tr>
<tr>
<td><strong>2000</strong></td>
<td>• Partial Encryption by Howard Cheng and Xiaobo Li</td>
</tr>
<tr>
<td><strong>2001</strong></td>
<td>• Advanced Encryption Standard (AES)</td>
</tr>
<tr>
<td><strong>2003</strong></td>
<td>• Frequency Domain Scrambling approach by Wenjun Zeng and Shawmin Lei</td>
</tr>
<tr>
<td><strong>2005</strong></td>
<td>• Selective Encryption by Xiliang Liu and Ahmet M. Eskicioglu</td>
</tr>
<tr>
<td><strong>2005</strong></td>
<td>• MHT Scheme by Chung Ping Wu and Jay Kuo C. C</td>
</tr>
<tr>
<td><strong>2006</strong></td>
<td>• Wavelet Packet Transform Algorithm by Dominik Engel and Andreas Uhl</td>
</tr>
<tr>
<td><strong>2007</strong></td>
<td>• PRESENT Algorithm by Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. Robshaw, Yanick Seurin and C. Vikkelsoe used for VLSI chip design</td>
</tr>
<tr>
<td><strong>2009</strong></td>
<td>• LCASE (Lightweight Cellular Automata-based Symmetric-key Encryption) by Somanath Tripathy and Sukumar Nandi</td>
</tr>
<tr>
<td><strong>2010</strong></td>
<td>• International Data Encryption Algorithm by Rajashekar Modugu, Yong-Bin Kim and Minsu Choi</td>
</tr>
<tr>
<td><strong>2011</strong></td>
<td>• Humming Bird-2 by Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer and Eric M. Smith</td>
</tr>
</tbody>
</table>
Fig. 1: Phaistos Disks

Fig. 2: Classification of Encryption Algorithms

into symmetric key and asymmetric key encryption algorithms. Classification of cryptography techniques is shown in Figure 2. Some of the popular algorithms are explained in subsequent subsections.

Substitution Ciphers: Substitution cipher was introduced during 600 BC. It is a cryptographic technique where each letter of plaintext is replaced by a different letter. Each letter retains its original position in the message, but the identity is changed. This type of technique was documented during Julius Caesar’s Gallic Wars. Caesar Cipher, Monoalphabetic Ciphers, Hill Cipher, Playfair Cipher and Polyalphabetic Ciphers are few examples for substitution ciphers. Steganography was introduced by Greek in 600 BC to hide messages under text or pictures. In Steganography, the actual message is hidden using video, audio, image and text. The word is derived from two Greek words *steganos* (covered) and *graphein*. SIGSALY (also known as the X System, Project X, Ciphony I and the Green Hornet) was used in World War II as a secured speech system for the highest-level allied communications between the then US President Roosevelt and his England counterpart Winston Churchill. Design of SIGSALY led to the development of digital communications concepts including transmission of speech using pulse-code modulation.

The substitution cipher systematically replaces all characters in the plaintext with other characters. The Caesar cipher was one of the primitive schemes based on substitution technique. In this method, each original letter is replaced with some other alphabet which is few positions apart. One example for Caesar cipher is given below. Consider that the message, “hello welcome how are you” is to be transmitted. The above plain text may be transmitted as the following cipher-text “khoor zhrfrh krz duh brx” using the following mapping mechanism.
Table 2: Numerical Equivalence of Alphabets Used in Caesar Cipher

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>n</td>
<td>o</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
<td>u</td>
<td>v</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Later, shift-3 code which is similar to excess-3 code in Boolean algebra was included in Caesar cipher for communication among generals in military camps. Table 2 presents numerical equivalence of alphabets used in Caesar cipher.

Each plain text ‘P’ in the message is substituted with a cipher-text ‘C’ using Table 2 by employing equation (1).

\[ C = E(3, p) = (p + 3) \mod 26 \] (1)

The shift may be of any amount ‘K’, which is between 1 to 25, equation (1) can be generalized as:

\[ C = E(k, p) = (p + k) \mod 26 \] (2)

Decryption is done using equation (3)

\[ p = D(k, C) = (C_k) \mod 26 \] (3)

Key Based Techniques: History of key based encryption starts from Second World War. The revolution in computers and electronic communication during the last century brought lot of opportunities for civilian research into cryptography. IBM’s former chairman Tomas Watson set up a cryptography research group during late 90’s in New York. The group was led by Horst Feistel. A private key encryption system called ‘Lucifer’ was developed by the IBM cryptography research group. Later, Lucifer was modified and adopted by National Beaufor of standards (NBS) and released as Data Encryption Standard (DES) during 1977. As explained earlier, for each character in the plaintext, substitution ciphers substitute another character to generate the cipher-text. Whereas, transposition ciphers change the position of each character in the plain-text to generate the cipher-text. However, key based encryptions employ a specific key or password to generate a cipher-text.

