

Approaches in RSA Cryptosystem Using Artificial Neural Network

Megha Sharma¹ Pankaj Rathi²

¹Research Scholar ²Assistant Professor

^{1,2}Department of (Digital Communication) Electronics and Communication

^{1,2}SITE, Nathdwara, India

Abstract— Cryptography is a technique to make information unreadable for unauthorized users. Today, building a secure channel is one of the most challenging areas for research in communication systems. Many forms of public key cryptography are available, but it requires more complex techniques and needs more computational power. Artificial Neural Network (ANN) and cryptography together can make a great help in field of networks security. Neural networks' most important property is their generalization capability. This ability ensures they produce reasonable results when they are fed with inputs not previously encountered. This makes them extremely useful for many applications. The other important property of ANNs is parallel implementation. Each layer is paralleled, so they can independently implement certain functionality. A special property of neural networks is confusion, which is caused by the non-linear structure of networks. The output, therefore, depends on the input in non-linear and complicated cases. Thus, it is not easy to define the exact input. As a result of this confusion property, ANNs could be preferable used for cipher design.

Keywords: RSA Cryptosystem, Artificial Neural Network (ANN)

I. INTRODUCTION

"Network security" refers to any activity designed to guard availability or honesty of the network and data. It targets various threats or prevents them from entering or spreading to our network. It covers various computer networks used in daily work, including public or private; transactions and communication among companies, public authorities and individuals. The network can be private, e.g. within a company, or it may be another network that is open to public access. The most general or easiest way to guard network resources is to assign an exclusive name or password. [2] Network security problems can be separated generally into four closely entangled areas:

- **Secrecy:** Only sender or proposed recipient should be able to appreciate content of sent message. Because the interceptor can interrupt message, this necessarily requires some degree of encryption of the message so that the intercept message cannot be decrypted by the interceptor.
- **Authentication:** Both the sender and the recipient must verify individuality of the other party participating in communiqué to confirm that other party is in fact the identity or identity they claim.
- **Message integrity:** Although the sender and receiver can verify each other, they hope that their communication

content does not change harmful or accidentally during transmission.

- **Non-Rejection:** refers to capability to guarantee that a party to a indenture or statement cannot refute dependability of its cross on a article or ability to send information it sends.

II. BIOLOGICAL MODEL

The human nervous structure can be wrecked down into 3 theatre that may be symbolize as follows:



Fig 1: Block Diagram of a Human Nervous System.

The receptor collects information from atmosphere. The effector interacts with situation, for example. Activate strength. The flow of information / activation is indicated by arrows. There is an intertwined organizational hierarchy:

- 1) Molecules and ions
- 2) Synapse
- 3) Neuron microcircuits
- 4) Dendritic wood
- 5) Neurons
- 6) Local circuit
- 7) Interzone circuits
- 8) Central nervous system

It is emitted from cell body or provides a receptor region that receives activation of other neurons. Axons are fibers that act as broadcast lines and can send opening signals to other neurons. The nodes that permit signal programme among axons or dendrites are called synapses. [twenty-one]

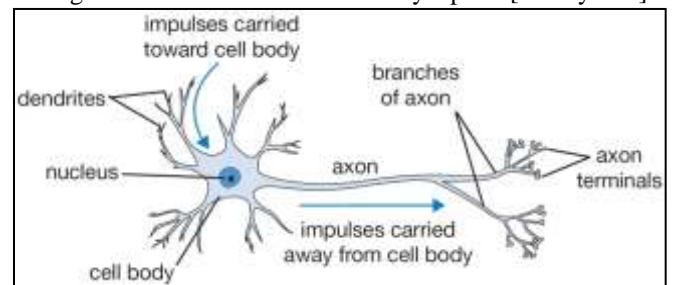


Fig. 2: Schematic diagram of a Biological Neuron

The image below will optimistically make this development clearer. In figure, left half or right half are represent as L0 and R0, respectively, and are denoted as L1, R1, L2, R2, etc. In subsequent rounds. The occupation f is accountable for all the above connections.

