International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 6, June 2014)

Implementation of Caesar Cipher and Chaotic Neural network by using MATLAB Simulator

Jitender Singh[1], Prof Shyam Sunder Yadav[2]

Computer Science & Engineering, Maharashi Dayanand University, Rohtak, India

***Abstract* - Today as every information is in form of electronic data. The security of data is increased due frequent attacks by outsiders. So, there is a need to secure this information by using cryptography. Cryptography is a technique to make information unreadable for unauthorized users. Various algorithms are used for cryptography to convert original information. In this paper we are going to implement encryption and decryption using Caesar cipher and a brief case study of chaotic neural network.**

***Keywords*-- CNN, Symmetric key, Asymmetric key, Hashes, ANN, Nervous, Decipher**

I. Introduction

1.1 Cryptography:

Cryptography is a technique to make information unreadable for unauthorized users. Cryptography is the science of writing in secret code. The goal of cryptography is to achieve the integrity, confidentiality and authenticity of all the information resources. There are three types of cryptography - secret key or symmetric cryptography, public key or asymmetric cryptography and hash function. Cryptography can be defined as the exchange of data into a single code that can be deciphered and sent across a public or private network. Cryptography is the practice and study of hiding information. It is a critical part of secure communication. Cryptography not only protects data from robbery or alternation but can be used as well for user authentication.

Cryptanalysis of the news is the inverse process, in which the receiver of the cipher transforms it to the original text. The cipher key must have several heavy attributes. The best one is the singularity of encryption and cryptanalysis.

The goal of cryptanalysis is to make it possible to take a cipher text and reproduce the original plain text without the corresponding key. Two major techniques used in encryption are symmetric and asymmetric encryption. In symmetric encryption, two parties share a single encryption-decryption key.

The sender encrypts [1] the original message (P), which is referred to as plain text, using a key (K) to generate apparently random nonsense, referred to as cipher text (C), i.e.:

$$\boldsymbol{C = \text{Encrypt}\ (K, P)}$$

Once the cipher text is produced, it may be transmitted. Upon receipt, the cipher text can be transformed back to the original plain text by using a decryption algorithm and the same key that was used for encryption, which can be expressed as follows:

$$\boldsymbol{P = \text{Decrypt}\ (K, C)}$$

In asymmetric encryption, two keys are used, one key for encryption and another key for decryption. The length of cryptographic key is almost always measured in bits. The more bits that a particular cryptographic algorithm allows in the key, the more keys are possible and the more secure the algorithm become. The following key size recommendations should be considered when reviewing protection.

Symmetric key:

- Key sizes of 128 bits (standard for SSL) are sufficient for most applications.
- Consider 168 or 256 bits for secure systems such as large financial transactions.

Asymmetric key:

- Key sizes of 1280 bits are sufficient for most personal applications.
- 1536 bits should be acceptable today for most secure applications.
- 2048 bits should be considered for highly protected applications.

Hashes:

- Hash sizes of 128 bits (standard for SSL) are sufficient for most applications.

Consider 168 or 256 bits for secure systems [1].

A system that provides encryption [7] and decryption is referred to as a cryptosystem and can be created through hardware components or program code in an application. The most cryptosystem algorithms are complex mathematical formulas that are applied in a specific sequence to the plaintext. Most encryption methods use a secret value called a key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text. In all cases, the initial unencrypted data is referred to as *plaintext*.

It is encrypted into *cipher text*, which will in turn (usually) be decrypted into usable plaintext.