Key based encryption techniques are classified into (i) symmetric key or secret key encryption and (ii) asymmetric key encryption. Asymmetric key encryption employs either a public key or a private key for encryption whereas symmetric key employs same key for both encryption and decryption.

Symmetric-Key Cryptography: In symmetric-key cryptography both receiver and sender will have the same key which is used for encryption and decryption. The architecture of symmetric-key encryption is shown in Figure 3. The plaintext is converted into cipher-text based on a unique key and function.

The strength of symmetric-key cryptography lies in the non-reversible function which uses the key to produce cipher text. The following functions are used for encryption and decryption.

\[ E_k(P) = C \] (4)
\[ D_k(C) = P \] (5)

In equation (4) and (5), \( E_k \) and \( D_k \) are encryption and decryption functions, \( K \) is the key, \( P \) is the plaintext and \( C \) is the ciphertext.
A 64-bit key can give reasonable security but 128 or 256-bit keys are required for mission critical applications. Increasing the key size improves security and mitigates security threats such as brute-force, plaintext, chosen plaintext and differential plaintext attacks. Symmetric-key methods are further classified into block ciphers and stream ciphers. In block ciphers, input data is encrypted as block by block, whereas, in stream ciphers, it is encrypted as bit by bit. In block ciphers, message size is altered whereas, in stream ciphers, it is altered.

**Asymmetric-Key Cryptography:** Figure 4 shows a typical asymmetric key encryption process. As the name indicates, two different functions and keys are used by the sender and the receiver. The keys are: (i) public key which is kept visible and is transmitted over network and (ii) private key which is kept secret between the sender and the receiver. Encryption and decryption functions used in asymmetric cryptography are given in equations (6) and (7) respectively.

\[
E_{K}(P) = C \quad \quad \quad (6)
\]

\[
D_{S}(C) = P \quad \quad \quad (7)
\]

In equation (6), \( K \) is the public key which encrypts plaintext \( P \) to generate cipher-text \( C \). In equation (7), \( S \) is the private key. The private key ‘\( S \)’ can be used for encryption and the public key ‘\( K \)’ can be used for decryption and vice versa. Asymmetric key algorithms are slower than symmetric key algorithms and are prone to security threats. Authentication using digital signature uses asymmetric key encryption. Table 3 lists all possible key sizes used in symmetric and asymmetric key algorithms.

**Hash Based Encryption:** Cryptographic hash function takes a message of any length as input and produces a fixed length string as output. It is also called as message digest or a digital fingerprint. A secure hash function is one in which the original message cannot be deciphered.
Table 3: Key Sizes of Symmetric Key and Asymmetric Key Encryption

<table>
<thead>
<tr>
<th>Key Size in Symmetric Key Encryption</th>
<th>Key Size in Asymmetric Key Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>56-bit</td>
<td>384-bit</td>
</tr>
<tr>
<td>64-bit</td>
<td>512-bit</td>
</tr>
<tr>
<td>80-bit</td>
<td>768-bit</td>
</tr>
<tr>
<td>112-bit</td>
<td>1,792-bit</td>
</tr>
<tr>
<td>128-bit</td>
<td>2,304-bit</td>
</tr>
</tbody>
</table>

Fig. 5: Hash Based Encryption

from the given hash (digest) value other than brute-force technique. Examples of good hash functions are SHA-512, SHA-256, SHA-160, MD5, RIPEMD and Tiger [15, 16]. Hashing takes binary or text data as input and creates a constant-length hash representing a checksum. Different hashing algorithms produce different sizes of hashes. The original message cannot be recreated using the hash generated. One-way Unix-based password authentication is based on message digest. The password is stored as a hash value in a table. During login, the password is hashed and compared against the stored hash value of the password. The password is accepted only if both the hashes match. Figure 5 shows a model for hash based encryption.