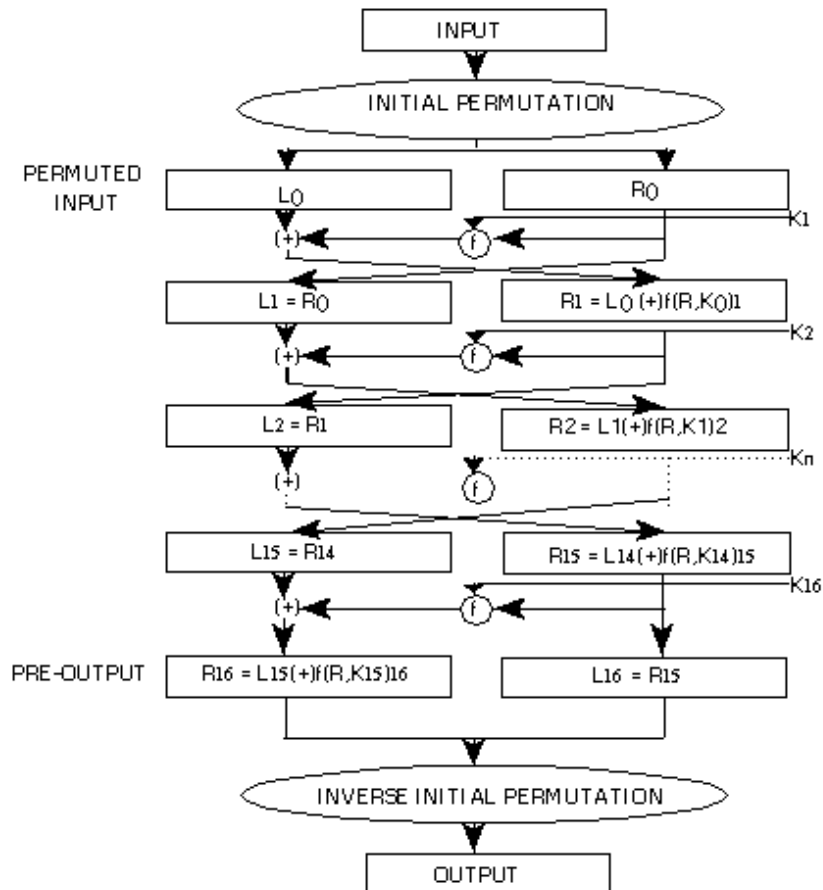


Fig. 3: DES working rounds.

III. NEURAL CRYPTOGRAPHY

Cryptography is practice or research of thrashing information throughout procedure support on chance. Therefore, artificial neural networks in neural cryptography must be a form of random topology. The network arrangement modify aimlessly. The network's training or delivery function is also randomly certain. Figure 4.3 depicts an ANN with a random topology. contribution is plain text, the encryption algorithm is used to encrypt it by NN, and output from NN is encryption text. The transfer function or training algorithm are also certain according to NN-based pseudo-random integer generator. [40]

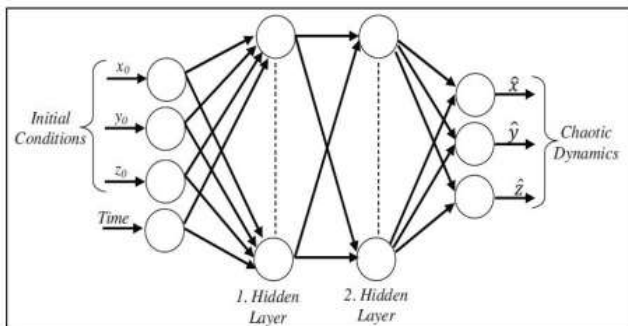


Fig. 4: Block Diagram of Trained ANN Model

IV. RESULT

Graph of Performance, Regression and Training State for both Encryption and Decryption technique is been shown in the figures below.

- Performance (plotperform): It plots graph between error vs epoch for the training, validation, and test performance of the training record. The plot performance chart shows the best verification performance in a given period. Training stops when the mean square error (MSE) of the validation test begins to increase.
- Training mode (plottrainstate): The graph of plottrainstate shows the state of the system after training according to the default values for various input parameters.
- Regression (plot regression): The plot regression diagram shows the curves between 0-output data and training examples, between output data and verification examples and between output data and test examples (R-value shows the relationship between output and target value.

