A Compound Algorithm Using Neural and AES for Encryption and Compare it with RSA and existing AES

Seema Rani
Department of Computer Science and Engineering, S.P.G.O.I., Rohtak, India.

Dr Harish Mittal
Director, S.P.G.O.I., Rohtak, India.

Abstract – In this paper we introduce a improved AES Algorithm which is a combination of AES and neural net. We trained our algorithm with plaintext text and cipher text produced by AES algorithm and test our algorithm for validation and verification either it produces same kind of cipher text pattern or not. In order to modify the performance of AES, AES is trained with the help neural network tool. In order to enhance the performance, we use the various algorithms: these are Data Division, Training, Performance and Derivative. In order to calculate performance, we use Mean Squared Error method. The Performance Plots are used to represent measures of all algorithms. All these Plots provide us information about training state, regression, Error Histogram and performance measures. The overall work provides us the improved performance over AES in order to increase security.

Index Terms – Plain text, cipher text, Cryptography, AES, RSA and Neural net.

1. INTRODUCTION

Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called Decryption

What is cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across in secure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical crypt analysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

1.1. RSA

In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir andLeonardAdleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.

1.1.1. Operation

The RSA algorithm involves three steps: key generation, encryption and decryption.

key Generation:

RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way: Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test. Compute $n = p*q$. n is used as the modulus for both the public and private keys. Its key length, usually expressed in bits. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q -1)$, where φ is Euler's totient function. Choose an integer e such that $1 < e <\varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime. e is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. Determine d as $d \equiv e^{-1} (\bmod \varphi\ (n))$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$$d$ is kept as the private key exponent. The *public key* consists of the modulus *n* and the public (or encryption) exponent *e*. The *private key* consists of the modulus *n* and the private (or decryption) exponent *d*, which must be kept secret. *p*, *q*, and φ(*n*) must also be kept secret because they can be used to calculate *d*.

Encryption:

Alice transmits her public key *(n, e)* to Bob and keeps the private key secret. Bob then wishes to send message *M* to Alice. He first turns *M* into an integer *m*, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text corresponding to C=~M^E(MOD N)This can be done quickly using the method of exponentiation by squaring. Bob then transmits *c* to Alice. Note that at least nine values of *m* will yield a cipher text *c* equal to *m*,[note 1] but this is very unlikely to occur in practice.

Decryption: Alice can recover *m* from *c* by using her private key exponent *d* via computing M=~C^E(MOD N)Given *m*, she can recover the original message *M* by reversing the padding scheme.

1.2. AES

The Advanced Encryption Standard (AES) is formal encryption method adopted by the National Institute of Standards and Technology of the US Government, and is accepted worldwide. In 1997 the National Institute of Standards and Technology (NIST), a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES).

The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption. AES is based on the principle Known as Substitution-permutation.

A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term “rounds” refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key.

1.2.1. Encryption Keys

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm.

The key size used for AES cipher specifies the Numbers of repetitions of transformation rounds:

10 cycles of repetition for 128-bit keys

12 cycles of repetition for 192-bit keys

14 cycles of repetition for 256-bit keys

Rounds

1.) Initial Round: Add Round key - each byte of the state is combined with a block of the round key using bitwise xor.

*2.) Rounds: (*a) Sub Bytes – a nonlinear substitution step where each byte is replaced with another acc to a lookup table

(b) Shift Rows – a transposition step where the last three rows of the state are shifted cyclically a certain no of steps

(c) Mix Columns- a mixing operation which operates on the columns of the state, combining the four bytes in each column,

(d) Add Round key

3.) Final Round (a) Sub Bytes – a nonlinear substitution step where each byte is replaced with another acc to a lookup table

(b) Shift Rows – a transposition step where the last three rows of the state are shifted cyclically a certain no of steps

(c) Add Round key

2. NEURAL NET

The basic unit in a neural network is a *neuron* or *unit*. Each unit receives a set of inputs, which are denoted by the vector *Xi*, which in this case, correspond to the term frequencies in the i^th document. Each neuron is also associated with a set of weights *A*, which are used in order to compute a function $f(\cdot)$ of its inputs. A typical function which is often used in the neural network is the linear function as follows:

$Pi = A \cdot Xi$ (6.14)

Thus, for a vector *Xi* drawn from a lexicon of *d* words, the weight vector *A* should also contain *d* elements. The magnitude of the update is regulated by a learning rate μ. In general there are so many factors that can affect artificial neural networks forecasting ability.