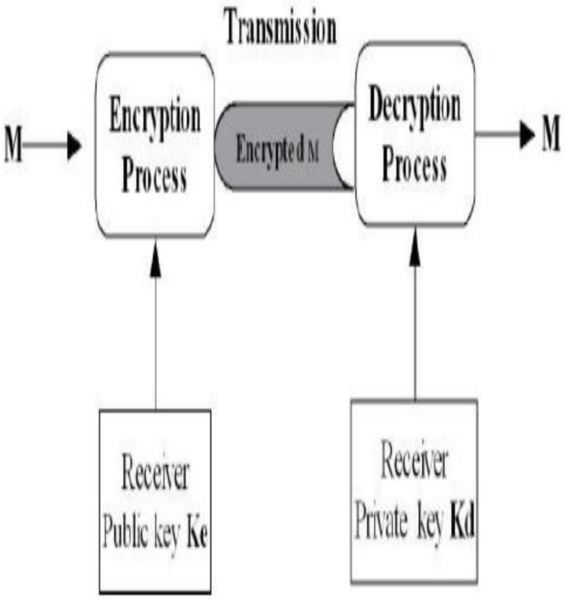


FIGURE 1: CRYPTOGRAPHY PUBLIC KEY COMPONENT [1]

II. NEURAL NETWORK

A neural network [2] is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use. It resembles the brain in two respects:

1. Knowledge is acquired by the network from its environment through a learning process.
2. Interneuron connection strengths, known as synaptic weights, are used to store the acquired knowledge.

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. An Artificial Neural Network (ANN) [4] is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information.

The key element of this paradigm is the structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurones) working in unison to solve specific problems.

Axon:-is a singular fibre that carries information away from the soma to the synaptic sites of other neurons (dendrites and somas), muscles, or glands.

Axon hillock:-is the site of summation for incoming information. At any moment, the collective influence of all neurons that conduct impulses to a given neuron will determine whether or not an action potential will be initiated at the axon hillock and propagated along the axon.

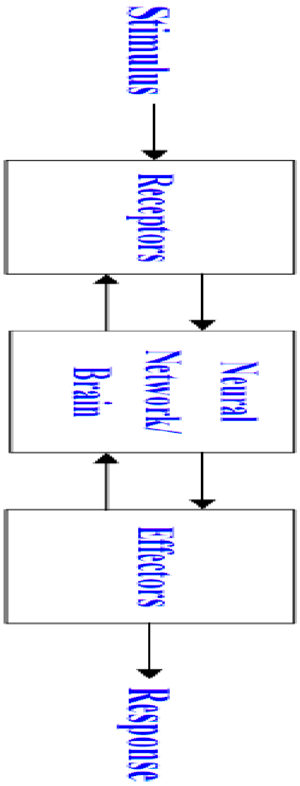


Fig. Block Diagram of a Human Nervous System.

The receptors collect information from the environment. The effectors generate interactions with the environment e.g. activate muscles. The flow of information/activation is represented by arrows.

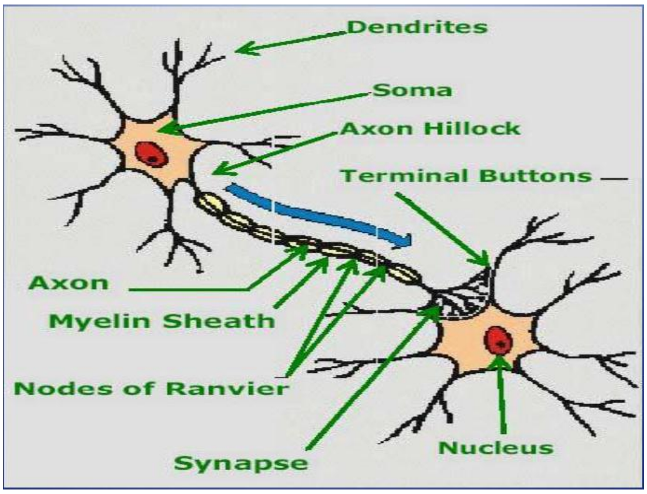


Fig. Schematic diagram of a Biological Neuron

Myelin Sheath:-consists of fat-containing cells that insulate the axon from electrical activity. This insulation acts to increase the rate of transmission of signals. A gap exists between each myelin sheath cell along the axon. Since fat inhibits the propagation of electricity, the signals jump from one gap to the next.

