International Journal of scientific research and management (IJSRM)
||Volume||3||Issue||11||Pages|| 3762-3769||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Chaotic Based Asymmetric and Symmetric Key Encryption Using Augmented Lorenz Equations

Winnie Sara Simon[1], Josy Elsa Varghese[2]
[1] Pursuing M.Tech, Dept. of Computer Science and Engineering,Caarmel Engineering College, MG University, Kerala
E-mail:winniesara@gmail.com
[2] Assistant professor, Dept. of Computer Science and Engineering,Caarmel Engineering College, MG University, Kerala
E-mail:josy.varghese@bccaarmel.ac.in

Abstract:
In the proposed paper, a comparison on the asymmetric key cryptographic system and the symmetric key cryptographic system over augmented Lorenz equations is conducted. In asymmetric secret key system, at both sender side and the receiver side, the corresponding private key, public key and the secret key are generated. The chaotic signal for encryption and decryption are generated at the sender and the receiver from augmented Lorenz equations using the corresponding secret keys which are generated at the sender and the receiver. The cipher text is therefore generated by applying XOR function between the chaotic signal and the plain text. The plain text can be extracted from the received cipher text by again applying XOR function between the chaotic signal and the cipher text. In symmetric secret key system, a shared secret key is generated for the sender and the receiver using the QKD protocol. The shared secret key is used for generating chaotic signal from augmented Lorenz equations at both sender side and the receiver side. The chaotic signal is then masked with the plain text to obtain the cipher text. Consequently at the receiver side, the regenerated chaotic signal is unmasked from cipher text to obtain the plain text.

Keywords: Augmented Lorenz Equations, Quantum Key Distribution (QKD) protocol, Chaotic Cryptography

INTRODUCTION

Chaotic Cryptography is one of the interesting applications of chaos to engineering. It makes use of chaos theory, which studies the behavior of dynamical systems to perform different cryptographic tasks in a cryptographic system. In chaotic cryptography, encryption is done by superimposing a chaotic signal generated through different techniques on to a plain text. During decryption, the chaotic signal is unmasked from the cipher text to obtain plain text. The complex behavior of chaotic dynamical systems is used to hide or mask information in chaotic cryptosystems.

In chaos based message encryption, the bifurcation parameters (the chaotic system parameters) or the initial conditions of chaotic dynamics are used as secret keys that are shared between sender and receiver. The Prandtl number σ, reduced Rayleigh number R_0 and geometrical parameter φ are known as the bifurcation parameters. The number of possible combinations of bifurcation parameters and initial conditions of the chaotic system determine the size of the key space. However, the size of the key space is not significantly large and a slight difference in secret key would not have much impact on the dynamic behavior of the signal. This makes it easy for an adversary to guess the secret key from the reduced key space using Brute Force attack and then eventually break the secret key. The traditional public-key cryptography has key size limitation and the keys are vulnerable to brute force attack. Also the traditional public-key cryptosystems based on chaotic systems perform encryption / decrypti on processdepending on addition/subtraction operations

DOI: 10.18535/ijsrm/v3i11.18

that leads to limitation on the length of the message and weakness in encryption.

In the symmetric secret key cryptographic system, the bifurcation parameters σ, R_0 and φ determine the dynamical properties of the augmented Lorenz model and can be used as secret keys for message encryption and decryption. However, the number of combinations of these bifurcation parameters for which the augmented Lorenz model yields chaos is not sufficiently large, similarly to in the case of the Lorenz model. Instead, the key matrix is used to generate the secret key in the proposed symmetric key cryptographic method, keeping the bifurcation parameters σ, R_0 and φ constant. In the proposed symmetric secret key mechanism, the bifurcation parameters are set to σ=25, R_0=3185 and φ=0.36[rad]. In the proposed asymmetric secret key mechanism, the limitation on the length of the message and the key size are eliminated.

2. Preliminaries

This section introduces the augmented Lorenz equations, the logistic map and the beta transformation map.