These factors are:

1. Number of input neurons
2. Training period
3. Learning Rate
4. Momentum Learning
5. Number of input neurons

This layer has as many neurons as there are input categories. The number of input variables is important parameter that affects neural network forecasting capability. The number of input neurons is one of the easiest parameter to select once the independent variables have been preprocessing because each independent variable is represented by its own input neurons. If an inadequate number of neurons are used, the network will be unable to model complex data, and the resulting fit will be poor.

If too many neurons are used, the training time may become excessively long, and, worse, the network may over fit the data. When over fitting occurs, the network will begin to model random noise in the data. The result is that the model fits the training data extremely well, but it generalizes poorly to new, unseen data. Validation must be used to test for this.

3. RELATED WORK

Lot of research work has already been done in this field to improvise security in the data while the transfer. Some of the reviews are as follows

- Vishwagupta ,GajendraSingh ,Ravindra Gupta [1] performed a work, “Advance cryptography algorithm for improving data security”.
- Mohammed AbuTaha, MousaFarajallah, RadwanTahboub, Mohammad Odeh [2] performed a work,” Survey Paper: Cryptography Is The Science Of Information Security”.
- Thai Duong, Juliano Rizzo[3] performed a work,” Cryptography in theWeb: The Case of Cryptographic Design Flaws in ASP.NET”.
- Sonalsharma, jitendrasinghyadav, parshantsharma [4] performed a work,” Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm” .
- B.Persis Urbana Ivy, PurshotamMandiwa.Mukesh Kumar [5] performed a work,” A modified RSA cryptosystem based on ‘n’ prime numbers”.
- Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou,NadiaHeninger, Tanja Lang, and Nicko van Someren [6] performed a work ,” Factoring RSA keys from certified smart cards:Coppersmith in the wild”.
- M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop[7] performed a work ,” Cryptography: A New Approach of Classical Hill Cipher”.
- RajinderKaur, Er.Kanwalprit Singh [8] performed a work,” Image Encryption Techniques: A Selected Review”.

4. PORPOSED MODELLING

In my dissertation work we used MATLAB platform for implementation of my proposed work that provide a good programming environment. The dataset which we have taken also describe there on that dataset we implement our algorithm. Our compound Algorithm contains AES and Neural Net serially. Firstly we have plaintext that we need to encrypted .we encrypt the plain text using AES and provide the plaintext and cipher text resulting from AES to neural net for learning process so that in future whenever we have same plaintext, neural net generate same pattern of cipher text and save time for encryption .This result in a better algorithm when compare to existing Algorithms like RSA and AES.

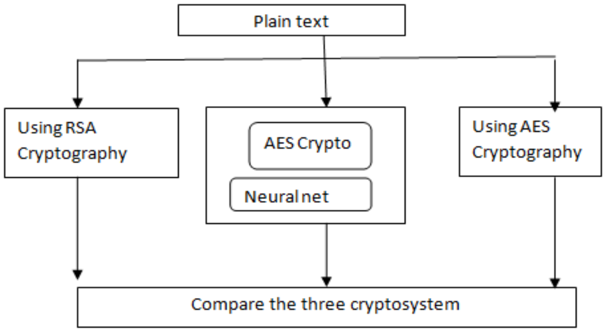
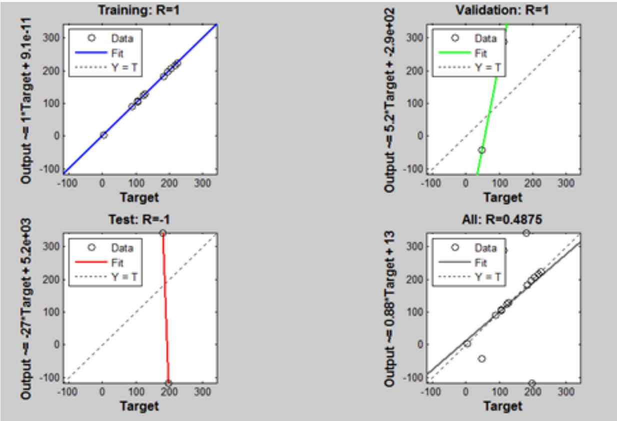


Fig: block diagram of my dissertation work.

5. RESULTS AND DISCUSSIONS



.

Fig1: - The figure shows Training of neural net.