Medieval and Modern Encryption Algorithms: Encryption algorithms are used for achieving security and confidentiality during information sharing. As explained earlier, encryption is the process of converting message (plaintext) into an incomprehensible format called cipher text. The cipher text cannot be easily understood by an unauthorized user [17].

Lightweight and Heavyweight Encryption Algorithms: Lightweight algorithms are faster when compared to heavyweight algorithms as the former employ selective encryption technique [18]. Low power devices, networks, designs and operating systems tend to use lightweight encryption algorithm because of its less computational overhead and memory utilization. Lightweight algorithms are increasingly used in a variety of applications, such as wireless and power-constrained devices, civilian, military and tracking applications, mobile phones, smart cards and electronic passports etc. Though, lightweight algorithms are developed for energy-efficient systems initially, they gain importance because of their widespread usage in pervasive/ubiquitous computing. On the other hand, heavyweight encryption algorithms provide better security when compared to lightweight algorithms. Lightweight algorithms attempt to make a balance between security, performance and low overall cost in terms of throughput, area, power consumption and price in low-resource environments. The term lightweight does not necessarily mean weak cryptographic designs, but it tries to make a better trade-off between the factors mentioned above. Consequently, they are employed in hand held devices, low power operating systems and low power wireless sensor networks. Lightweight algorithms are typically hardware-oriented and designed to be particularly compact and efficient. Serpent, Blowfish, Pretty Good Privacy (PGP), Twofish are few examples for lightweight encryption algorithms.

Heavyweight algorithms are not adopted for real time applications, mobile devices and wireless networks due to high resource requirements such as memory, power and computational overhead. Rivest-Shamir-Adelman (RSA) algorithm and Advanced Encryption Standard (AES) are commonly employed heavyweight encryption algorithms for video data encryption [18]. General steps involved in heavyweight and light weight encryption algorithms are shown in Figures 6 and 7.

Independent and Joint Encryption Algorithms: Another classification of encryption algorithm is based on how encryption and compression is done. There are two approaches. In the first approach, both compression and encryption are done independently as two different processes by employing suitable and appropriate compression and encryption algorithms. This approach is called compression-independent encryption technique.
and is shown in Figure 8. In this approach, only selective portions of compressed video streams are encrypted and thereby exploiting the characteristic of the compressed video streams. As both compression and encryption are performed separately, this technique involves high CPU and memory overhead. In the second approach, both compression and encryption are integrated together as a single process. This approach is called as joint compression and encryption technique. Two strategies are followed in joint compression and encryption algorithm. The first strategy employs encryption after compression, while, the second one employs encryption before compression. Both strategies are illustrated in Figure 9(a) and 9(b). As encryption is done after compression in the first strategy, we get two-fold advantages, namely, reduction in data size and execution time. The second strategy encrypts data without compression and takes more time for encryption. However, both strategies provide two level security and consume less time when compared to compression independent encryption algorithms. Secure Motion Picture Experts Group (SECMPEG) [19], Video Encryption Algorithm (VEA) [20], Real-time Video Encryption Algorithm (RVEA) [21], are few examples for joint compression and encryption algorithms. Joint compression and encryption algorithms are faster in encrypting video data when compared to independent encryption algorithms.

As early as 1900 B.C, Egyptian scribes used hieroglyphs in substandard fashion, most probably to conceal the sense from those who did not know the meaning [5]. As for the Greek’s for using a stick, the method was known as letter shifting or substitution. It was very simple matter of trying out sticks of various diameters until the messages became understandable. The writing would be meaningless while the tape was unwound [6]. The Romans also found their own methodology was known as a Ceaser shift cipher. This name originated because of Julius Ceasar. In his correspondence, he allegedly uses the simple substitution method. Then Romans utilized the idea of shifting letter by a granted numbers and writing information in this historical manner simply calls it as letter shift. The receiver side used the same method to decipher.

**Ceaser Shift Cipher:** It is most commonly known and simplest encryption technique, which is an example of substitution cipher. This method is named behind Julius Ceaser, who is used for his personal correspondence.
The action of Ceaser cipher is to substitute each letter in plain text to another fixed letter or number behind in the alphabet. It simply calls it as 3 to right method [7]. In this method, it is a typical shift cipher which is derived the cipher text from plain text alphabet by shifting certain amount space between. For performing encryption of plain text, simple substitution method is followed. Ceaser considered as the first person who is using encryption for sake of private communication.