2.1 Augmented Lorenz Equations

The Lorenz model is a three-dimensional system of nonlinear ordinary differential equations consisting of scalar variables labeled as X, Y and Z, and is specified by three dimensionless fluid- mechanical parameters, i.e., the Prandtl number σ, the reduced Rayleigh number R_0, and a geometrical parameter φ. Lorenz subsystems when truncated at a finite number of N are referred to as augmented Lorenz equations. The augmented Lorenz model is a (2N+1)-dimensional system of nonlinear ordinary differential equations for 2N+1 generalized coordinates, which are the dimensionless angular velocity labeled as X, and N sinusoidal and N cosinusoidal Fourier coefficients of the dimension-less dynamic pressure of the air inflow, labeled as Y_i and Z_i with i running from 1 to N, respectively.

The augmented Lorenz equations in their original form are given as

$$\dot{X} = \sigma \; tr[(n\text{-}\{\})^2 \; Y]\} - X \qquad (1)$$

$$\dot{Y} = RX - nZX - Y \qquad (2)$$

$$\dot{Z} = nYX - Z \qquad (3)$$

Here, X is a dimensionless scalar variable, Y and Z are dimensionless $N \times N$ diagonal matrices whose diagonal components are labeled as Y_n and Z_n, respectively, with n running from 1 to N. $\dot{X}$, $\dot{Y}$ and $\dot{Z}$ represent the first-order derivatives of X, Y and Z with respect to dimensionless time τ, respectively and tr(.) expresses the diagonal sum of a matrix. The dimensionless matrix parameter R is defined using

$$R = R_0 n^2 \varphi W \qquad (4)$$

$$\text{Where-}n = diag(1,....,n,...N) \qquad (5)$$

$$\varphi = diag[\varphi - \tfrac{1}{2}\sin 2\varphi, ..., \tfrac{1}{n-1}\sin(n\text{-}1)\varphi - \tfrac{1}{n+1}\sin(n+1)\varphi,$$
$$...., \tfrac{1}{N-1}\sin(N\text{-}1)\varphi - \tfrac{1}{N+1}\sin(N+1)\varphi] \qquad (6)$$

$$W = diag(\sin\varphi, ..., \sin(n\varphi), ...\sin(N\varphi) \qquad (7)$$

2.2 Logistic Map

The logistics map is given by the equation

$$X_{n+1} = rX_n(1 - X_n) \qquad (8)$$

where X_{n+1} is the current state variable, X_n is the previous state variable and r is a constant in the range 2<r<4.

2.3 Beta Transformation Map

Let a_1, $b_1 > 0$ and $a_1 \neq b_1$.The beta-transformation map is described by the equation

$$x_{m+1} = F^K(x_m) = [\, x_m + a_1 x_{m-1}] \; (\text{mod } 1) \,, \; K_i = 0$$
$$= [b_1 x_m + x_{m-1}] \; (\text{mod } 1) \,, \; K_i = 1 \qquad (9)$$

where m=0, 1, ….., x_{-1}=0, a_1x_{m-1}, b_1x_m are evaluated via the beta-transformation, k is binary string and k_i is a binary value 0 or 1 of position of (i). This system is sensitive to a change in a_1, b_1 parameters.

3. Proposed System

The proposed system uses the augmented Lorenz equations to generate chaotic signal necessary for chaotic based symmetric and asymmetric key

DOI: 10.18535/ijsrm/v3i11.18

cryptography. The block diagram of the proposed system is given as:

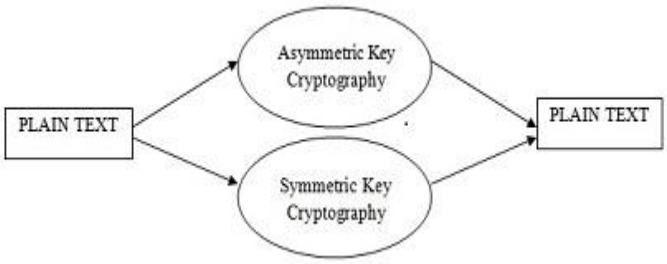


Figure 1: Block Diagram of Proposed Asymmetric and Symmetric Key Cryptography

The block diagram for asymmetric key cryptography using augmented Lorenz equations is given below:

