FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

# Analysis of Tools and Techniques in Cryptography

**Prof. Dr. Amit Verma[1] and Anjali Gakhar[2]**

[1]*Department of Computer Science Chandigarh University, Mohali, India, amit.verma@cumail.in*

[2]*Department of Computer Science Chandigarh University, Mohali, India, anjaligakhar7@gmail.com*

***Correspondence:** *amit.verma@cumail.in*

**ABSTRACT-** In the epoch of advanced electronic and communication systems, it is being observed most of the times that the information is being assaulted with worms and viruses. To shield the data, a secure and sophisticated cryptosystem is required to devoid any type of dilemma. There are several tools and techniques that are being used, to meet the challenging needs for a highly secure transmission and reception system. Previously security was mainly concerned with the exchange of messages that took place in communication. After that some techniques came into existence that provided more truthful and superior results. But the prerequisite for a more clandestine system is mounting day by day. As the communication system is being more complex, according to the demand more sophisticated and protected cryptograms are necessitated. In the following paper various cryptographic techniques have been analyzed that serve the purpose of security from 1900 B.C up to the present day scenario.

**General Terms:** Security Algorithms, Pseudo codes, Hierarchy of Cryptography, Language of encryption.
**Keywords:** Hieroglyphics Enigma Machine, DES, AES, RSA Quantum Cryptography.

**ARTICLE INFORMATION**

**Author(s)**: Prof. Dr. Amit Verma and Anjali Gakhar;
**Received**: 04/04/2022; **Accepted**: 30/07/2022; **Published**: 30/08/2022;
**e-ISSN**: XXXX-XXXX;
**Paper Id**: IJCSR-010106;
**Citation:** 10.37391/IJCSR.010106

**Publisher's Note:** FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

## 1. INTRODUCTION

It is propensity of humans to veil their information from others. Even children apply different tricks to hide messages from their parents, friends or from siblings. There are lots of examples where distinct trick and technique are applied to cosset the communication from adversaries. [1] There are many techniques that are used to perform security tasks. In past only pen paper-based methods were employed to exchange the message from one position to another. In World War II various machines were introduced that helped to scramble the message. Hence there are various arts and techniques that are employed to provide security to the information. Moreover, numerous methods are available that can be utilized efficiently for breaking the cipher unethically. (There are also various ways to break the cipher unethically.) All the techniques and tricks for both cipher making and cipher breaking come under the category of cryptography. Therefore, cryptography is the study of computer science that deals with different procedures and activities to scramble and unscramble the data. Scrambling of data has started 4000 years ago in 1900 B.C by one of the Egyptian scribes. They made use of non-standard symbols known as hieroglyphics, but this was not a serious attempt for hiding the data. [2] After this many techniques came into existence that somehow provided the security. In a cryptosystem if sender sends the message first he will encrypt it using an encryption key and on the other side while deciphering the message the receiver also makes use of a key known as the decryption key. The key used for the two can be a symmetric key or an asymmetric key.

## 2. CRYPTOGRAPHY

In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy, and typically for confidential communications. Encryption can also be used for authentication, digital signatures, and digital cash etc. [3] the fundamental objective of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent, cannot understand what is being said. This channel could be a telephone line or a computer network.

| Mathematical_ Notation_ of_ Cryptosystem |
|---|
| From the above cryptosystem there are basically five tuples (*O, C, K,E,D*), where the following conditions are satisfied:<br>1. O is the finite set of possible originate message;<br>2. C is the finite set of possible cipher texts;<br>3. K is the finite set of possible keys;<br>*Rule:* - For each task there is an encryption rule $e_K \in E$ and corresponding rule $d_K \in D$ where, $e_K: O \rightarrow C$ and $d_K \in C \rightarrow O$ are functions such that $d_K (e_K (m))= m$ for every original message $m \in O$. [3] |