Eg: using Ceaser shift, encrypt the following plain text.
“WELCOME TO HOME”
“ZHOFRPH WR KRPH”

The timeline of cryptography showed us that, Hebrews also enciphered certain words in the scriptures anciently. In 1200s, Roger Bacon described various methods and the famous Geoffrey Chaucer included different ciphers in his works consequently. Then in 1460’s, Leon Alberti devised a cipher wheel and defines the principles of frequency analysis. And then published a book on cryptology by Blasé de Vigenere in 1585. He described about poly alphabetic substitution cipher also.

The classic cryptographic having two components known as classic cipher, named as, substitution ciphers and transposition ciphers. In substitution ciphers, letters are replaced by other letters while in transposition the letters are arranged in a different fashion. According to the combination of these ciphers, it can be classified as two are; mono alphabetic and poly alphabetic. Mono alphabet having only one substitution or transposition used even as poly alphabetic having several substitutions or transposition used. Several such ciphers concatenated mutually to form a product cipher. The Ceaser shift cipher is an example of a mono alphabetic cipher. While comparing with poly alphabetic, mono alphabetic method of encryptions is very easy to break. Here only one time substitution is possible. It is easy to make the sense of the message. Frequency analysis of each letter in the encrypted messages makes easy to decrypt. But in case of poly alphabetic, rearranging the letter in n-grams (anagramming) give the highest frequency. Hence frequency analysis no more supported.

Jefferson Cylinder: Jefferson cylinder developed and comprised 36 disks device with a random alphabet in 1970’s.
The science and art of cryptography showed no further changes or advancements until the middle ages. At that time, methodology of cryptography was used by all the western European government in one form to another [10]. The major use of cryptography in that era is keeping touch with ambassadors. Especially Leon Battista Alberti was known as “the father of western cryptography” at that time due to his invention in polyalphabetic substitution. He used two copper disks on his method that fit together. The alphabet extolled on each of these disks. After every few alphabets, the two disks were rotated to modify the encrypting sense. Thus the preventive use of frequency analysis to split cipher. Even criminals also used the cryptographic methods.

Alberti Cipher: It was created at the peak time of cryptography by Leon Battista Alberti. It is an example of polyalphabetic substitution. But the variable period and alphabets were mixed with polyalphabetic substitution first time.

This device is called as ‘formula’. It is made up of two discs attached with a pin. The large disc is called as stabilis, is always stable and the small one is mobilis, is in movable state [4]. The boundary of each disc is divided into 24 identical cells. The outer disc contains an uppercase alphabet for plain text and an inner ring having a lower case alphabet for corresponding cipher text.

Polyalphabetic substitution went throughout a range of changes and is most especially attributed to Vigenere, even if Rubin claims that he in fact had nothing to do with its creation. Rubin further points out that the use of the cipher disks continued during the Civil war. Although the North regularly cracked the messages With the South using brass cipher disks.

Gilbert Venam and Venam – Vignere Ciphere: In 1918, Gilbert Vernam worked to develop the broken cipher and created a new cipher called as Vernam-Vigenere cipher. But the drawback is they are unable to modify the greater strength on it. His works helps to invent one time pad which is typical keyword use for once and it provide greater security to prevent near unbreakable. Venam proposed a bit wise exclusive one stream which has common by sender and receiver. The proposed cipher having previously prepared key and is kept on the paper tape [5]. It is combined with character by character in plaintext to produce ciphertext. And for decryption again combined characters with the key.

Even criminals also used the cryptographic methods during the proscription to communicate with others, was reported by Whitman. In addition to this, it is vital to declare about the newly popularized “Windtalkers”. The Navajo’s used own languages as a source for cryptography. The code was not at all broken and was involved in the success in the Pacific Theatre during WWII. A dispute could be finished that the spoken language was not strictly cryptography, but it should be noted that in each communication, the message was written behind as a matter of method.

In this modern era, the drastic growth of cryptography and its techniques were originated from basic message confidentiality to include various phases of message integrity checking, digital signers and sender or receiver identity authentication with the other things. The modern field of cryptography can be divided into various areas of study which are discussed in the subsections below.