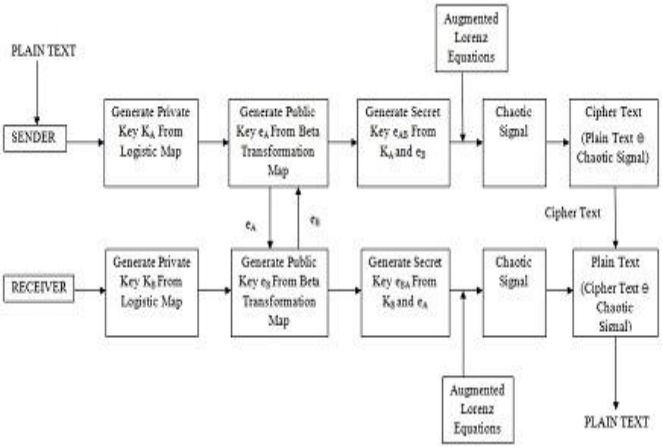


Figure 2: Block Diagram of Proposed Asymmetric Key Cryptography Using Augmented Lorenz Equations

The block diagram for symmetric key cryptography using augmented Lorenz equations is given below:

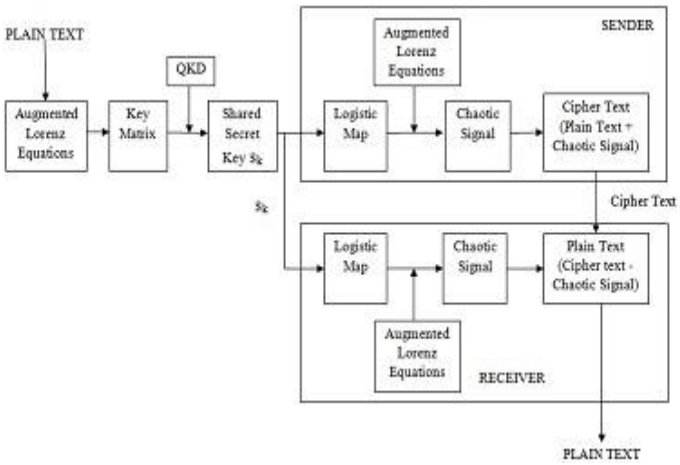


Figure 3: Block Diagram of Proposed Symmetric Key Cryptography Using Augmented Lorenz Equations

The methodology of the system is described as follows:

3.1 Key Generation and Distribution

In the proposed method, for asymmetric key cryptography using augmented Lorenz equations, the logistic map given in equation (8) is used as the generator for private key at both sender and the receiver side. Three logistic maps are used for private key generation.

At both sender side and receiver side, private key is generated from the following set of equations.

$$x_1 = rx_0(1-x_0) \quad (10)$$
$$x_2 = rx_1(1-x_1) \quad (11)$$
$$y_1 = ry_0(1-y_0) \quad (12)$$
$$y_2 = ry_1(1-y_1) \quad (13)$$
$$z_1 = rz_0(1-z_0) \quad (14)$$
$$z_2 = rz_1(1-z_1) \quad (15)$$

$$\text{If } x_1 > x_2,\ K_x = 1 \text{ else } K_x = 0$$
$$\text{If } y_1 > y_2,\ K_y = 1 \text{ else } K_y = 0$$
$$\text{If } z_1 > z_2,\ K_z = 1 \text{ else } K_z = 0$$

Therefore, the private key for sender is obtained as $K_A = (KA_x, KA_y, KA_z)$ and the private key for receiver is obtained as $K_B = (KB_x, KB_y, KB_z)$ from the equations (10) to (15).

Once the private keys are generated, the next step is to generate the public key for both sender and the receiver. The public key on both sides are generated using the beta-transformation map given in equation (9).

At both sender side and receiver side, the public key is generated from the following set of equations.

$$x_{m+1} = F^K(x_m) = [\, x_m + a_1 x_{m-1}] \pmod 1,\ K_x = 0$$
$$= [b_1 x_m + x_{m-1}] \pmod 1,\ K_x = 1 \quad (16)$$
$$y_{m+1} = F^K(y_m) = [\, y_m + a_2 y_{m-1}] \pmod 1,\ K_y = 0$$
$$= [b_2 x_m + y_{m-1}] \pmod 1,\ K_y = 1 \quad (17)$$
$$z_{m+1} = F^K(z_m) = [\, z_m + a_3 z_{m-1}] \pmod 1,\ K_z = 0$$
$$= [b_3 z_m + z_{m-1}] \pmod 1,\ K_z = 1 \quad (18)$$

The initial values x_0, y_0, z_0 for sender and receiver and the parameters of three dimension beta-transform (a_1, b_1, a_2, b_2, a_3, b_3) are already set and thus the public key for sender is obtained as $e_A(X_A,Y_A,Z_A) = F^K{}_A(x_0,y_0,z_0)$ and the public key for receiver is obtained as $e_B(X_B,Y_B,Z_B) = F^K{}_B(x_0,y_0,z_0)$ from the equations (16) to (18).

