CHAPTER II

LITERATURE SURVEY

Cryptography is the art and discipline of codifying the messages, so as only the authorized users can have access to the text. Further subsections of this chapter discuss various Substitution and Transposition techniques, Symmetric key, Asymmetric key algorithms and recent improvements in Cryptography.

2.1 SUBSTITUTION STRATEGIES

We revisit few of the replacement strategies which have been implemented previously. The original text is possibly filled up by numerals, characters and symbols. The detail study of few well known encryption procedures in light of substitutions is specified in this part.

2.1.1 Caesar cipher

A flexible and more convenient process by Julius Caesar , which goes through a strategy of exchanging every letter of the alphabet with another letter ‘3’ positions further below the alphabet[13].

For example,

Plain-text: party over

Cipher-text: sduwbwyhu

A set of alphabets are aligned such that Z is preceded by A. The numbers 0 to 25 are allotted to the alphabets then at that instance cipher-text character c is given as

\[ c = E (3, p) = (p + 3) \mod 26. \]
2.1.2 Modified Caesar Cipher

Uniform replacement indicates a shift of $K$ characters rather than 3 characters which is nothing but the modified Caesar cipher. Considering the cipher-text character as $c$ and proceeding out assumption that taking the plain-text character $p$ and key $k$, the functions for both encryption $E$ and decryption $D$ are determined as \[13\].

$$C = E(p, k) = (p + k) \mod 26, \text{ where } 1 \leq k \leq 25$$

$$P = D(c, k) \mod 26$$

2.1.3 Mono alphabetic cipher

In contrast to the uniform replacements shown in Caesar cipher, the Mono alphabetic cipher utilizes a specific way in which cipher-text of a ‘c (a)’ will be filled up by any other character b by means of z, also the filling up of b is completed confined to any other character a by means of z other than b soon \[13\].

$$c(a) = \{b, c, d, e, ..., z\}, c(b) = \{a, c, d, e, ..., z\}, c(f) = \{a, b, c, d, e, g, h, ..., z\}$$

Plain-text: cryptography

Cipher-text: esijwqygyf

2.1.4 Homophonic Substitution Cipher

A part of individual character replacements specified above ciphers, Homophonic substitution cipher possess a well-designed set of cipher text character so that the base text character $p$ will be filled up using one of the cipher-text characters in the designed set\[13\].

$$c(a) = \{h, r, d, p\}, c(b) = \{e, i, q, s\}, c(c) = \{f, j, r, t\} \text{ soon.}$$
2.1.5 Polygram Substitution Cipher

The conversion of base text to cipher – text is done chunk by chunk rather than byte by byte [13] is the basic process opted for the Polygram substitution cipher.

\[ c (\text{the}) = \{\text{sam}\}, c (\text{sri}) = \{\text{ghj}\}, \text{so on.} \]

2.1.6 Poly alphabetic Substitution Cipher

A cipher which is based on replacement by means of multiple replacements of alphabets is named as Polyalphabetic Substitution Cipher. The best suited example [13] for this kind of cipher is the vigenere cipher.

2.1.7 Play fair cipher

A cipher which is generally utilized for encryption purpose is play fair cipher which is well known as the play fair square. This cipher was well utilized by the troops of British and Australians during the world wars. This particular strategy comprises of two pivot steps [13]

i. Create and Populate the Matrix

ii. Encryption Procedure

The following steps will best explain about Create and Populate the Matrix

a) A 5X5 matrix is formed for row-wise left to right; then from top to bottom considering the keyword, thereby eradicating the replicate letters.

b) In order to fill up the left over spaces of the matrix, the English alphabets [A-Z] are utilized which has no role in our keyword text.

c) By doing so the same cell matrix is used to combine I and J, being I or J is a part of key that has been utilized, disregard both I and J while filling the other cell of the matrix.
The proceeding steps will explain the standard Encryption Procedure

a) A set of alphabets are formed by breaking the actual text message that we wish to encrypt there by creating the possibility that encryption proceeds only on the message which got divided.

b) Add “X” after the first letter when either letters are present in same set (or only one letter is left) thereby proceeding to encrypt a new set and continue.

c) Exchange the letter to their next right correspondingly when a letter is present on the same row of your table. In case the original set is situated at the right side of the row then opt for the process of wrapping around towards left side of the row.

d) If the letters show up on a similar column of your table, supplant them with the letters immediately down the lane letter. Fold over to the top side of the column if a letter in the original pair was on the bottom side of the column.

e) If the letters are not on a similar row or column, supplant them with the letters on a similar row separately yet at the other pair of corners of the rectangle characterized by the original pair. The request is making a difference much here. The first letter of the encoded pair is the one that lies on similar row as the main letter of the plain content pair.

