Bio – Security Metrics for Cryptanalysis

R. P. Jaia Priyankka
M.Phil Research Scholar, Dept. of Computer Science
St. Joseph's College of Arts & Science (Autonomous)
Cuddalore, India
jaiapriyankka@gmail.com

G. Jenitha
M.Phil Research Scholar, Dept. of Computer Science
St. Joseph's College of Arts & Science (Autonomous)
Cuddalore, India
Jenitha.joel@gmail.com

V. Vennila
M.Phil Research Scholar, Dept. of Computer Science
St. Joseph's College of Arts & Science (Autonomous)
Cuddalore, India
vennilamphil@gmail.com

***Abstract*—Encryption and decryption technique are protecting our world. More secured information's are encrypted before that data could travel all around the world. There are more types of encryption techniques used by all. Some of the techniques which used are Rotor machine, Elliptic Curve, in the same order we have designed a cipher technique. Every encryption data travels along with its key. When the hackers want to break the code they refer the key to find out the techniques and they easily hack our secured data but our cipher even if delivered with key directly in the hands of the hacker he could not decrypt it. We have framed it by analyzing every nook and corner of the thread infecting the Crypto world. We have combined the biometric process along with the cipher technique to create a new impression in the field of encryption.**

Keywords*— *Encryption, Decryption, cipher, Military, Elliptic curve, Biometric.

I. INTRODUCTION

A key is a piece of information that determines functional output of an algorithm or cipher [1]. Without a key the algorithm would not produce more successful result. In encryption, the key specifies the information of a plain text into a cipher text and vice versa during decryption [7]. Encryption is the form of converting data that cannot be easily understood by unauthorized people [3]. The use of encryption/decryption is an art of communication. During war time, a code can be employed to keep the enemy to obtaining the content of the message [10]. In order to recover the content of an encrypted message, the correct decryption key is required. Encryption/ Decryption Is essentially important in wireless communication [14]. The stronger the cipher it is harder for the unauthorized people to break. Biometrics associates the use of unique physiological characteristic of the individual [11]. Biometrics traits have been developed to authenticate the person's identity [13]. Biometrics is a pattern recognition system which makes a personal identification by determining the authenticity of a specific behavioral characteristic [12].

A. Existing Finger Print Application

Finger print biometrics are widely used for secured purposes in various filed like documents where they authenticate the user by their thumb impression [4]. Bank uses finger print application for the security purposes; government officials also use the finger print application for the security of data [9]. Finger print applications are widely used in many fields for the security of data.

II. LOGIC CIPHER

All types of encryption technique used till this moment are trying to reveal its best on security measures [2]. Same way all the analysis on the biometrics process proves out to be outstanding hence we have integrated both the concept to route our new cipher process called logic cipher [8].

III. CIPHER METHODOLOGY

We have 26 alphabets according to that the numbers are assigned to the certain alphabet as in Fig 1.

A. For Example

According to the number mentioned above, the text RED ALERT is taken as

R=18, E = 5, D=4, A=1, L=12, E=5, R=18, T= 20 .Three persons are considered as 1-jai, 2-jeni, 3- veni. R represents Right Hand, M represents Middle Finger. The middle finger is taken in four directions

1. Center
2. Center Up
3. Center Down
4. Full

Middle finger center impression given in Table 1 it gives the finger print image and the value derived from it. With help of the key the encrypted value must be must be known. If it is R take the opposite value or R it is I

C represents Centre, F represents full then symbols are used for manipulation like addition ⊕, Subtraction Θ, Multiplication ⊗, division ⊘. Then represent above the midpoint of a thumb impression, represent below the midpoint of a thumb impression. The encrypted code is about to be sent to jai. The ciphered examples are

1) Encryption for Center Up:

PLAIN TEXT: RED ALERT

R=18, E = 5, D=4, A=1, L=12, E=5, R=18, T= 20

KEY: 1RMC 

(Here the center up encryption is 25)

CIPHER TEXT : Take the opposite alphabet and its value 9 22 23 26 15 22 9 7 then add our value with it 34 47 48 51 40 47 34 32

a) Decryption for Center Up:

CIPHER TEXT : 34 47 48 51 40 47 34 32

KEY: 1RMC 

Work Out: 34-25 =9, 47-25=22, 48-25=23, 51-25=26, 40-25=15, 47-25=22, 34-25=9 and 32-25 =7 and then reverse its alphabet value 18 5 4 1 12 5 18 20

PLAIN TEXT: RED ALERT

2) Encryption for Center:

PLAIN TEXT: RED ALERT

R=18, E = 5, D=4, A=1, L=12, E=5, R=18, T= 20

KEY: 1RMCϴ

(Here the center encryption is 15)

CIPHER TEXT : Take the opposite alphabet and its value 9 22 23 26 15 22 9 7 then subtract our value with it -6 7 8 11 0 7 -6 -8.

a) *Decryption for Center:*

CIPHER TEXT : -6 7 8 11 0 7 -6 -8

KEY: 1RMCϴ

Work out: -6+15 =9, 7+15 =22, 8+15 =23, 11+15=26, 0+15 =15, 7+15 =22, -6+15 =9, and -8+15=7 and then reverse its alphabet value 18 5 4 1 12 5 18 20