**Figure 1:** Mathematical Notation of Cryptosystem

## 3. CRYPTOGRAPHIC TECHNIQUES

Cryptography, the art or technique of enciphering and deciphering the message in a secret code has played and still playing vital roles in the history of every nation. It is becoming a necessary step in this crazy world where there is fight among the code makers and code breakers [4]. From 1900 B.C the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

process of cryptology was initiated by the Egyptian scribe while attempting to uphold the records in their own language. They made use of the non-standard hieroglyphics for communication purpose. It was the first endeavor and after this in 1500 B.C one more effort was made in Mesopotamia, where a miniature encipher flap was found that was roofed with the veiled the formula for glazing pottering [5]. Cryptography is not restricted to an individual or to a group of individuals; it serves the whole world for keeping their information secure from others. The use of cryptography is mounting day by day; it is being employed in wars and used in many organizations. The cryptography is generally alienated into three main era's that is classic cryptography where enciphering is done only with the help of pen and paper, then medieval era of cryptography where various substitution and transposition came into existence and at last the modern era of cryptography where revolutionary encryption techniques are introduced such as DES, AES, RSA etc. When we come down to it all the algorithm are classified into two terms that is symmetric and asymmetric key encryption.

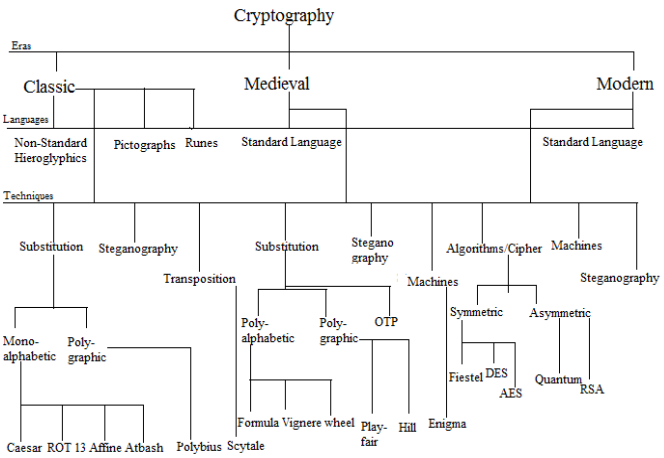



**Figure 2:** Hierarchy of Cryptography

The above hierarchy is showing some of the important cryptographic tools and techniques.

## 3.1 Classic Era

In Classic era non-standard hieroglyphics, pictographs runes etc were used to encrypt the messages at that time and were pretty strong according to that time because less number of people was there who knew about these languages or symbols so the techniques worked effectively at that time but when people got educated and the language became a part of everyone's daily life, new and even more complex techniques came into existence [6].

### 3.1.1 Substitution Techniques

In cryptography substitution ciphers plays a vital role to scramble the message. In substitution, every single bit of message is being replaced with other and a particular sequence is followed for the whole procedure. Substitution can be either substituting one bit at a time or many bits at a single moment and called as mono alphabetically or poly alphabetically respectively. In it 26 alphabets are permuted in many ways so as to perform the encryption and decryption function [3].

***Definition:*** Sequential replacement of an original message with cipher text in order to scramble every single bit of the plain text so that no other unauthorized party can take advantage of it.

| Substitution_ Cipher |
|---|
| Assume O=C= $X_{26}$, whereas K includes set of all possible permutations starting from 0 to 25.<br>There should be a random permutation say, $\Omega$ and belongs to K.<br>Encryption can be done as<br>$E\Omega(\alpha) = \Omega(\alpha)$,<br>And,<br>Decryption is defined as<br>$D\Omega(\beta) = \Omega^{-1}(\beta)$<br>Where,<br>$\Omega^{-1}$ is the inverse permutation to $\Omega$. |

**Figure 3:** Pseudo code of Substitution Cipher

The above substitution basics followed in both mono and polyalphabetic substitution. In monoalphabetic substitution only single letter is substituted with other letter or symbol. The use of monoalphabetic substitution is not new; it is used by the Hebrew scribes known as Atbash cipher. In this first letter is swapped with the last letter of the alphabet and is also known as the mirror writing [7]. For long period of time this substitution technique was used in various ciphers such as Atbash cipher and many more. The substitution method can be used in two ways one is monoalphabetic and another one is polyalphabetic. In first only one symbol is substituted and in second more than one symbol is substituted. The substitution technique that is described above has a special case named as the shift cipher. In which a symbol or a letter is shifted according to the predefined key. The shift cipher performs cryptography function that is based on modular arithmetic.

