Implementation of AES and RSA Using Chaos System

Bhavana Agrawal, Himani Agrawal

ASSISTANT PROFESSOR, ET&T, K.I.T.E, Raipur, C.G

ASSOCIATE PROFESSOR, ET&T, SSCET, BHILAI, C.G

ABSTRACT: In this paper we propose two cryptographic algorithm AES and RSA Using Chaos. Chaos has attracted much attention in the field of cryptography. It describes a system which is sensitive to initial condition. It generates apparently random behavior but at the same time is completely deterministic Chaos function is used to increase the complexity and Security of the System.AES and RSA are the two cryptographic algorithms. In AES we apply the Chaos on S-box where as in RSA we mix the plaintext with Chaos sequence First then apply for encryption and decryption. After Implementing AES and RSA we compare both the technique on the basis of speed.

***Keywords*: AES, RSA, Chaos, Logistic mapping, Encryption, Decryption, Cryptography**

1. INTRODUCTION

Data security is going to have an increased importance; therefore, security category includes several common algorithms. [1] Chaos functions have mainly used to develop mathematical models of non linear systems. They have attracted the attention of many mathematicians owing to their extremely sensitive nature to initial conditions and their immense applicability to problems of daily life. Chaotic maps can be used to generate random looking data to be used for aiding cryptography, being completely deterministic means that we can always obtain the same set of values provided we have exactly the same mapping function and initial value. Since chaotic functions are sensitive to initial conditions, any slight difference in the initial value used will mean that the cipher-text produced using chaos will be drastically different. This means that the system will be 'strong' against brute force attacks. These properties of chaos have much potential for applications in cryptography as it is hard to make long term predictions on chaotic systems [2].

AES has a computationally intensive and parallel structure, thus giving implementers a lot of flexibility and does not allow effective cryptanalytic attacks. This work is devoted to generating a new S-box instead of the random sequence generated from the affine transformation of its multiplicative inverse. The generated chaotic S box distribution is noisy, and is sensitive to initial condition and spreading out of trajectories over the whole interval

Ron Rivest, Adi Shamir, and Leonard Adleman. RSA gets its security from the difficulty of factoring large numbers. The public and private keys are functions of a pair of large (100 to 200 digits or larger) prime numbers. Recovering the plaintext from the public key and the cipher-text is conjectured to be equivalent to factoring the product of the two primes.[3]

2. ALGORITHM PRINCIPLES

2.1. AES, Advanced Encryption Standard:

AES has key size of 128 bits and a substitution-linear transformation network with 10 rounds. A data block to be encrypted by AES is split into an array of bytes, and each encryption operation is byte oriented. AES's round function consists of four layers. In the first layer, an 8x8 S-box is applied to each byte. The second and third layers are linear mixing layers in which the rows of the array are shifted, and the columns are mixed. In the fourth layer, sub key bytes are XORed into each byte of the array. In the last round, the column mixing is omitted. So, the algorithm consists of four main steps: a substitution step, a shift row step, a mix column step and a sub key addition step. The substitution step consists of S-boxes. The shift row step consists of cyclic-shifting of the bytes within the rows. The key addition is a straight forward XOR

operation between the data and the key.[4] row step consists of cyclic-shifting of the bytes within the rows. The key addition is a straight forward XOR operation between the data and the key.[4]

1) Byte Substitution:

In the Sub bytes step shown in Fig. 1,each byte in the array is updated using an 8-bit substitution S-box, the chaotic S-box. This operation provides the nonlinearity in the cipher. The S-box used is derived from chaotic map in GF (28) [3]and [4], known to have a good nonlinearity properties. The S-box is also chosen to avoid any fixed points along with any opposite fixed points. The new chaotic S-box depends on a chaotic map which is a dynamically discrete-time continuous value equation which describes the relation between present state and the next state of chaotic system [5]. In this study one dimensional chaotic map is considered. The logistic map is a typical one dimensional chaotic map which will be used. The logistic map is defined as in

$$W_{i+1} = \mu W_i (1 - W_i) \text{ ----------(1)}$$

Where $0<W_i<1$ and $0<\mu<4$

and $i = 0,1,2,3,\ldots\ldots,n$

W_{i+1} is the chaotic sequence and μ is the bifurcation parameter. When μ increases to values near 4, the logistic map enters the chaotic state and the sequence that iteration produces is chaotic.