PLAIN TEXT: RED ALERT

3) *Encryption for Center down:*

PLAIN TEXT: RED ALERT

R=18, E = 5, D=4, A=1, L=12, E=5, R=18, T= 20

KEY: 1RMC 

(Here the center down encryption is 16)

CIPHER TEXT : Take the opposite alphabet and its value 9 22 23 26 15 22 9 7 then multiply our value with it 144 352 368 416 240 352 144 112

a) Decryption for Center Down:

CIPHER TEXT : 144 352 368 416 240 352 144 112

KEY: 1RMC 

Work Out: 144/16=9, 352/16=22, 368/16=23, 416/16=26, 240/16=15, 352/16=22, 144/16=9, 112/16=7 and then reverse its alphabet value 18 5 4 1 12 5 18 20

PLAIN TEXT: RED ALERT

4) Encryption for Full:

PLAIN TEXT: RED ALERT

R=18, E = 5, D=4, A=1, L=12, E=5, R=18, T= 20

KEY: 1RMCF ⍜

(Here the center down encryption is 40)

CIPHER TEXT: Take the opposite alphabet and its value 9 22 23 26 15 22 9 7 then divide our value with it 0.225 0.55 0.575 0.65 0.375 0.55 0.225 0.175.

a) Decryption for Full:

CIPHER TEXT : 0.225 0.55 0.575 0.65 0.375 0.55 0.225 0.175

KEY: 1RMCF ⍜

Work Out: 0.225*40 =9, 0.55*40 =22, 0.575*40=23, 0.65*40=26, 0.375*40=15, 0.55*40=22, 0.225*40=9, 0.175*40=7 and then reverse its alphabet value 18 5 4 1 12 5 18 20

PLAIN TEXT: RED ALERT

IV. FINGERPRINT

There is some procedure on how fingerprint looks like and work out. The types of fingerprint are given in Fig 2. The calculative procedure is simple but changes for each finger type of finger print. The radius should be taken to find the center part of the finger print. The two sides of the finger print should be counted separately if it gives the same count it can be taken otherwise add the total and take an average out of it. There are totally 320 ways of calculating the process of Bio security metrics.

V. MUTUAL RELATION WITH DATA MINING AND ARTIFICIAL INTELLIGENCE

The details of military utilities will be saved in a secure database. It may be accessed with bio metric finger print. If the person is not available our cipher text can be provided as an alternate password. Hence data mining field can be secured, when a humanoid computer is linked into our database for accessing our password. It is difficult because the finger prints are stored in image form, where system cannot read. While security access the system gives us Captcha half image and half word to prove ourselves as human. Thus this security measure is actually proven to be worthy.

VI. ADVANTAGES

The more advantage is that, the middle finger which we have used. Middle finger has the highest blood circulation even if our body is weak the circulation of blood is standard in the middle finger, which leads to good impression of fingerprint.

A. Example 1

If a particular person is called x derives an encryption technique called Grille cipher. First he implemented a new cipher by changing a little bit of concept from his base paper (altered encryption technique provided and used in the real world) [5]. Then he (x) later finishes the paper and publish it. X paper says a simple methodology can be changed in the original cipher so that fractionated Morse cipher is better efficient.

B. Example 2

- A person Y forms a new methodology of encryption technique how to be decrypted and he publishes the paper.

TABLE I. FINGER PRINT AND ITS CALCULATIVE NUMBER

Middle Finger Center Impression					
Names	**Finger Print**	**Center**	**Center Up**	**Center Down**	**Full**
Jai		15	25	16	40
Jeni		14	22	23	44
Veni		20	22	18	43