Secret Key Cryptography: In secret key cryptography, a single key is used for both encryption and compression. In this technique, the sender uses a single or various sets of instruction to make cipher text from plain text and sends encrypted data to receive [11]. The receiver uses a similar key for the decryption also. Hence it is oblivious that the
key must be known to both sender and receiver. But in that, distribution of key is the biggest difficulty faced up. Secret key cryptography schemes are classified into stream cipher or a block cipher. A stream cipher is defined as operating on a single bit at a time and implements some feedback mechanism. Hence the key is continuously changing. It has several flavors, but most important two is self-synchronizing ciphers and synchronous ciphers. In a block cipher, at a time schema encrypts one block using the same key on each block. Block ciphers can have several modes of operation. Most important modes are electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB). Mainly secret key cryptography is used in DES, AES, BLOWFISH, TWOFISH, RIVEST CIPHERS etc.

Hash Function: The cryptographic hash function is the third type of cryptographic algorithm. Hash functions are an algorithm that uses no key, is also called message digests and one-way encryption. Instead of a key, a fixed length hash value is computed based upon the length of the plain text to be recovered. It is also employed to encrypt passwords by many OS and provide a measure of file integrity [12]. Generally hash algorithms are used to provide a digital fingerprint of a file's contents. Hash algorithms are commonly used in MD algorithms, SHA (secure hash algorithm), RIPEMD, whirlpool etc.

Public Key Cryptography: Public key cryptography is the most significant development in cryptography in last 400 years. Mainly this technique depends upon the existence of called as one way functions or mathematical functions [13]. A pair of key is required, one is for encrypting the data and another is used for decrypting the data and this approach is also called asymmetric cryptography. In asymmetric cryptography, one of the keys designed as public key which is advertised as widely as the owner wants. The other key is the private key, is never revealed to another. The need of this cryptography is occurring due to the secretly establishing keys between the communities while does not exit a secure channel for communication. As we discussed above, a pair of keys is used in this algorithm. While Hellman and Diffie might not find such a system, they just present a Diffie-Hellman key exchange protocol for public key cryptography [8]. Now widely this idea used for secure communication to permit users with a secret agreement on shared encryption key. Publication by Diffie and Hellman widely spread and inspired to find out the public key cryptography. Finally Ronald Rivest, Adi Shamir and Len Adleman won the race by discovering an RSA algorithm in 1978. In addition to both of this algorithm are used more widely, Caremer-Shoup Cryptosystem, ElGamel encryption and other various elliptic curve techniques are also included. In 1997, Government Communications headquarters (GCHQ) published a document which reveals that cryptographers at GCHQ had expected various educational developments.

In around 1970, James H. Ellis had conceived the values of public key cryptography. Then in 1973, Clifford Cocks developed a solution that almost similar to the RSA algorithm. And Malcolm J. Williamson is claimed to have developed the Diffie-Hellman algorithm in 1974. Public key cryptography is also used in the scheme of digital signature for implanting. Simply digital signature is a suggestion of a normal message; they have the feature of being very easy for the user to produce but very difficult forge by others. In digital signature there are basically two algorithms, one is for signing and other is mainly for verification. RSA and DSA are the most popular digital signature schemes.

Encryption and Decryption: In cryptography, the two techniques are used for secure communication over a network are encryption and decryption. Different types of algorithms are used to performing encryption and decryption process on a message. According to the meaning, encryption is the process by which transforms the plain text into the cipher text [10]. Where as the decryption is the process of converting cipher to plain text. These two techniques are now common for all the multimedia communication.

Encryption is the process of transforming messages using a kind of algorithm to convert as an unreadable format with the appropriate key. Keys are sequences of numbers or alphabets used to encrypt. Key size is always determined the strength of the encryption technology. It is now used for protecting the communication in civilian systems. It is used to protect in transit and can produce the confidentiality on message by itself.
But other methods are required for the authentication and data integrity, which are digital signature and authentication code [12]. Encryption technique must be applied to message to avoiding tampering at its creation time itself with digital signature.

Decryption is the method of decoding the data with key or password which is already encrypted. It is the reverse process of encryption. This term is used to describe the un-encryption method and algorithms manually. Here also the presence of the key is needed for the privacy.

Different types of encryptions are in cryptography. Document encryption, file or folder encryption, full disk encryption and USB encryption. Other than this we can say that encryptions are of mutual encryption, transparent encryption, symmetric encryption, asymmetric encryption and email encryption. Here we are discussing about the chaotic encryption [13]. Mainly we focus on the features of this encryption and its performance on communication. Evaluating the studies are obtained its advantages and disadvantages also.