#### *3.1.1.1 Shift Cipher*

Shift Cipher is one of the special case substitution cipher. In this the cipher text is generated with shifting rule that is current alphabet is shifted to next n position so as to generate the code word. Here, is the pseudo code that will help to understand the logic behind the shift cipher.

| Shift_ Cipher |
|---|
| Assume O=C= K= $X_{26}$,<br>For $0 \leq K \geq 25$<br>Perform,<br>$E_K(\alpha) = (\alpha + K) \bmod 26$,<br>And,<br>$D_K(\beta) = (\beta - K) \bmod 26$<br>Where,<br>$(\alpha, \beta \in X_{26})$ |

**Figure 4:** Pseudo Code of Shift Cipher

FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

For the number of years shifting technique worked very well and it would be a difficult to crack the code at that time. In 50-60 B.C Julius Ceaser introduce one more way to scramble the message that is based on the shift technique. In his way of encrypting message current letter was replaced to the third letter that is he shifts the positions of the letter to make the text irrelevant. That is a will become d and d will become g [8]. There is an instance that will help to understand the working of the ceaser cipher.

| PT | a | b | c | d | e |
|---|---|---|---|---|---|
| CT | D | E | F | G | H |

*Example: Ceaser Cipher*

This technique was helpful to encode the message and can't be breakable by those who don't have the knowledge of the language. Here is pseudo code for both the encryption and decryption process.

| Pseudo code_ Ceaser_ Cipher_ Encryption |
|---|
| Assume O=C= K= $X_{26,}$ For $0 \leq K \geq 25$<br>Perform,<br>$E_K(\alpha) = (\alpha + K) \bmod 26,$<br>Where,<br>$(K=3)$ |

**Figure 5(a):** Pseudo code ceaser cipher encryption

| Pseudo code_ Ceaser_ Cipher_ Decryption |
|---|
| Assume O=C= K= $X_{26,}$ For $0 \leq K \geq 25$<br>Perform,<br>$D_K(\beta) = (\beta - K) \bmod 26$<br>Where,<br>$(K=3)$ |

**Figure 5(b)**: Pseudo code ceaser cipher decryption

Same technique work as the base for number of techniques for instance ROT 13 in which shifting is done for thirteen place. All of them will follow the same sequence. This is all about the historical ciphers where all the attempts were made on the paper with pen. These are some of the basic attempts to encipher the message that may be easily deciphered when one can have the basic knowledge about the language and key. These ciphers were broadly used by various encoders. But in 500 A.D cryptology entered to the Dark Age after the collapse of Roman Empire and they were lost for 4000 years [9]. This was an end of classic cryptography era where the encryption takes place only with the help of pen and paper, or some techniques relay on spoken words, although it was not an end of cryptography. As the time passes new ciphers were introduced to encode the messages. After the end of classic era, medieval era of cryptography started

## 3.2 Medieval Cryptography

After the classic era the cryptography reach to the next level of science where more sophisticated and advanced tools and techniques came into existence. This new eon came to known as medieval era of cryptography. While the cryptography enters to the Dark Age there is another civilization was rising in the east. In 900 A.D Arabs society was one of the most literate cultures in the world and the study of code flourished. The Arabs were the first to record methods of transposition, the scrambling of letters as well as substitution the replacement of letters with numbers and symbols. They were the first to outline specific techniques of code breaking. It involves mathematical or frequency analysis. They were very interested in letter studies and count the number of times a character occurs. Such as aleph (first letter of Hebrew alphabet) appeared in the Quran and they discovered which letter occur very frequently. They use this information as a statistical source to learn how to break code. The most frequent coded letter represents the most frequent plain text letter and that's how they began to solve code and they were the first to do it. With the Ramazan's cryptology has a re-birth in Europe [5, 6].

### 3.2.1 Polyalphabetic Substitution (1466)

In 1466 an Italian architect Leon Battista Alberti develops a greatest crypto logic invention in 1000 years at the urging Vatican. He often called as the "father of western cryptology" and invented a polyalphabetic cipher to encode the message. It was a system of rotating cipher disk with two rings of letter and several numbers by scrambling so many letters randomly. It was the first to challenge Arab code breaking method of frequency analysis. Previous systems just replace A D only at a time but according to the Alberti cipher disk used as disk in which these letters combination could be change from time to time. And as a consequence letter "A" would be representing not only by one letter but by many letters. This was called as polyalphabetic substitution and it was the basis for many modern cipher systems [2].