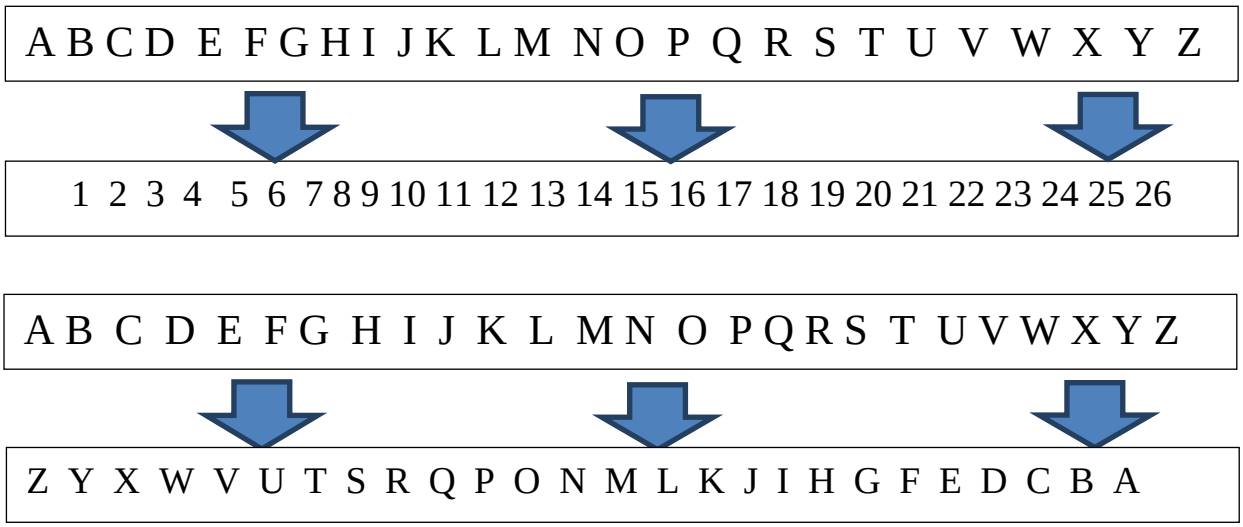

Fig. 1. Alphabetical Order (Numbers) and the reverse order of the Alphabets.

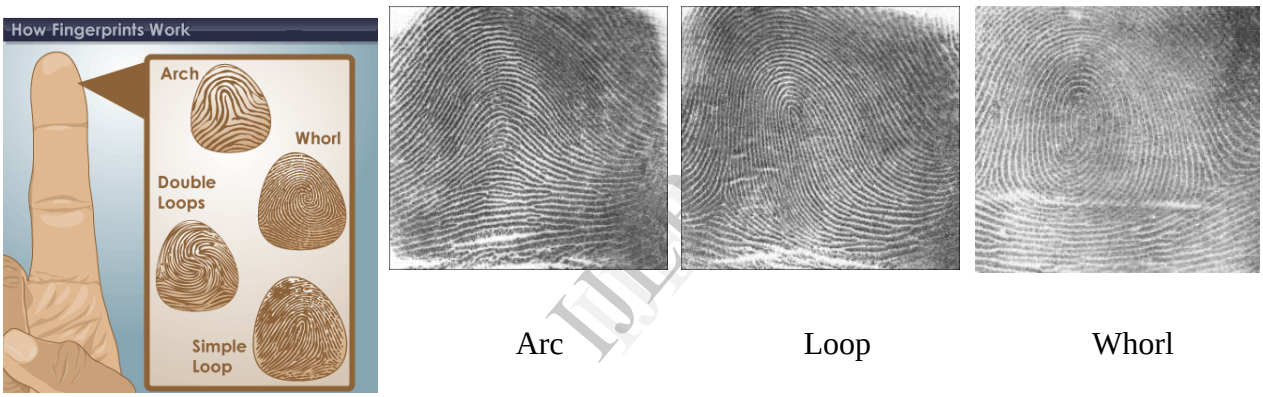

Fig. 2. Types of curves in Fingerprint.

- A few companies after reading those papers, Try to implement their data. Now this company is using X/Y encryption and sends their encrypted cipher to the real world [6]. Now the hacker can also have the possibility to learn the paper of X, Y. So if the hacker wants to hack the data of company Z it is very easy.
- In our proposed paper even if the hacker steals our data and the key from the internet or if he is going to see and learn the concept of our paper it is 95% very critical to hack our data. We really have strong reason to beat on 95% security.
    1) Any hacker 80% steals a data through internet, courier, postal and mainly through the social networking site.
    2) 2. 65% of normal persons use only thumb fingers for government use/ personal use or any type of activities.

VII. Conclusion & Future Enhancement

The logic cipher proposed in our paper is really secure and it can be used in high secured areas like military, CBI and government official data. This cipher is really unique and proves the tendency of satisfaction for encryption and decryption. This cipher can be still extended to left middle finger, right and left ladies finger, and also for all fingers in the toe.

References

[1] Curry, Ian, Entrust Technologies, "Getting Acquainted With Entrust/Solo and Public-key Cryptography", version 1.0, July 1997
[2] Netscape, "Introduction to Public-Key Cryptography",
[3] http://developer.netscape.com/docs/manuals/security/pkin/contents.htm
[4] Curry, Ian, Entrust Technologies, "Version 3 X.509 Certificates", July 1996, version 1.0
[5] Branchaud, Marc, "A Survey of Public-key Infrastructures", Department of Computer Science, McGill University, Montreal, 1997

[6] Curry, Ian, Entrust Technologies, “Key Update and the Complete story on the Need for Two Key Pairs”, version 1.2, August 2000

[7] R. Clarke, "Biometrics and Privacy," http : // www. rogerclarke. com /DV/Biometrics.html, 2001.

[8] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," IEEE Security and Privacy, vol. 1, no. 2, pp. 33-42, Mar. 2003, doi: 10.1109 / MSECP. 2003. 1193209

[9] Lakhmi C. Jain, Intelligent Biometric Techniques in Fingerprint and Face recognition

[10] Nalini K. Ratha, Andrew Senior and Ruud M. Bolle,”Automated Biometrics”. IBM Thomas J. Watson Research Center, PP 1-10

[11] Paul Reid, Biometrics for Network Security, Prentice Hall of India.

[12] Roger Clarke, “Biometrics And Privacy”

[13] Rula Abu Samaa‟n,”Biometrics Authentication Systems”, April 2003, PP 1-2.

[14] Vicki Koerper, “Biometrics: A Brief Introduction.