The Data Encryption Standard (DES): DES is a famous block cipher encryption algorithm. IBM’s Lucifer was adopted, modified and released as DES standard by National Institute of Standards and Technology (NIST) in 1977 (Valizadeh 2004). DES is commonly used to encipher PIN numbers in bank transactions. DES can generate block ciphers with each block containing 64 bits. A 64-bit key is used for encryption of blocks [22].

Rivest- Shamir Adelman (RSA) Algorithm: RSA is one of the widely used public key algorithms. It was invented in 1977 by Ron Rivest, Adi Shamir and Len Adelman. It is based on factorization of integers into their prime (Guido 2003). Consider that sender ‘X’ and receiver ‘Y’ want to communicate with each other. The receiver ‘Y’ chooses two distinct large primes $p$ and $q$ then multiplies them together to form $N = p*q$. It also chooses an encryption exponent $e$, such that the, greatest common divisor of $e$ and $[(p-1)*(q-1)]$ is 1. The receiver then computes decryption key $d$, $d = 1/e \ (mod \ [(p-1)*(q-1)])$. The pair $(N, e)$ is made as public; $p$ and $q$ are kept as secret. Let $M$ be the plain text block and $C$ be the cipher text block, then.
C = M \mod n

M = C_d \mod n

Both sender and receiver must know values of ‘n’ and ‘e’. Receiver should also know the value of ‘d’ also. The above mentioned scheme makes a public key encryption of \( K_e = \{e, n\} \) and private key encryption of \( K_d = \{d, n\} \).

Advanced Encryption Standard (AES): Rijndael cryptosystem [18] was adopted by NIST as AES standard in 2001. AES operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. The algorithm is capable of using a variable block length and key length [18]. The latest specification of AES allows any combination of key lengths i.e. 128, 192, or 256-bit keys and blocks of length 128, 192, or 256-bit.

Wavelet Packet Transform Algorithm: An encryption method based on wavelet packet transform is proposed in [23]. This method encrypts only selected portions of video and therefore consumes less time for ciphertext generation. As it does not encrypt entire data, it is vulnerable to security threats. Wavelet transform before encryption may increase the computational complexity when compared to other algorithms [23].

Elliptic Curve Cryptography Algorithm: The polynomial interpolation based Elliptic Curve Cryptosystem (ECC) is proposed in (Liew 2011). ECC uses 160-bit key which is shorter than keys used in other heavyweight algorithms such as RSA. As the key size is smaller in ECC, it takes less encryption time. Transferring video streams over wireless networks using ECC is prone to privacy and malicious attacks due to smaller key size [24].

Twofish Algorithm: Twofish [25] is an open source encryption algorithm which has the key size of 256-bits. Sixteen rounds of XOR operation is performed during encryption which leads to more computational steps. Twofish requires low computational resources but complex decryption processes. Twofish algorithm is prone to known-plaintext and piracy attacks. Hao et al have proposed a lightweight and scalable encryption algorithm for streaming video over wireless networks. The security architecture proposed in [26] is based on the lightweight public key scheme called Derivable Public Key (DPK).

Pretty Good Privacy (PGP) Algorithm: Pretty Good Privacy (PGP) is used for secured communication through the Internet [27]. This is based on Public Key Infrastructure (PKI) and some standard encryption mechanisms. PGP is an open source algorithm and allows anyone to evaluate and recommend modifications. In PGP, keys are of 512, 1024, or 2048-bit lengths. It can transfer text data faster than video data over the Internet.

Tiny Encryption Algorithm (TEA): Tiny Encryption Algorithm (TEA) is the fastest encryption algorithm. This is based on Feistel function which involves more number of rounds to get better security. TEA performs mixed operations such as XOR, ADD and SHIFT which are used to provide better secrecy. The block size and key size are 64-bit and 128-bit respectively. TEA encrypts data into a machine language format and is vulnerable to brute-force attacks.

RC 4 and RC 6 Algorithms: Rivest Cipher 4 (RC4) is good for Secured Socket Layer (SSL) security. The Rivest Cipher 6 (RC6) is a symmetric key based lightweight block encryption technique. RC6 is structurally similar to its previous version RC5 and uses dependent data rotation, XOR operation and modular addition. It employs more number of rounds, wide variety of wavelengths and different key sizes [26]. RC6 supports keys with 128, 192 and 258 bits which has a block size of 128 bits. In RC6, four working registers and integer multiplication inclusion method are used whereas only two registers are used in RC5. The multiplication process of RC6 provides better security and higher throughput when compared to RC5.