Once the public keys for both sender and receiver are generated, the next step is the asymmetric key generation, that is the generation of secret keys e_{AB} and e_{BA} between sender and receiver. To generate the secret keys e_{AB} and e_{BA} , the public keys of both sender and receiver has to be exchanged. The public key e_{AB} is then sent to the receiver and the public key e_{BA} is sent to the sender.

So at the sender side, the secret key e_{AB} is generated from sender's private key K_A and the receiver's public key e_B using the beta-transformation given by the equation (16), (17) and (18) and is obtained as $e_{AB}(X_{AB},Y_{AB},Z_{AB}) = F^K{}_A(e_B(X_B,Y_B,Z_B))$. At the receiver side, the secret key e_{BA} is generated from receiver's private key K_B and sender's public key e_A using the same equations and is obtained as $e_{BA}(X_{BA},Y_{BA},Z_{BA}) = F^K{}_B(e_A(X_A,Y_A,Z_A))$.

In symmetric key cryptography using augmented Lorenz equations, the secret key that is shared between sender and receiver is obtained from the key matrix M. The secret key matrix, $M=diag(M_1,M_2,....,M_N)$ is generated from the diagonal matrices Ẏ and Ż of augmented Lorenz equations given in equations (2) and (3). The shared secret key s_k is then generated from the key matrix M using the Quantum Key Distribution (QKD) protocol and is then distributed between sender and receiver.

3.2 Chaotic Signal Generation

In chaotic based cryptography, the chaotic signal generated using different techniques is used for encryption and decryption of the message. In the proposed paper, the chaotic signal can be generated from augmented Lorenz equations.

In asymmetric key cryptography using augmented Lorenz equations, the chaotic signal used for encryption is generated using the secret key e_{AB} known to the sender and the Ẏ matrix and the Ż matrix of the augmented Lorenz equations given in equations (2) and (3). e_{AB} is the secret key obtained at the sender side using beta-transformation.

In symmetric key cryptography using augmented Lorenz equations, logistic map is used for the generation of the chaotic signal for encryption, with the help of the shared secret key s_k and Ẏ matrix and Ż matrix of the augmented Lorenz equations given in (2) and (3). The shared secret key is generated by the sender and the receiver using the QKD protocol. Once the shared secret key has been generated, it is given as the initial condition for the logistic map. The chaotic signal is then generated from the output of the logistics map and the Ẏ matrix and Ż matrix of the augmented Lorenz equations given in equations (2) and (3).

3.3 Encryption

In public key cryptography using augmented Lorenz equations, the cipher text is obtained by masking it with the chaotic signal to prevent it from eavesdropping. Here, the plain text is encrypted by XORing it with the chaotic signal. The chaotic signal for message encryption is generated using the secret key e_{AB} and augmented Lorenz equations.

Here, cipher text = plain text XOR chaotic signal

In symmetric key cryptography using augmented Lorenz equations, the plain text which is to be transmitted safely is masked with the chaotic signal. Here, the chaotic signal is generated from the shared secret key s_k between sender and the receiver, the logistic map and also the augmented Lorenz equations. The technique used for masking chaotic signal with the plain text is one time padding. One time padding is an encryption technique which involves modular addition of the message and the key. The key here is the chaotic signal. For one time padding, both the message and the key have to be of same length.

3.4 Chaotic Signal Regeneration

Once the cipher text has been transmitted and is received at the receiver side, the receiver has to

unmask the chaotic signal from the cipher text to obtain the plain text. To unmask the chaotic signal from the received cipher text, the receiver has to regenerate the chaotic signal.

In asymmetric key cryptography using augmented Lorenz equations, the chaotic signal used for decryption is regenerated using the secret key e_{BA} and the Ẏ matrix and the Ż matrix of the augmented Lorenz equations given in equations (2) and (3). e_{BA} is the secret key that is obtained at the receiver side.