Nodes of Ranvier:-are the gaps between myelin sheath cells long axons are since fat serves as a good insulator, the myelin sheaths speed the rate of transmission of an electrical impulse along the axon.

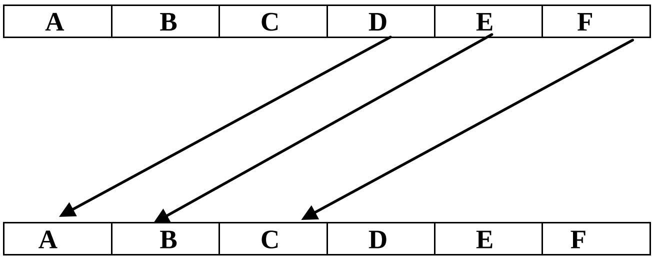
Synapse:-is the point of connection between two neurons or a neuron and a muscle or a gland. Electrochemical communication between neurons takes place at these junctions.

Terminal Buttons:-of a neuron are the small knobs at the end of an axon that release chemicals called neurotransmitters. [2]

III. Implementation Of Caesar Cipher And Chaotic Neural Network

3.1 Caesar Cipher:

Caesar cipher is one of the simplest [6] types of substitution method. In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A; E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.



The Action of ceasar cipher is to replace each plain text letter with one fixed number of places down the alphabet. In the above diagram a left shift of three, so that E in plaintext becomes B in cipher text.

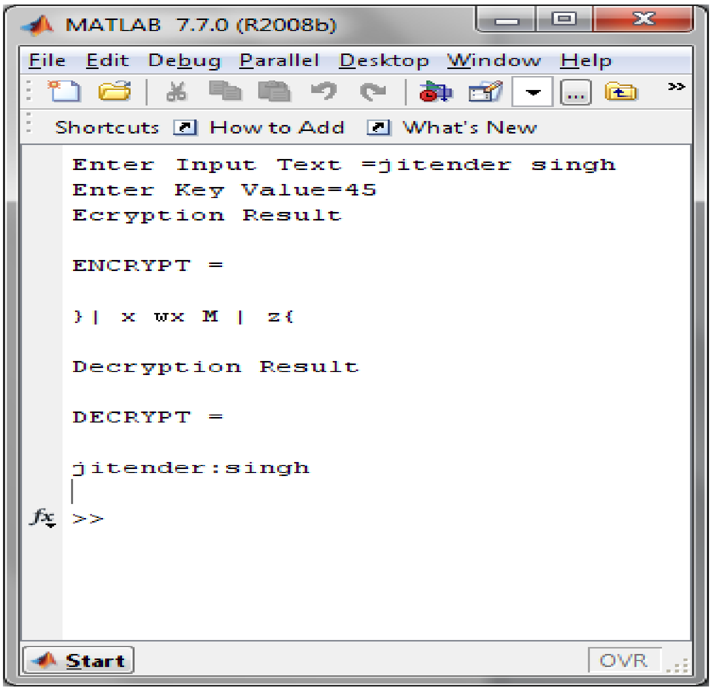
3.2 Advantage of Ceasar Cipher:

Ceasar Cipher is the ability to use these ciphers without the need to send any key information or have the cipher written down and subject to capture by the enemy. While other monoalphabetic cipher would normally require that cipher to be written down, they do offer a much stronger cipher.

3.3 disadvantage of ceasar cipher:

An attacker that knows the block size can separate out characters encoded with different different keys.

3.4 Result for Ceasar Cipher encryption and Decryption of messages:



```
Enter Input Text =jitender singh
Enter Key Value=45
Ecryption Result

ENCRYPT =

}| x wx M | z{

Decryption Result

DECRYPT =

jitender:singh

>>
```

3.5 Chaotic neural Network:

The chaotic neural network [3] can be used to encrypt digital signal. A network is called a chaotic neural network if its weights and biases are determined by a chaotic sequence. A chaotic sequence highly depend upon the initial condition and parameters, x (0)=0.75 and μ =3.9 are set. Difficult to encrypt and decrypt the data without knowing the x (0) and μ.