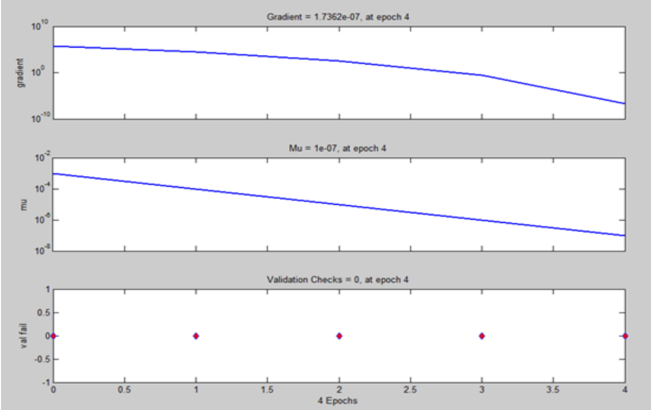


Fig2:-The figure shows the performances of above training of neural net.

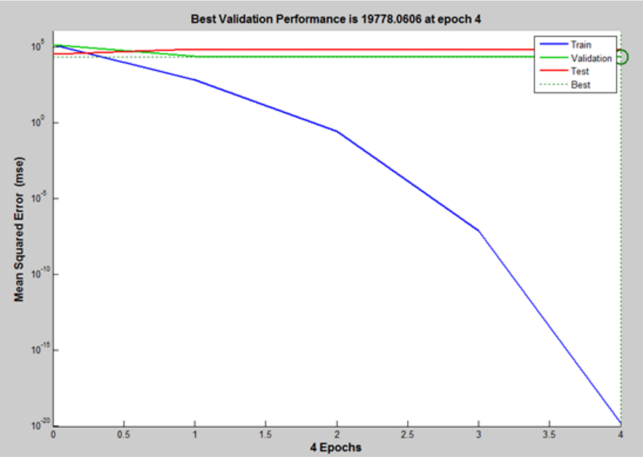


Fig3:-The figure shows the best validate performance of training of neural net at epoch 4.

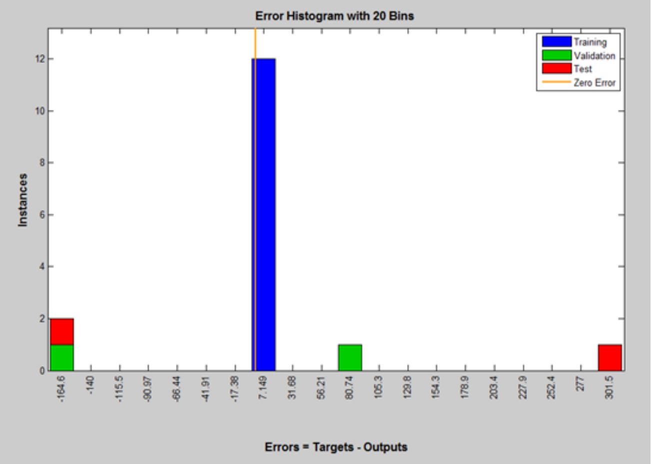


Fig3:-The figure shows the error histogram with 20 bins.

6. CONCLUSION

With the implementation the modified AES with neural, a conclusion is achieved that for better security of any text or image we can apply any two techniques one by one on each other that make it more secure like neural with AES. For an illusion designing of this work we chose a text and apply RSA algorithm on it with encryption key. We got some encrypted text and after that apply the AES algorithm on the text and further modified AES also implemented then got an encrypted text that is very difficult to any other person to decrypt it. This is achievement in our conclusion that makes a text more secure.

REFERENCES

[1] Ron Rivest , Adi Shamir and Leonard Adleman , who first publicly described the algorithm in 1977.

[2] Advanced Encryption Standard (AES) is formal encryption method adopted by the National Institute of Standards and Technology of the US Government, in 1997

[3] Vishwagupta , Gajendra Singh , Ravindra Gupta , "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[4] Sonalsharma, jitendrasinghyadav, parshant sharma," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012 ISSN: 2277 128X.

[5] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar," A modified RSA cryptosystem based on 'n' prime numbers", International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66.

[6] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lang, and Nicko van Someren," Factoring RSA keys from certified smart cards: Coppersmith in the wild", Permanent ID of this document:278505a8b16015f4fd8acae818080edd.Date: 013.09.16.

[7] CRYPTOGRAPHY,https://en//.wikipedia.org/wiki/cryptography.

Authors

Seema Rani (M.Tech/CSE/2013-15 in S.P.G.O.I., Rohtak)

Dr Harish Mittal(director of the S.P.G.O.I., Rohtak)