In symmetric key cryptography using augmented Lorenz equations, the chaotic signal is regenerated using the shared secret key s_k, the logistic map and the augmented Lorenz equations. Here, the shared secret key s_k is the key known to both sender and the receiver and is calculated using QKD protocol. The shared secret key s_k is given as the initial condition for the logistic map. The chaotic signal is then generated from the output of the logistics map and the Ẏ matrix and Ż matrix of the augmented Lorenz equations given in equations (2) and (3).

3.4 Decryption

To obtain the plain text back from the cipher text, the chaotic signal has to be unmasked from the cipher text. To decrypt the cipher text, the chaotic signal has to be regenerated. Once the chaotic signal has been regenerated, in asymmetric key cryptography using augmented Lorenz equations the cipher text is XOR-ed with the chaotic signal to obtain the plain text.

Here, plain text = cipher text XOR chaotic signal

In symmetric key cryptography using augmented Lorenz equations, the receiver first regenerates the replica of chaotic signal. To unmask the chaotic signal from the received cipher text, he then subtracts the replica of the chaotic signal from the cipher text to obtain the plain text. The decryption takes place as reverse process of encryption where modular subtraction of the cipher text and the chaotic signal takes place.

4. Algorithms

4.1Algorithm for Asymmetric Key Cryptography Using Augmented Lorenz Equations

1. Set initial values x_0, y_0, z_0 for both sender and receiver and set the parameters of three dimension beta-transform (a_1,b_1,a_2,b_2,a_3,b_3).
2. Generate the private key K_A for sender using three logistic maps.
3. Generate the private key K_B for receiver using three logistic maps.
4. Generate the public key e_A for sender using three beta-transformation maps.
5. Generate the public key e_B for receiver using three beta-transformation maps.
6. Send public key of sender e_A to receiver.
7. Send public key of receiver e_B to sender.
8. The sender calculates the secret key for sender e_{AB} using the beta-transformation map.
9. The receiver calculates the secret key for receiver using the beta-transformation map.
10. The sender generates the chaotic signal for encryption using e_{AB} and the augmented Lorenz equations.
11. The sender encrypts the plain text by XOR-ing it with the chaotic signal and the cipher text is sent to the receiver through the classical data communication channel.
12. The receiver regenerates the chaotic signal for decryption e_{BA} and the augmented Lorenz equations.
13. The receiver decrypts the cipher text by XOR-ing it with the regenerated chaotic signal to obtain the plain text.

4.1 Algorithm for Symmetric Key Cryptography Using Augmented Lorenz Equations

1. The secret key matrix M is generated from the augmented Lorenz equations.
2. The shared secret key s_k for the sender and receiver is calculated using the Quantum Key Distribution (QKD) protocol.
3. The shared secret key s_k is then given as the initial condition for the logistic map.
4. The sender generates the chaotic signal which is used for masking the plain text from the output of

DOI: 10.18535/ijsrm/v3i11.18

the logistic map and the augmented Lorenz equations.

5. The sender encrypts the plain text by masking it with the chaotic signal using one time padding.

6. The sender then transmits the cipher text through the classical data communication channel.

7. At the receiver side, the shared secret key s_k is given as the initial condition for the logistic map.

8. The chaotic signal is regenerated from the output of the logistic map and the augmented Lorenz equations.

9. The receiver then unmasks the chaotic signal from cipher text to obtain the plain text using the reverse process of encryption.

5. Experimental Results and Discussion

Analysis is conducted to find out the chaos generated by the dynamic behavior of the augmented Lorenz equations, the encryption and the decryption time of symmetric and asymmetric key cryptography using augmented Lorenz equations and signal intensity of plain text and cipher text.

5.1 Dynamic Behavior of Augmented Lorenz Equations

To exemplify chaos generated by the augmented Lorenz equations, the equations are integrated by the fourth-order Runge-Kutta method. The equations for fourth order Runge-Kutta method are given as

$$y_{n+1} = y_n + [k_1 + 2k_2 + 2k_3 + k_4]/6 \quad (19)$$

$$k_1 = hf(x_n, y_n) \quad (20)$$

$$k_2 = hf(x_n + 1/2h, y_n + 1/2k_1) \quad (21)$$

$$k_3 = hf(x_n + 1/2h, y_n + 1/2k_2) \quad (22)$$

$$k_4 = hf(x_n + h, y_n + k_3) \quad (23)$$

$$h = x_{i+1} - x_i \quad (24)$$

From the analysis, it is found that augmented Lorenz equations generate sufficient high dimensional chaos necessary for the system.