Depending upon the chaotic sequence a weight matrix and bias matrix is obtained and the net input is obtained. Chaotic neural network offers [5] greatly increase memory capacity. Each memory is encoded by an Unstable Periodic Orbit (UPO). Let g denote a digital signal of length M and g(n), 0<=M-1,be the one –byte value of the signal g at position n.

3.5.1 Features of CNN:

High Security
No distortion
Suitable for system integration

3.5.2 Steps followed to encrypt the message by chaotic neural network (CNN):

Step 1: Set the value of parameter M.

Step 2: Determine the parameter, U and the initial point x (0) of the 1-D logistic map.

Step 3: Evolve the chaotic sequence x(l), x(2), ... , x(M) by x (n+l) = μ(n)(l-x(n)), and create b(O), b(l), ..., b(8M-1) from x(l), x(2), ..., x(M) by the generating scheme that 0.b(8m-8)b(8m-7) ….. b(8m-2)b(8m-l) … is the binary representation of x(m) for m = 1, 2,. . . ., M.

Step 4: FOR n: 0 TO (M - 1) DO

$$Let\ \ g(n) = \sum_{i=0}^{7} d_i \times 2^i$$

For i= 0 TO **7** DO 1

$$w_{ji} = \begin{cases} 1 & \text{if } j = i \text{ and } b(8 \times n + i) = 0, \\ -1 & \text{if } j = i \text{ and } b(8 \times n + i) = 1, \\ 0 & \text{if } j \neq i, \end{cases}$$

J € (0, 1, 2, 3, 4, 5, 6, 7)

$$\theta_i = \begin{cases} -\frac{1}{2} & \text{if } b(8 \times n + i) = 0, \\ \frac{1}{2} & \text{if } b(8 \times n + i) = 1, \end{cases}$$

END
For i=0 to7 Do

$$d_i' = f\left(\sum_{i=0}^{7} w_{ji} \times d_i + \theta_i\right)$$

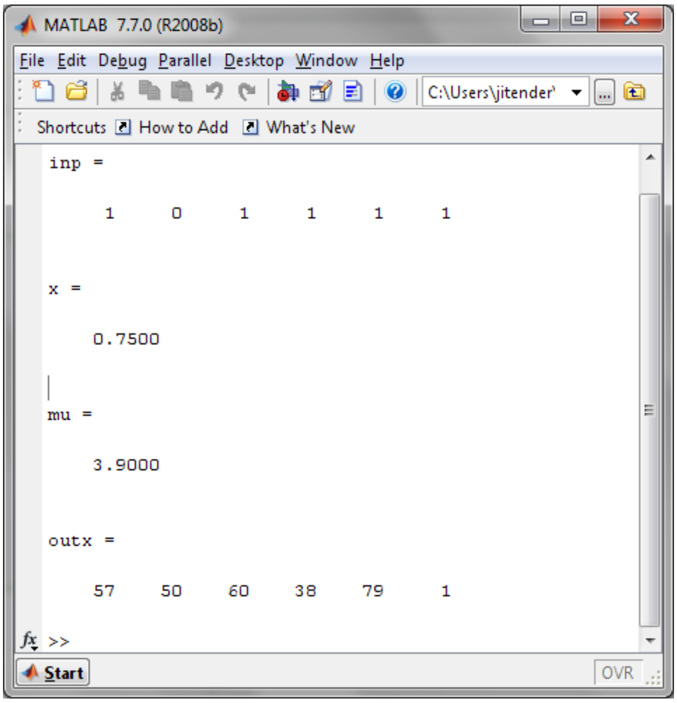
Where f(x) is 1 if x2 0 and 0 otherwise
END

$$Let\ \ g(n) = \sum_{i=0}^{7} d_i \times 2^i$$

END

Step 5: The encrypted signal g’ is obtained and the algorithm is terminated.