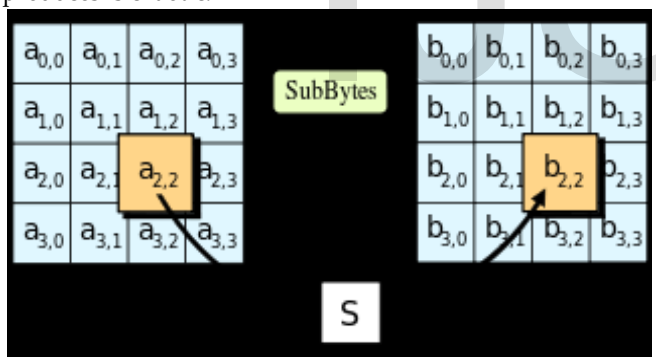


Fig.1 Chaotic S-box Byte substitution

2) The Shift Rows:

This step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset as shown in Fig. 2. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three, respectively. For the block of size 128 bits, the shifting pattern is the same. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state.

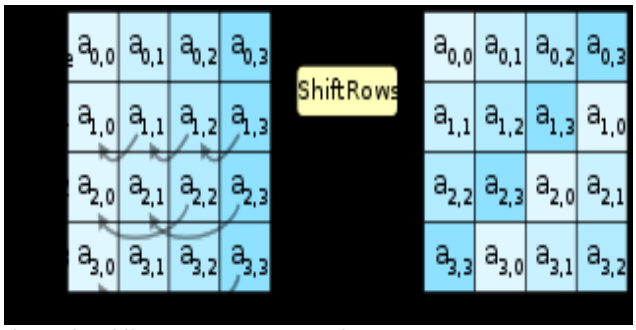


Fig. 2 The shift row step representation

3) The Mix Column

In this step, the Mix Columns step, the four bytes of each column of the State are combined using an invertible linear transformation as shown in Fig. 3. The Mix Columns function takes four bytes as input and output, where each input byte affects all four output bytes. Together with Shift Rows, Mix Columns provides diffusion in the cipher.

During this operation, each column is multiplied by the known matrix that for the 128-bit key is:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

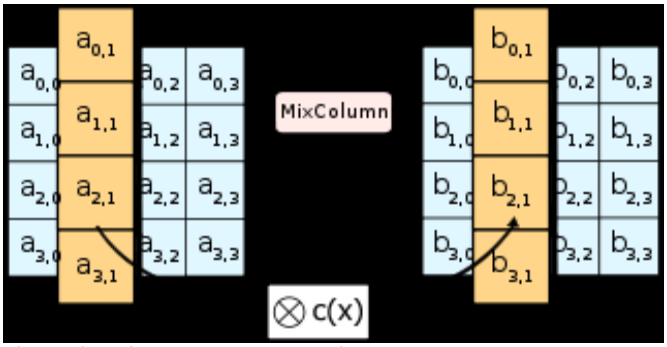


Fig. 3 Mix Column Step representation

4) Add Round Key:

In this step, the sub key is combined with the State. For each round, a sub key is derived from the main key using Rijndael's key schedule where each sub key has the same size as the State. The sub key is added by combining each

byte of the State with the corresponding byte of the sub key using bitwise XOR. This process is indicated in Fig. 4.