Table 1: Numerical Solutions of $\dot{X}$

N	Numerical Solutions of $\dot{X}$
0	-518147096.00000376
1	67467080078204.48
2	-15302513122558704e19
3	2.59026914834978e25
4	-7.264376617968133e30
5	3.749747975234668e36
6	-3.958771088719032e41
7	2.628871426102482e47
8	-4.228423709264103e52
9	-5.781048040009516e58

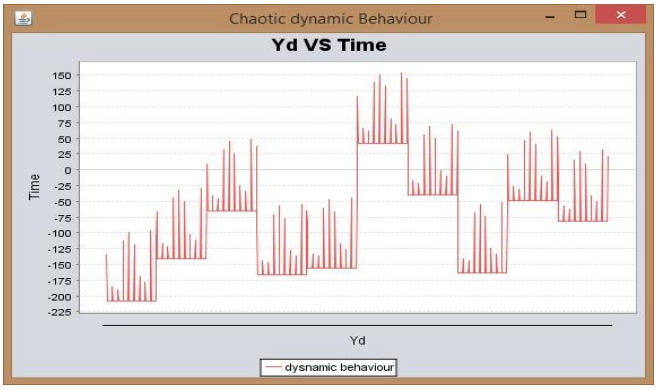


Figure 5: Dynamic Behavior of $\dot{Y}$

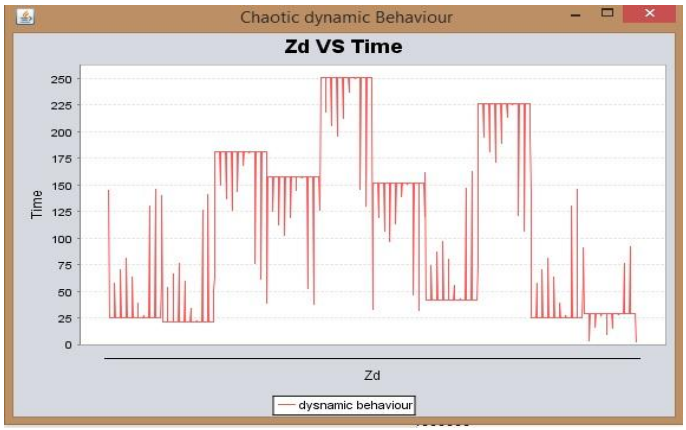


Figure 6: Dynamic Behavior of $\dot{Z}$

5.2 Encryption Time and Decryption Time

Encryption time is the time taken to compute cipher text from plain text and decryption time is the time taken to compute plain text back from cipher text. From the analysis, the encryption time and decryption time of symmetric key cryptography is found to be higher than the encryption and decryption time of asymmetric key cryptography.