3.5.3 Result for Encryption using Chaotic Neural Network:

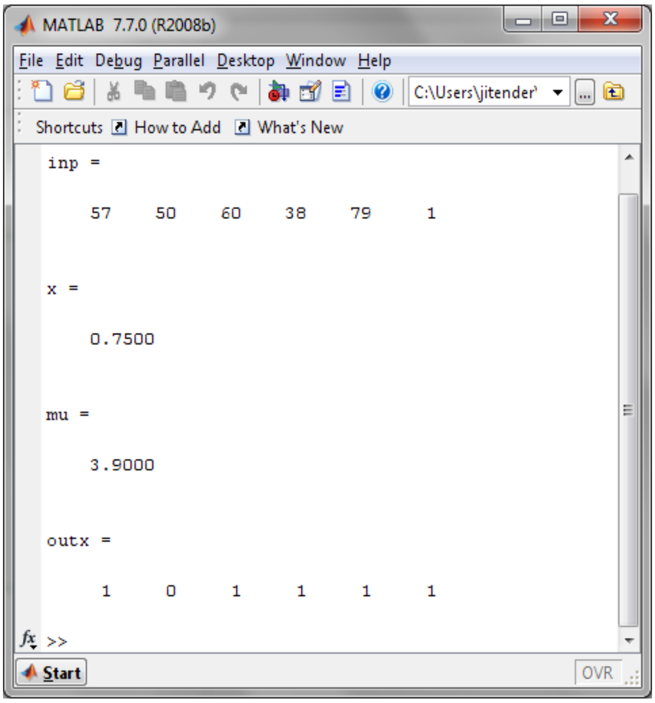

MATLAB 7.7.0 (R2008b)
File Edit Debug Parallel Desktop Window Help
C:\Users\jitender'
Shortcuts How to Add What's New
Start
OVR

```
inp =

     1     0     1     1     1     1


x =

    0.7500


mu =

    3.9000


outx =

    57    50    60    38    79     1

>>
```

3.5.4 Decryption process in Chaotic Neural Network:

The decryption procedure is the same as the above one except that the input signal to the decryption CNN should be g’(n) and its output signal should be g”(n).

3.5.5 Result for decryption using Chaotic Neural network:


MATLAB 7.7.0 (R2008b)
File Edit Debug Parallel Desktop Window Help
C:\Users\jitender'
Shortcuts How to Add What's New
Start
OVR

```
inp =

    57    50    60    38    79     1


x =

    0.7500


mu =

    3.9000


outx =

     1     0     1     1     1     1

>>
```

IV. Conclusion

Numbers of attacks on the electronic data are increasing day by day. But on the other side cryptography technique is also improving. By using cryptography the probability of stealing information becomes down. So, cryptography plays major role in information securing. But using neural network in cryptography plays also an important role. So, our future work involves the implementation of cryptography using neural networks.

REFERENCES

[1] M. E. Smid and D. K. Branstad, “The Data Encryption Standard: Past and Future,” Proceedings of The IEEE, vol. 76, no. 5, pp. 550-559, 1988.

[2] "An Introduction to Neural network" by Ben Krose and Patrick van der Smagt Eighth editionNovember 1996.

[3] http://www.wikipedia.org

[4] "Artificial Intelligence A Modern Approach" by Stuart J. Russell and Peter Norvig.

[5] “Design and Realization of A New Chaotic Neural Encryption/Decryption Network” by Scott Su, Alvin Lin, and Jui-Cheng Yen.

[6] http://www.wikipedia.org

[7] C. J. Kuo and M. S. Chen, “A New Signal Encryption Technique and Its Attack Study,” IEEE International Conference on Security Technology, Taipei, Taiwan