### 3.2.2 Vigenere Cipher

The successor of Alberti continued his work in the field of security. In 1585 Blaise de Vigenere publishes his work on the principle of polyalphabetic substitution. He proposed a table of 26*26 in which 26 alphabets arranged row wise and 26 alphabets are arranged column wise and the table is named as Vigenere table [10]. For generating covert message same length of key is used.

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 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 |
| B | 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 | A |
| C | C | 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 |
| D | 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 |
| E | 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 | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | 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 |

**Figure 6:** Vigenere Square

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

Following is the pseudo code that is showing the operation that is performed in Vigenere cipher.

| Pseudo code_ Vigenere_ Cipher_ Encryption |
|---|
| Let n be a positive integer<br>Assume<br>$O=C= K=(X_{26})^n$<br>For $K= (K_1 - - - K_n)$<br>Execute,<br>$E_K(\alpha_1, \alpha_2, \alpha_3 - - - - \alpha_n) = (\alpha_1+K, \alpha_2+K_2 - - - - \alpha_n+K_n)$<br>Where,<br>All operations are performed in $X_{26}$ |

**Figure7(a):** Pseudo Code of Vigenere Cipher Encryption

| Pseudo code_ Vigenere_ Cipher_ Decryption |
|---|
| Let n be a positive integer<br>Assume<br>$O=C= K=(X_{26})^n$<br>For $K= (K_1 - - - K_n)$<br>Execute,<br>Decryption;<br>$D_K(\beta_1, \beta_2, \beta_3 - - - - \beta_n) = (\beta_1-K_1, \beta_2-K_2, - - - - \beta_n-K_n)$<br>Where,<br>All operations are performed in $X_{26}$ |

**Figure 7(b):** Pseudo Code of Vigenere Cipher Decryption

### 3.2.3 Wheel Cipher

In 1790 one more polyalphabetic substitution technique introduced by Thomas Jefferson in which 26 letters of alphabets are arranged. Wheel cipher contains a set of 36 wheels or disks and each having 26 letters of alphabet is arranged on it. One axle is present in between the centre of the 36disks that combine them together. To generate a scrambled message, a disk is rotated along the one row and second disk is used for having the cipher text [11].

### 3.2.4 Play Fair Cipher

In 1854 one more substitution technique came into existence known as play fair cipher. In this cipher a 5*5 matrix is used in which the message is written. Then it is enciphered both row wise and column wise. If the character of an alphabet that has to encrypt was in same row or in same column then it was replaced by the character that is written right to it. And if it lies in different rows and in different column then it is replaced by the letter that coincide with respect to their positions [12].

### 3.2.5 Hill Cipher

The idea of encrypting the information using matrix method is employed in one more encryption technique. In 1929 Lester S. Hill proposed a new way to encrypt the message and named his technique after his name that is hill cipher. In this method n linear combinations of the n alphabetic character in one original text element, thus producing the n alphabetic character in one cipher text element. There is a pseudo code that will help to understand the working of the hill cipher [3].

| Pseudo code_ Hill_ Cipher |
|---|
| Let n be a positive integer<br>Assume<br>Let n be a integer<br>Let $O=C=(X_{26})^n$<br>$K=$ (n*n) invertible matrices over $X_{26}$<br>For key k,<br>Execute,<br>$E_K(\alpha) = (\alpha K)$<br>and<br>for decryption;<br>Perform<br>$D_K(\beta) = (\beta K^{-1})$<br>Where,<br>All operations are performed in $X_{26}$ |

**Figure 8:** Pseudo Code of Hill Cipher

### 3.2.6 Vernam Cipher

Vernam cipher is also known as onetime pad. In this the plain text is encrypted by pairing it with a secret random key. Then every bit of the text is encrypted by combining it with the corresponding character from the pad using modular addition [13].