Lightweight Cellular Automata-based Symmetric Key Encryption: Somanath et al have proposed a Lightweight Cellular Automata-based Symmetric Key Encryption (LCASE) technique which generates a 128-bit lightweight block cipher with 128, 192 and 256-bit keys. LCASE is mainly used in resource constrained devices which require low processing power and low-end-devices that need less memory storage. LCASE is against differential cryptanalysis and linear cryptanalysis which may be affected by timing attacks.

International Data Encryption Algorithm (IDEA): IDEA is a symmetric block cipher encryption technique proposed in [28]. Initially, IDEA was called as Improved Proposed Encryption Standard (IPES) and performs eight
identical transformations for encrypting the data. It has the key size of 128 bits and block size of 64 bits. IDEA uses the same features and framework for both encryption and decryption but uses different keys for encryption and decryption. Two operations namely, key mixing and addition are performed in each round. Key mixing combines four 16-bit input words with sub-key words in parallel by using either modular addition or modular multiplication operation. Subsequently, output generated in previous round is given as input to the next round. IDEA uses sub-keys which are 0 or 1 for key mixing and XOR operation. These sub-keys are very weak and create problems during XOR operations.

Humming Bird-2 Algorithm: Daniel et al have proposed an authenticating encryption algorithm, Humming Bird-2 (HB-2) for the hardware implementation of lightweight process using low end microcontrollers [29]. This consists of 128-bit secret key and 64-bit initialization vector. It includes properties of both traditional stream ciphers and block ciphers. As authenticated encryption process is involved HB-2 provides confidentiality and integrity. The important drawback of this algorithm is hardware leakage which leads to complex calculations.

PRESENT Algorithm: One of the most compact video encryption algorithms, PRESENT, is proposed in [30]. This is 26 times smaller than the standard encryption algorithm AES. Its block size is 64-bit and the key size is either 80-bit or 128-bit. This is used in low-power consumption and high chip efficiency devices. In PRESENT, both hardware efficiency and security have been equally considered for cipher design. Main goal behind the development of PRESENT is that the level of security should offer 64-bit block and 80-bit key. This algorithm is suitable for low-power designs.

Probabilistic Encryption: Main objective of probabilistic encryption is the randomness which gives different constants for same messages and different ciphertexts. Security is improved in probabilistic encryption by hiding partial information about the plaintext. During encryption, the plaintext is padded with the random string generating the padded encrypted cipher. Decryption is done by using the reverse process by eliminating padding from the probabilistic encryption.

SECMPEG Algorithm: The joint compression and encryption algorithm proposed in [19], SECMPEG, does selective encryption using conventional encryption algorithms. This has been designed to provide security for high volume video signals such as, ISO standard 11172 or MPEG-1. Before decoding, the video is segmented and converted into block of streams which is represented using four layers and five confidentiality levels (C-levels). Then, Huffman coding is used for compression and DES is used for encryption. In level 0, encryption is not performed. Level 1 and level 2 consist of details about layers 1 to 4. The level 3 contains all I-frames which are intra-coded macro-black blocks. Encryption takes place in level 4. In SECMPEG algorithm, all layers of video stream are not encrypted due to selective encryption.

Zig-Zag Permutation Algorithm: The proposed solution in [31] performs compression and encryption with minimum overhead using random permutation and probabilistic encryption. It provides different levels of secrecy for various multimedia applications. The proposed strategy employs Discrete Cosine Transformation (DCT) to map smaller blocks of size 8x8 to bigger blocks of size 1x64. The output of DCT is uniformly quantized and all quantized coefficients are arranged in zig-zag order. Finally, entropy coding is done for compression. In this technique, compression is done before encryption which leads to less execution time. But the computational complexities involved in both zig-zag order and mapping decreases the speed of video compression. The zig-zag permutation is prone to known-plaintext attack [31].

Video Encryption Algorithm (VEA): The Video Encryption Algorithm (VEA) is introduced by Changgui Shi and Bharat Bhargava for joint compression and encryption of video data [20]. This is an efficient video encryption algorithm which has less computational complexity. Only a streamed video can be encrypted using VEA technique. Before encryption, size of the video data should be reduced using any standard compression method. MPEG-2 or MPEG-4 is used for compression, because VEA and MPEG are mutually dependent on their statistical properties.