A. Plottrainstate

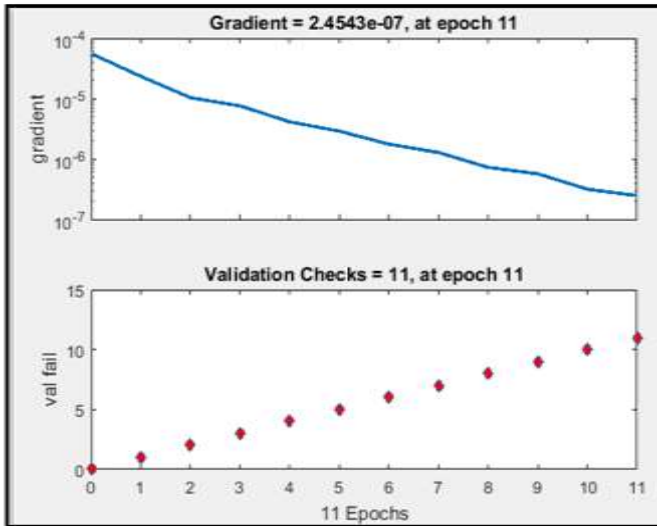


Fig. 5 : Training State Plot for Encryption

B. Plotregression

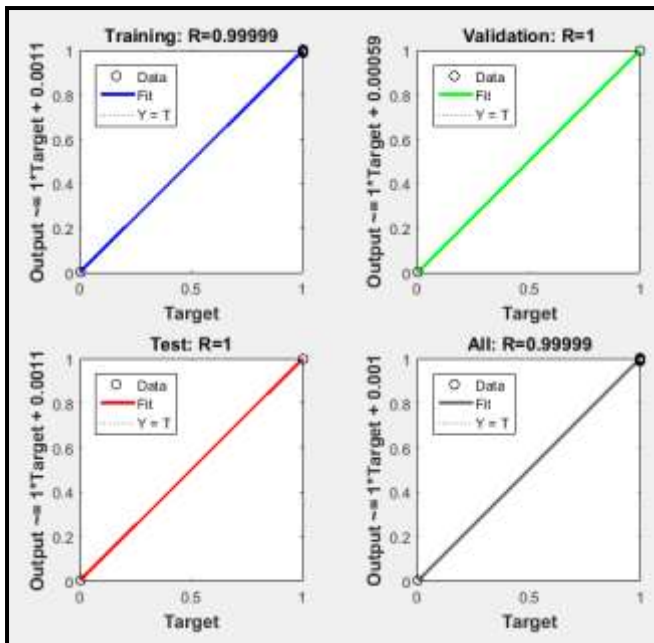


Fig. 6 : Regression Plot for Encryption

The tabel 1 shows the comparison between the system made using a neural network and without using a neural network on different issues.

S.No.	Different Issues	With NN	Without NN
1	Synchronization Time	Required	Not Required
2	Randomness	More	No
3	Security	More	Less

Table 1: Comparison based on different issues

V. CONCLUSION

We have tested behaviour of neural network for the encryption and decryption process. The proposed neural network has been experienced for different statistics of education iteration or for changed number of hidden neurons and input data. The reproduction result has shown a very good

consequence, with comparatively better presentation than conventional encryption technique.

The algorithm used for training neural network was Scaled Conjugate Gradient. The reason behind using this algorithm over other training algorithm was that firstly, it gives better result when used for larger data sets. Secondly, it avoids the time consuming line search which is performed in other algorithms and thirdly, this algorithm unite model-trust region advance (used in Levenberg-Marquardt algorithm) with conjugate gradient advance.

REFERENCES

- [1] M.Bishop. (19 February, 2003). "What is Computer Security". IEEE Security and Privacy (pp. 67-69). IEEE.
- [2] M.Guizani. (23 January, 2006). "Computer and Network Security". Global Telecommunication Conference. St. Louis, MO, USA: IEEE.
- [3] A.Eskicioglu, & L.Litwin. (February, 2001). "Cryptography". IEEE Potentials. 20, pp. 36-38. IEEE.
- [4] N.Ferguson, & B.Schneier, T. (2010). In "Cryptography Engineering: Design Principles and Practical Applications". Wiley Publishing.
- [5] Kumar, P., & Sharma, P. (2014). "Artificial Neural Network - A Study". International Journal of Emerging Engineering Research and Technology (IJEERT) , 2 (2), 143-148.
- [6] Kinzel, W., & Kanter, I. (05 June, 2003). "Neural Cryptography". IEEE, (pp. 1-4). Singapore.
- [7] R.Mislovaty, E.Klein, I.Kanter, & W.Kinzel. (2004). Security of Neural Cryptography. IEEE, (p. 3).
- [8] T.Godhavari, Alamelu, N., & Soundararajan, R. (2005). Cryptography Using Neural Network. IEEE, (p. 4).
- [9] E.C.Laskari, G.C.Meletioui, D.K.Tasoulis, & M.N.Vrahatis. (5 December, 2005). "Studying the Performance of Artificial Neural Network on Problems Related to Cryptography". Nonlinear Analysis: Real World Application. Elsevier.
- [10] T.Schmidt; H.Rahnama; A.Sadeghian (09 December, 2008). "A Review of Applications of Artificial Neural Network in Cryptosystem". Automation Congress. WAC 2008. World. Hawaii, USA: IEEE
- [11] Yu, H., & M.Wilamowski, B. "Levenberg-Marquardt Training".
- [12] A.Forouzan. (2007). "Cryptography and Network Security". USA: McGraw-Hill.
- [13] S.R.Subramanya. (05 July 2006). "Digital Signature". IEEE Potentials (pp. pages 5-8). IEEE.
- [14] Sheshasaayee, A. (13 July 2017). "Digital Signatures Security Using Cryptography for Industrial Application". Innovative Mechanisms for Industry Applications. Banglore, India: IEEE.
- [15] Digital Signature. (n.d.). Retrieved from Search Security: <http://searchsecurity.techtarget.com/>
- [16] Volna, E., Kotyrba, M., Kocian, V., & Janosek, M. "Cryptography Based on Neural Networks". 26th European Conference on Modelling and Simulation.