| Pseudo code_ Vernam_ Cipher |
|---|
| Let n be a positive integer and $n \geq 1$<br>Let $O=C=(X_2)^n$ ;<br>$K= (X_2)^n$ ;<br>Execute,<br>$E_K(\alpha) = (\alpha K_1 + \alpha_2 K_2 - - - \alpha_n K_n) \bmod 2$ // $E_K$ exclusive or (XOR) of two terms.<br>and<br>for decryption;<br>Perform<br>$D_K(\beta) = (\beta_1 K_1 + \beta_1 K_1 - - - \beta_n K_n) \bmod 2$ |

**Figure 9**: Pseudo Code of Vernam Cipher

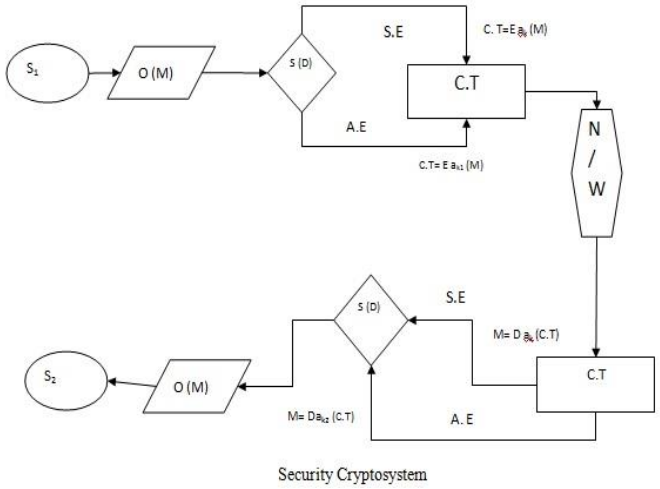
### 3.2.7 Enigma Machine

In World War I enigma machine plays a vital role in enciphering the messages that is exchanged between one stations to the other. Enigma Machine was proposed by Arthur Scherbius in 1923. The enigma machine consists of four parts the rotors, a lamp board, a plug board and a keyboard. For ciphering the text message a letter was typed on the keyboard. It passed through the rotors that scramble the text and display the cipher on the lamp board [14]

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

## 3.3 Modern Cryptography

In Modern era of cryptography more complex and strong techniques are proposed that ensures the high level of security. The algorithms are categorized in two categories one is symmetric key encryption and another one is asymmetric key encryption.




Security Cryptosystem

**Figure 10**: Security Cryptosystem

This is the basic flow that how the encryption and decryption take place.

| Symmetric Equations | Asymmetric Equations |
|---|---|
| Encryption : - C.T= $E_{ak}$ O(M) | Encryption : - C.T= $E_{ak1}$ O(M) |
| Decryption : - O(M)= $D_{ak}$ (C.T) | Decryption : - O(M)= $D_{ak2}$ (C.T) |

| | |
|---|---|
| $S_1$ | Source |
| $S_2$ | Sink |
| O (M) | Original Message |
| C (M) | Covert Message |
| K | Key |
| $E_{ak}$ | Encryption Algorithm |
| $D_{ak}$ | Decryption Algorithm |
| S.E | Symmetric Encryption |
| A.E | Asymmetric Encryption |
| S(D) | Sink, Source Decision |

### 3.3.1 Symmetric Key Encryption

In symmetric key encryption only one key is used for both encryption and decryption process

### 3.3.2 Digital Encryption Standard

Digital encryption standard is based on the Fiestel structure. It consists of 16 rounds that are the main algorithm is repeated for the 16 times. In DES, the input is taken in the form of blocks, as it is block cipher. Here the block size is of 64 bits and the key is 56 bits. In DES plaintext is divided into two equal block size of 32 bits, say Left side and right side. After this the internal process likes expansion or the permutation, substitution, permutation is performed. At the end both the sides are swapped to each other say, left become right and right become left [15].