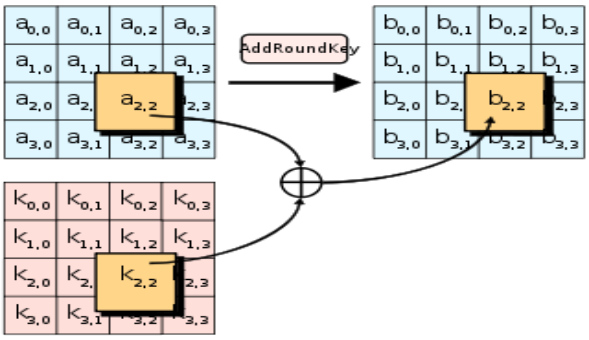


Fig. 4 Add round key Step representation

2.2 The RSA Algorithm:

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public key Cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization.The RSA algorithm involves three steps: key generation, encryption and decryption

1) Key generation:

RSA involves a public key and a private key**.** The public key can be known to 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:

To generate the two keys, choose two random large prime numbers *p* and *q*. For maximum security, choose *p* and *q* of equal length. Compute the product

K=P * Q

Then randomly choose the encryption key *e* such that *e* and (*p* −1) (*q* −1) are relatively prime. Finally, use the extended Euclidean algorithm to compute the decryption key *d* such that

d= e^{-1} mod ((p-1) * (q-1))

Note that *d* and *n* are also relatively prime. The numbers *e* and *K* are the public key; the number *d* is the private key. The two primes *p* and *q* are no longer needed. They should be discarded, but never revealed [4].

2) Encryption:

Firstly receiver transmits her public key (n, e) to sender and keeps the private key secret. If sender wishes to send message M to receiver.

Sender change the message M in to integer m, such that $0 \le m < n$. Then sender computes the cipher text *c* corresponding to

$C \equiv m^e \pmod n$

3) Decryption:

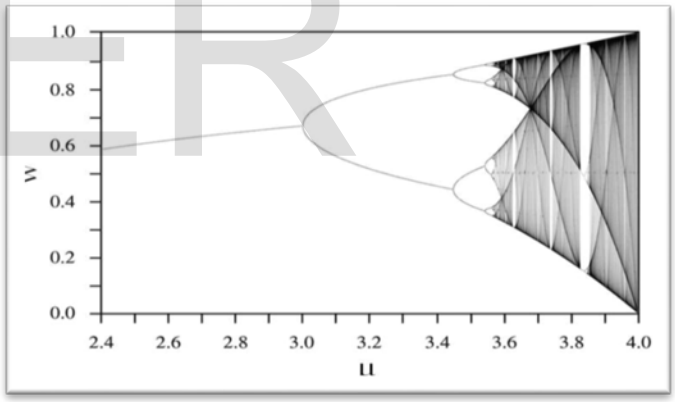
Receiver can recover *m* from *c* by using her private key exponent *d* via computing

$M \equiv c^d \pmod n$

3. RESULTS

The Chaos AES is simulated under MATLAB program environment. The S-box used is derived from the logistic maps. The bifurcation parameter is chosen to be μ = 4, which ensures that the logistic map enters chaotic state sequence as shown in Fig. 5.

Fig. 5 Bifurcation Diagram[1]



There are two reasons to choose a chaotic sequence instead of a random sequence generated by the affine transformation of its multiplicative inverse. Firstly, chaotic sequence is determined by the initial conditions and the chaotic map. Secondly, due to the good features including ergodic, confusion and deterministic properties, Chaos based S-box provides promising methods to show a good

performance. The comparison of AES and RSA is shown in table.

It is observed that RSA WITH CHAOS i.e .16 sec will take less time to execute as compare to RSA i.e.12. So RSA with Chaos is more Faster and secured as compared to RSA. Similarly AES WITH CHAOS i.e .16 sec will take less time to execute as compare to AES i.e.12. So on applying Chaos speed of the system increases

Simulation Time of AES and RSA

S.no	ALGORITHM	General	Chaos
1	AES	2.92	2.90
2	RSA	0.16	0.12

The result of AES is shown IN Fig-6. Firstly we enter the plain text in the main window then we press "Process for Cryptography ". It will show the Encryption and decryption of AES and AES with Chaos. It will also show the execution time of Both Encryption and Decryption. We can see from figure that AES with Chaos will take less time to execute as compare to AES. So after applying Chaos System performance increases