Key: cryptography
Plain-text: my name is sriram
Broken Plain-text: my na me is sr ir am
Cipher-text: nrwfvmkqmtepgnct

2.1.8 Description of Hill cipher

Lester Hill had proposed this cipher in 1929 that works on multiple characters at a time. It has its underlying foundations in mathematics, specifically about the operations on the matrix viz., Matrix multiplication, Inverse of a matrix (for decryption). The significant steps of encryption involved in this algorithm are as follows [13].

a) Consider the Plain-text character values as 0-25 for the characters a-z.
b) Based on the above consideration the numbers obtained with respect to the plain-text are organized as a matrix of desired order $m \times n$, $m$ shows count of rows and $n$ demonstrates count of columns.

c) Select a key matrix of randomly chosen decimal numbers of order $m \times m$, where $m$ shows count of rows in the plain-text matrix.

d) Apply multiplication task between the key matrix and the plain-content matrix.
   [Resultant matrix is order $m \times n$]

e) Now compute $mod\ 26$ to the matrix obtained above.

f) Thus the matrix will have the values with range 0-25 and replace them as characters $a$-$z$, produces the cipher-text.

### 2.2 TRANSPOSITION STRATEGIES

We revisit few of the transposition strategies which have been implemented previously. A Transposition strategy is one where characters of plain content are permutated i.e., position of the letters being changed. Even the permutations have been done; the length of plain and cipher contents is same.

#### 2.2.1 Rail-Fence Technique

At first the plaint content characters are placed as series of diagonals, then cipher content is generated by writing plain content characters row-wise [14].

**Plain-text:** cryptography  **Key:** 2 (two rows)

```
  c       y       t       g       a       h
  r       p       o       r       p       y
```

**Cipher-text:** cyngahrporpy

#### 2.2.2 Simple Columnar Transposition Technique

It is a technique which has a slight variation in Rail-fence technique. The following is the sequence of steps involved in this encryption technique [14].
a) Consider a box of predefined size and represent the plain content row-wise.

b) Cipher content can be generated by representing the characters column-wise.

\[
\text{Plain-text: cryptography}
\]

\[
\begin{array}{ccc}
\text{c} & \text{r} & \text{y} \\
\text{p} & \text{t} & \text{o} \\
\text{g} & \text{r} & \text{a} \\
\text{p} & \text{h} & \text{y}
\end{array}
\]

Key: 213 Cipher-text: rtrhcppgyoay

### 2.2.3 Simple Columnar Transposition with Multiple Rounds

It is a strategy of using multiple rounds instead of having one round of encryption as mentioned [14].

a) Write the Plain content/Intermediate Cipher-text characters row-wise in a rectangle of predefined size

b) Write the text column-wise, results in intermediate cipher-text.

c) Repeat steps a through b for desired number of times and the latest text obtained can be considered as cipher-text.

### 2.2.4 Vernam Cipher (One time pad)

The Vernam cipher, whose particular subset likewise called the “one-time pad”, is actualized utilizing an arbitrary arrangement of non-repeating characters as input cipher content. The point here is that "once an input cipher content utilized for the transposition, it is never utilized again for some other messages" essentially legitimizes the word “one-time pad”. The following is the sequence of steps involved in this encryption technique [14].

a) Consider the Plain-text character values as 0-25 for the characters a-z.

b) Generate the key characters of the length same as plain-text and write their corresponding values as same as the step ‘a’.

c) Add the Corresponding values of the steps ‘a’ and ‘b’.
d) If the resultant sum is greater than 25, then do step ‘c’-25. [Positive value]
e) Write the corresponding characters such that 0-25 replaces a-z.