DOI: 10.18535/ijsrm/v3i11.18

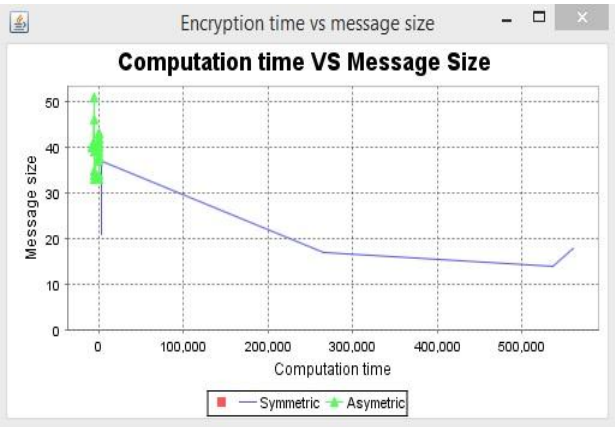


Figure 7: Encryption Time Taken for Symmetric and Asymmetric Key Cryptography

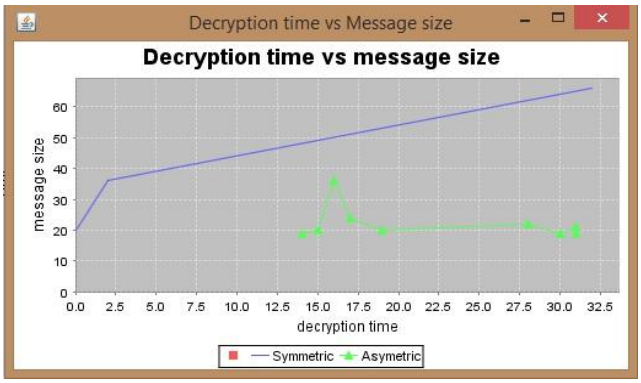
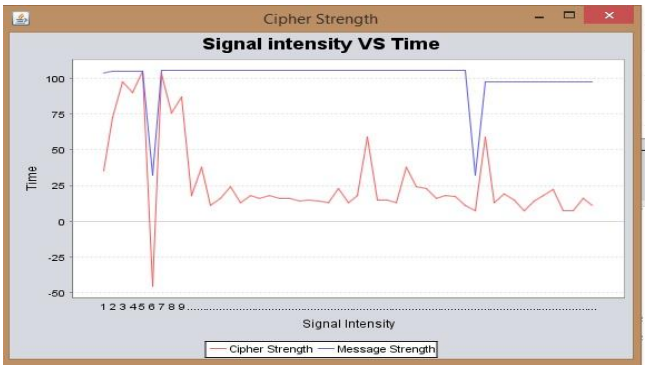


Figure 8: Decryption Time Taken for Symmetric and Asymmetric Key Cryptography

5.3 Signal Intensity of Plain Text and Cipher Text

The strength of the original message and the cipher text after encryption is computed by plotting the signal intensity against time. From the analysis, the signal intensity of cipher text is found to be stronger than the signal intensity of the plain text.



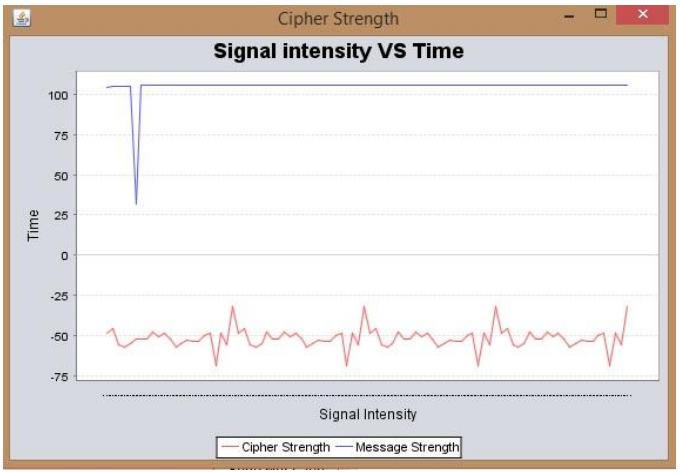


Figure 9: Signal Intensity of Plain Text and Cipher Text in Symmetric Key Cryptography

6. Conclusion

The performance of symmetric and asymmetric key cryptography using augmented Lorenz equations are compared and analyzed. The application of the augmented Lorenz equations adds more chaoticity to the system. Also it is found that the signal I ntensityof cipher text is stronger than the signal intensity of plain text in both symmetric and asymmetric key cryptography using augmented Lorenz equations. The main disadvantage of the proposed system is the large execution time in symmetric key cryptography. As a future work, measures can be taken to reduce the total execution time when augmented Lorenz equations are used for symmetric key cryptography. Future work can also include using the proposed public key cryptosystem to enhance Internet security protocols.

References

1. K. M. Cuomo and A. V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, Phys. Rev. Lett., vol. 71, no. 1, pp. 6568, 1993.
2. ”Chaotic Cryptography Using Augmented Lorenz Equations Aided by Quantum Key Distribution”, Kenichiro Cho and Takaya Miyano, Member, IEEE

3. ”Chaotic Based Key Management and Public-keyCryptosystem”,MazenTawfikMohammed , Alaa Eldin Rohiem, Ali El-moghazy and A. Z. Ghalwash, Military technical College, Cairo, Egypt
4. H.Dedieu, M. Kennedy, and M. Hasler, Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua’s circuits, IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 40, pp. 634642, 1993.Hatem Ltaief1, Jaku
5. F. Anstett, G. Millerioux, and G. Bloch, Chaotic cryptosystems: Cryptanalysis and Identifiability, IEEE Trans. Circuits Syst. I, Reg.Papers,vol.53,no. 12, pp.26732680,