### 3.3.3 Advanced Encryption Standard

Drawbacks that lead DES down is cover up in Advanced Encryption Standard. The main disadvantage of DES is the key size. But in AES the key size is large enough to encode the message into the cipher code. Here in AES three key sizes are available that is 128 bits that is used normally and 192 and 256 bits that is use where high security is required [16].

```
Algorithm _Advanced _ Encryption _Standard_ Encryption
Begin
{
Read Plaintext Pt;
Perform ADK ;                 //  Add Round Key
    Current Block ⊗ Portion of the Expanded key;
If R<9;
For (R=1,R<9,++R)
{
   //Round
            SB;              // Substitute Bytes

            SR;             // Shift Rows

             MC;           // Mix columns

            ADK;
}
End
          If R=9;
For (R=1,R<=9,++R)
{
   //Round
            SB;             // Substitute Bytes

             SR;           // Shift Rows

            ADK;         // Add Round Key
 }
End
}
end
```

**Figure 11(a):** Pseudo Code of AES Encryption

### 3.3.4 Asymmetric Key Encryption

In Asymmetric key encryption pair of key is used for encryption and decryption purpose. In this one key is used for encryption by the sender and another key used by the receiver for decryption purpose. There are some of the techniques that follow the asymmetric key encryption principle. Two techniques are described

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

```
Algorithm _Advanced _ Encryption _Standard_ Decryption
Begin
{
Read Ciphertext Ct;
Perform ADK ;                    // Add Round Key
    Current Block ⊗ Portion of the Expanded key;
If R<9;
For (R=1,R<9,++R)
{
            // Round

    ISR;                         // Inverse Shift Rows

    ISB;                         // Inverse Shift Bytes

    ADK;

    IMC;                         //Inverse Mix Columns
}

End

          If R==9
For (R+1,R<=9,++R)
{

       ISR;

       ISB;

       ADK;
}
End
}
End
```

**Figure 11(b):** Pseudo Code of AES Decryption

***3.3.4.1 RSA***

The approach of using public key cryptography was first introduced by Diffie and Hellman in their paper and that will lead to RSA [17]. RSA is well known public key encryption algorithm. Here, in RSA the cipher code is generated from the equation:

$$C=Me \bmod n$$

And the inverse would be calculated from the following equation:

$M=C\ d \bmod n$

$= (Me)\ d \bmod n$

$=Med \bmod n$

| Pseudo Code_ RSA_ Key _ Generation | |
|---|---|
| Select a, b | p an q both prime , $a \neq b$ |
| Calculate n= a x b | |
| Calculate $\phi(n)$ =(a-1) (b-1) | |
| Select integer I | gcd $\phi(n)$, I =1; 1<i< $\phi(n)$ |
| Calculate d | $d= i^{-1} \bmod \phi(n)$ |
| Public key | KU=[I,n] |
| Private key | KR= [d,n] |
| For Encryption | |
| Original Message: | M<n |
| Cipher Text: | $C= M^e \pmod n$ |
| For Decryption | |
| Cipher Text: | C |
| Original Message: | $M= C^d \pmod n$ |

**Figure 12:** Pseudo Code of RSA

***3.3.4.2 Quantum Cryptography***

The use of quantum cryptography initiated in 2003. In it two protocols are used for quantum key distribution these are BB84 and E91. The message initiated from the sender side is in either horizontal or in vertical basis or in diagonal or anti diagonal basis. In quantum cryptography some of the devices are required for the encryption of the message. These are the photon device, polarization optics and photon detectors. In quantum cryptography problem of distance between sender and receiver occurred because it covers nearly 200 km [18, 19, 20].

## 4. CONCLUSION

From the ancient times it is seen that the security is one of the important aspects in the ways of communication. Lots of tricks and concepts have been exercised to maintain the high security. Since the classic era various methods are used to hide the information. Vernam cipher, play fair ciphers are some of the examples. These were very effective and not easy to break. But as the time moved, more complex security systems were required to secure the communication over the network. In medieval era more techniques came into existence that promised to veil the information from the third party. Moving forward various machines was designed at the time of World War II which played an enormous role in securing the information over the wide area the network e.g. the enigma