<table>
<thead>
<tr>
<th>Plain-text</th>
<th>c</th>
<th>r</th>
<th>y</th>
<th>p</th>
<th>t</th>
<th>o</th>
<th>g</th>
<th>r</th>
<th>a</th>
<th>p</th>
<th>h</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain-text Values</td>
<td>2</td>
<td>17</td>
<td>24</td>
<td>15</td>
<td>19</td>
<td>14</td>
<td>6</td>
<td>17</td>
<td>0</td>
<td>15</td>
<td>7</td>
<td>24</td>
</tr>
<tr>
<td>Key</td>
<td>n</td>
<td>c</td>
<td>b</td>
<td>t</td>
<td>z</td>
<td>q</td>
<td>a</td>
<td>r</td>
<td>x</td>
<td>q</td>
<td>r</td>
<td>x</td>
</tr>
<tr>
<td>Key Values</td>
<td>13</td>
<td>2</td>
<td>1</td>
<td>19</td>
<td>25</td>
<td>16</td>
<td>0</td>
<td>17</td>
<td>23</td>
<td>16</td>
<td>17</td>
<td>23</td>
</tr>
<tr>
<td>Sum</td>
<td>15</td>
<td>19</td>
<td>25</td>
<td>34</td>
<td>44</td>
<td>30</td>
<td>6</td>
<td>34</td>
<td>23</td>
<td>31</td>
<td>24</td>
<td>47</td>
</tr>
<tr>
<td>Resultant Value</td>
<td>15</td>
<td>19</td>
<td>25</td>
<td>8</td>
<td>18</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>23</td>
<td>5</td>
<td>24</td>
<td>21</td>
</tr>
<tr>
<td>Cipher-text</td>
<td>p</td>
<td>t</td>
<td>z</td>
<td>g</td>
<td>s</td>
<td>e</td>
<td>g</td>
<td>i</td>
<td>x</td>
<td>f</td>
<td>y</td>
<td>v</td>
</tr>
</tbody>
</table>

2.3 CRYPTOGRAPHY ALGORITHMS

In this section we would like to present a few cryptographic algorithms that have been studied in formulation of this thesis. The secret key cryptosystems that uses two identical keys for the process of enciphering and deciphering are said to be Symmetric-key algorithms. The algorithms DES, IDEA, AES were discussed under this category. The public key cryptosystems that uses two un-identical keys for the process of enciphering and deciphering are said to be Asymmetric-key algorithms. The RSA algorithm was discussed under this category.

2.3.1 DES[15]

The most broadly utilized encryption conspire depends on the Data Encryption Standard (DES) [15] issued in 1977, as Federal Information Processing Standard 46 (FIPS 46) by the National Bureau of Standards, now known as the National Institute of Standards and Technology (NIST). The procedure itself is alluded to as the Data Encryption Algorithm (DEA).

Description of the Algorithm: The plaintext is 64 bits long and the key is 56 bits long; longer plaintext sums are handled in 64-bit squares. The DES structure is a minor variety of the existing Feistel structure. There are 16 rounds of handling. From the first 56-bit key, 16 sub keys are produced, one of which is utilized for each round. The procedure of
unscrambling with DES is basically the same as the encryption process. The trick is as follows: Use the cipher content contribution to the DES calculation, yet utilize the sub keys Ki in turn around arrange. That is, utilize K16 on the primary cycle, K15 on the second emphasis, et cetera until the point that K1 is utilized on the sixteenth and last cycle [14-15].

2.3.2 AES[18-19]

AES utilizes a block length of 128 bits and a key length that can be 128, 192, or 256 bits. In the depiction of this area, we accept a key length of 128 bits, which is probably going to be the one most usually actualized. Fig 2.1 demonstrates the general structure of AES [18-19].

![Diagram of AES encryption and decryption process]

Fig 2.1: Detailed execution of Encryption and Decryption in AES
2.3.3 RSA-Rivest-Shamir-Adleman Algorithm

The vital feature of RSA public-key cryptosystem is that the encryption and decryption procedure are done with two different keys - public key and private key respectively. Its security is based on the issues like difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution”. The following algorithm gives the brief description of RSA [20].