Fig-6 GUI version of AES and AES with Chaos

The result of RSA is shown in Fig-7. Firstly we enter the plain text in the main window then we press "Process for Cryptography ". It will show the Encryption and decryption of RSA and RSA with Chaos. It will also show the execution time of Both Encryption and Decryption. Here also we can see from figure that RSA with Chaos will take less time to execute as compare to RSA. So after applying Chaos System performance increases

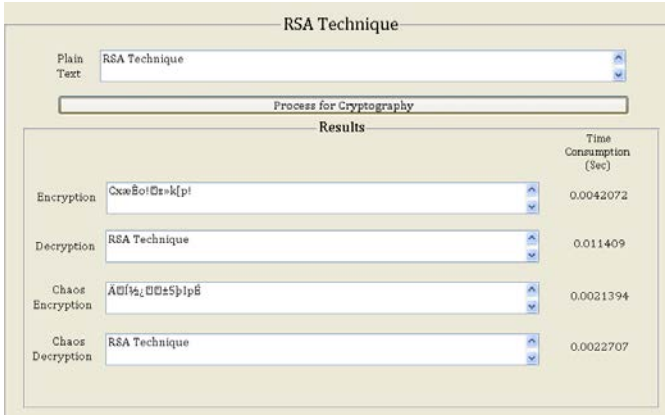


Fig-7 GUI version of RSA and RSA with Chaos

4. Conclusion

In this paper we used the Chaos system at AES and RSA This encrypted signal can withstand many of the different attacks including the brute force attack. The characteristics of the chaotic maps have attracted the attention of cryptographers since it has many fundamental properties such as ergodicity , sensitivity to initial condition and system parameter and mixing property,…. etc [6],[7], and [8]. This gives the algorithm the ability to be used as another key for more security and confidentiality. The results of the proposed chaos based AES and RSA gives a significant improvement for the accepted sequences probability over a wide range of chaos initial conditions. Chaos based AES and RSA makes the system more complex and fast as compare to the Conventional AES and RSA.

References

[1]. El-Sayed Abdoul-Moaty ElBadawy et al.(2010),"A New Chaos Advanced Encryption Standard(AES) Algorithm for Data Security",ICSES 2010-The International Conference on Signals and Electronic Systems,Gliwice,Poland,

[2]." Chaos and Cryptography: *Applications and Analysis "Project Submitted Towards thePartial Fulfilment of USC 3001 Complexity*. Lecturer: Dr Rajesh R. Parwani,

[3]. Dalia H. Elkamshoushy, A.Khairy Aboulsoud(2008) "Cryptographic Scheme Using Chaotic System"25th NATIONAL

RADIO SCIENCE CONFERENCE (NRSC 2008), March 18-20, 2008, Faculty of Engineering, Tanta Univ., Egypt
[4]. William Stalling ," Cryptography and Network Security : Principles and Practice," ,3rd Edition , Prentice Hall , 2003.
[5]. The Mathworks: Galois Field Computations. ttp://www.mathworks-.com/Access/help-desk/help /toolbox/comm./tutor3.shtml, Communications Toolbox, 2001.
[6]. J. Fridrich, " *Image Encryption Based on Chaotic Maps* " , In Proc. IEEE INT.Conference on systems, Man and Cybernetics (ICSMC'97) , vol.2 ,pp.1105-1110,1997.
[7]. F.Belkhouche and U.Qidwai , " *Binary Image Transformation Using Two-Dimensional Chaotic Maps* " , Proc. of the 17th International Conference on Pattern Recognition, (ICPR 2004).
[8]. G. Alvarez and S. Li, " *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems* " . Available online at http ://www .hooklee.com/pub.html

---

- *Bhavana Agrawal(persuing M.tech) in Communication in C.S.V.T.U, RAIPUR, C.G, INDIA,PH-99261-48600. E-mail:bagrawal3@gmail.com*
- *Himani Agrawal, M.tech in communication from C.S.V.T.U,RAIPUR,C.G,INDIA, PH-98274-05681 E-mail: himaniagrawaljka @gmail.com*