International Journal of Computer Science Research (IJCSR)
Review Article | Volume 1, Issue 1 | Pages 24-30 | ISSN XXXX-XXXX

machine. As clock is moving continuously more and more techniques came and serve the purpose of securing the information. In the modern era some of the remarkable techniques were developed and it was difficult to break them. For instance in the category of symmetric key encryption, the DES and AES were developed and in the category of asymmetric key encryption RSA like algorithms were generated. DES makes use of 56 bit keys to encrypt the message whereas AES make use of 128, 192 and 256 keys to encrypt the message. As from the key size it is easy to judge the breakability of the technique. It is clear from the previous knowledge in the cryptography that number of keys are directly proportional to the security provided by the algorithm. From the above analysis, security has become an paramount concern in our daily lives. In the competitive world everybody wants to move ahead of others through their introspection and innovations. But side by side the ethical issues are coming into existence that hampers the confidentiality and integrity of somebody's personal information. In such cases cryptographic techniques come into play and help in securing the data from being hacked. However, choosing the right package with right security parameters can lead to a secure and best performance communication environment. Encryption and Decryption requires generating a matrix which is essentially the power of security. As the time passes the 256 bit encryption algorithm may also fail. From the above it is learnt that various techniques that aid in granting more safe and sound security system for will be in demand.

## 5. ACKNOWLEDGMENT

This work was supported in part by the CSE Department of Computer science and engineering", Head and faculties.

Prof. (Dr.) Amit Verma is professor and head department of Computer Science and Engineering, University institute of Engineering, Chandigarh University Gharaun. (E-mail: amit.verma@cumail.in).

Er. Anjali Gakhar is ME Student, department of Computer Science and Engineering, University institute of Engineering Chandigarh University Gharaun (Email: anjaligakhar7@gmail.com).

## REFERENCES

[1] Wade Trappe and Lawrence C. Washington," Introduction to cryptography with coding theory"2nd Edition, ISBN 0-13-198199-4, 2006.

[2] David Khan "The Code Breakers-The Story of Secret Writing", February, 1973.

[3] Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, 1995.

[4] Gardner, M. "Codes, Ciphers, and Secret Writing", ISBN 0-486-24761-9, pp 7-96, December 1972.

[5] [A Short History of Cryptography Available at "https://www.youtube.com/watch?v=H9Cu36Qj3dQ "Access on 12/28/2014. Richard W. Selby."Enabling Reuse-Based Software Development of Large-Scale Systems ", 2005, IEEE.

[6] Ancient Civilization available on "http://www.dl.ket.org/humanities/connections/class/ancient/index.htm" Accessed on 31/1/2015

[7] A Brief History of Cryptography." Cryptozine. 16 May 2008.

[8] Dennis Luciano and Gordon Prichett,"From Ceaser to public Key Cryptosystem", published in Mathematical Association of America, vol. 18(1), pp 2-17, January 1987.

[9] Atul Kahate "Cryptography and Network Security" Tata McGraw- Hill Edition 2008 ISBN-10:0-07-064823-9.

[10] Richard A. Mollin "An Introduction to Cryptography

[11] Bedini, Silivio A. "Thomas Jefferson: Statesman of Science", ISBN 0028970411, Newyork: Macmillan c1990

[12] Mauborgne, "An Advanced Problem in Cryptography and its Solution" The Army Service Schools, Port Leavenworth, Kansas, 1914.

[13] C.E. Shannon "Communication Theory of Secrecy System", Bell System Technical Journal, vol. 28(4), pp. 656-715, ISSN 0005-8580, October 1949.

[14] Louis Kruth and Ciphere Deavours "The Commercial Enigma: Beginnings of a Machine Cryptography", Cryptologia, Vol. XXVI (1), pp. 1-14, January 2002.

[15] Miles E. Smid and Dennis K. Brantad "The Data Encryption Standard: Past and Future", Proceedings of IEEE, vol. 76(5), pp. 550-559, May 1998.

[16] Federal Information Processing Standards Publication 197"Specification for the Advanced Encryption Standard", pp 1-47, 26 November 2001.

[17] Whitfield Diffie and Martin E. Hellman" New Directions in Cryptography" IEEE Transactions on Information Theory, Vol. IT 22 No. 6, pp. 644-654, November 1976.

[18] N. Gisin, G. Ribordy, W.Tittel, and H. Zbinden, "Quantum Cryptography", Rev. Mod. Phys. 74, pp- 145-195, 2002

[19] Damien Stucki. Et. al."Continuous High Speed Coherent One-way Quantum Key Distribution" OPTICS EXPRESS, Vol. 17(16), pp-13327-13334, 3 August 2009.

[20] Artur Scherer, Barry C. Sanders, and Wolfgang Tittel" Long- distance practical key distribution.