Step1. Key Generation
Step2: Encryption
Step3: Decryption

Procedure for Step1 (Key Generation):
- Select two distinct prime numbers \( p \) and \( q \).
- Calculate \( N = p \times q \).
- Calculate \( \phi(n) = (p - 1) \times (q - 1) \).
- Select an integer \( \phi \) whose \( \gcd(\phi(n), \phi) = 1; 1 < \phi < \phi(n) \).
- Determine \( d \) (using modular arithmetic) which satisfies the congruence relation \( d \times e \equiv 1 \pmod{\phi(n)} \). \( d \) is kept as private key component.
- Public key = \( \{e, N\} \).
- Private key = \( \{d, N\} \).

Procedure for Step2 (Encryption): \( C = M^e \pmod{N} \).

Procedure for Step3 (Decryption): \( M = C^d \pmod{N} \).

Where, \( C \) - Cipher text, \( M \) - Message, \( p \) and \( q \) - Prime Numbers, \( N \) - Common Modulus, \( e \) and \( d \) - Public and Private Keys Respectively.

2.4 RECENT IMPROVEMENTS IN CRYPTOGRAPHY

The process of enciphering a message using public key into nonlinear equations thereby transforming to get the actual information by the assigned party using private key is better suggested through an algorithm by “Zirra Peter Buba & Gregory Maksha Wajiga” [21]. An attempt by the intruder to intercept the information which lead to the enhanced complexity in deciphering, as multilevel ciphers exist in the proposed application.
An innovative method for providing security to the data during the process of encrypting the same, which possess Armstrong numbers and colors as authentication is well explained by “Kranti Sonawane, Sneha Phulpagar & Prof. A.P. Yadav” [22]. Considering color as an important security element, authentication is provided by making use of a combo of three key pairs.

By combining public and private key along with the assistance of third prime number “Al-Hamami Alaa Hussein and Abdallah Aldariseh Ibrahim” [23] suggested a new way of enhancing the RSA algorithm. As a result of that, the complexity in factoring the variable will be enhanced, also the procedure of its study with the progress of equipment and tools can be done with relative ease.

The complexity involved in factorization which is linked to security is accomplished by “Priyanka Trikha, Ashish Vijay & Ashik Hussain” [24] using RSA Digital Signature Algorithm (RSADSA). Breaching the factorization problem will ultimately lead to achievement of private key also. The suggested RSADSA is vulnerable to factorization of prime along with other small private power d and little of public exponent e breaches.

Creation of public and private keys on smart card by utilizing crypto-Coprocessor and True Random Number generator to provide secure and rapid generation of RSA yielded 50% less in overall of key generation time along with 10% reduction of cumulative time in the process of creating key sets which are intended to do the main processor activities and other 90% is for crypto-coprocessor functions are all explained using an unique approach by M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani [25].

A result of 10% computational costs, decrease of 66% in computational costs to decryption methods basing on CRT and 2.9 times speed compared to decryption method based on CRT is obtained based on a theory proposed by H. Ren-Junn, S. Feng-Fu, Y. Yi-Shiung and C. Chia-Yao [26] using an efficient decryption method in RSA cryptosystem.
A high-speed execution of RSA was proposed by “Nagar, S.A.; Alshamma, S”. [27], affects the system by storing the keys indexes as Nid, Eid, Did instead of n, e, d, which will have a better level of security.

An encryption/decryption rate between 328 to 578Kb/s has been achieved by considering the remainder theory on Chinese by means of RSA cryptosystem designed by Chung-Hsien Wu; Jin-Hua Hong; Cheng-Wen Wu, [28].

The challenges linked to factoring large numbers and estimating discrete logarithms where the security is depended on these, also to achieve high flexibility parameters are adopted as an advantage is suggested by Wang Rui; Chen Ju; Duan Guangwen, [29] using “A k-RSA algorithm.

Two variants of RSA-CRT were proposed by Hung-Min Sun and Mu-En Wu, [30], for fast encryption. One among them works on encryption time which has been reduce to about 2.7 of time required by existing Rebalanced RSA-CRT, another variant states that encryption is three faster than existing one, but the decryption is slower than that of Rebalanced RSA-CRT.

In view of increasing the security of the cryptosystems through natural numbers, Sharma, Sonal, Jitendra Singh Yadav, and Prashant Sharma [31] proposed a Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm which uses two natural numbers in pair of public and private keys.