MPEG Video Encryption Algorithm (MVEA): A MPEG Video Encryption Algorithm (MVEA) is proposed in [21] for joint video compression and encryption of video applications. This is an improved version of Video Encryption Algorithm (VEA) (Changgui 1998a) where the XOR operation is used with a secret key whereas in VEA, XOR operation is used without passing any secret key.
(Changgui 1998a). Sign bit of discrete cosine coefficient in I-frame block is also encrypted. In MVEA, the differential sign value of DC coefficient and motion vectors in P-frames and B-frames are XOR-ed with a secret key. This method is used in secure video-on-demand, video conferencing and video email applications. The main disadvantage of MVEA is, the huge size of secret key used in encryption.

Real-time Video Encryption Algorithm (RVEA): To overcome known-plaintext attack, Changgui et al have proposed RVEA [32]. The difference between VEA, MVEA and RVEA lies in the use of XOR operation. VEA uses only XOR operation and MVEA uses XOR operation with a secret key. In RVEA, the XOR operation is replaced by DES algorithm. RVEA is a selective encryption algorithm which operates on sign bits of both DCT coefficients and motion vectors of MPEG-compressed-video. RVEA can use any secret key cryptographic algorithms to encrypt selected sign bits. Encryption time of RVEA is much less than naive algorithms because it encrypts only 10% of the total bit stream. RVEA can defend known-plaintext attack, but, it may be affected by perceptual attacks.

Chaotic Cryptography: In the modern cryptography, various algorithms are used for encryption and decryption. Here we are considering the chaotic encryption techniques and its performances on text. Basically the term “chaos” is meant that confusion or complete disorder. The chaos, an absorbing event that is observed in nature and laboratory circuits. The behaviour of a chaos is also found in different kinds of technology fields and their applications.

The time line is starting in early 1950, Shannon clearly mentions that the chaos can be used in cryptography, because of its basic stretch and fold mechanism. The time period until 1980’s, the necessity of cryptography becomes more important and chaos theory becomes more popular among the cryptographers [6, 7, 8]. The implementation of chaos by shannon has developed the chaos theory at 1980s. In 1990, the first chaos based ciphers were proposed and more over the synchronization of chaos entered the scene. Approximately 30 more publications were obtained about chaos. In 1998, the chaotic encryption was developed by Baptista. The year of 2000, chaos started to recognize widely and obtained an application for secure communication.

The chaotic systems are defined on a complex or real number space called as boundary continuous space. Chaos theory mainly aims that to understand the asymptotic behaviour of the iterative process [9]. The properties required for chaotic systems for cryptography is sensible to an initial condition and topology transitivity.

The chaotic encryption method is proposed by Baptista in 1998, it seems to be a much better encryption algorithm than traditional algorithms were used. To encrypt a message, we first define the mapping scheme for trajectory. Then decide the initial condition and parameters as the key. Set the initial condition as current trajectory [5]. For each message symbol, iterate the chaotic equation until the trajectory reaches the destination site and then store the number of iterations as a cipher. Encrypt the next message symbol by iterating the current trajectory and producing the next cipher and so on.

To decrypt the cipher, set the initial condition and parameters and apply the same mapping scheme for decryption. Iterate the chaotic equation by the cipher (number of iterations). Find out the site that the trajectory belonged to and store the symbol of the site as message symbol. Decrypts next symbol by iterating the current trajectory and producing the next message symbol and so on.

The general chaos encryption method is the simplest way to encrypt Message using chaotic equation. This method can help to find out some important information and determine the basic level of security.

Chaotic encryption is used for image encryption also. For this encryption, rotation of pixels is the main role to perform [14]. The image is considered as the system input and will perform some gray scale substitution on it. This cause to change the pixel size and order. Here we consider as each pixel is as a block, then it will encrypt with key and algorithm. The first section deal with the already existing image encryption technique based on the chaotic technique in spatial domain. Next part will be dealing with the different algorithm which can be discovered by experiment in the frequency domain.

CONCLUSION

Many of the techniques ranging from secure commerce, protecting passwords or pin and payments to private communications. As we know, one of the essential aspects of secure communication is Cryptography. Simple description of cryptography is the science of writing secret codes. In this paper a study is done about the historic expedition of cryptography.
REFERENCES


