ISSN 2047-3338

Chaotic Encryption Based PGP Protocol

Mazen Tawfik Mohammed[1], Alaa Eldin Rohiem[2], Ali El-moghazy[3] and A. Z. Ghalwash[4]
[1, 2]Military technical College, Cairo, Egypt
[3]Higher Technological Institute, Cairo, Egypt
[4]Helwan University, Egypt
[1]mazen.mtc@gmail.com, [2]alaa_rohiem@yahoo.co.uk, [3]moghazymtc@yahoo.com

***Abstract*— E-mail service is one of the most important Internet services. E-mail security includes confidentiality, authentication, message integrity, non-repudiation. Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME) are email security protocol. They are used to provide security services for email system. PGP is widely used as de facto protocol for securing e-mail. The used algorithms in PGP suffer from problems such as low performance and weakness in encryption. The chaotic encryption system is new trend in cryptography. This paper focuses on designing a new cryptosystems based on chaotic system which makes the complexity of breaking more than the default so the new cryptosystem is more secure. The used chaotic system is built on Lorenz system with random initial conditions which increase the randomness of output sequences. The proposed technique is integrated with the PGP protocol. It is implemented using c# programming language and open source for OpenPGP. The results of proposed system tests show that the security and performance are improved.**

***Index Terms*— PGP, S/MIME, Chaotic and E-mail**

I. INTRODUCTION

SECURITY is one of most important issue in mail. The fundamental mechanism for providing security for messages in unsecure network is encryption. The encryption of messages is done using algorithms that are common and known such as International Data Encryption Algorithm (IDEA) [4], Data Encryption Standard (DES) [5], Triple Data Encryption Standard (TDES) [6], and Advanced Encryption Standard (AES) [3]. The security of an encryption algorithm is based on the security of the key. It is called secret-key or symmetric-key encryption, one key is used for both encryption and decryption. The key distribution problem is solved by public key algorithm. It is called an asymmetric algorithm that uses a pair of keys. A public key is used for encryption and a private is used for decryption. An e-mail security is needed to provide confidentiality, data origin authentication, message integrity, non repudiation of origin. The chaotic cryptography is an important field of information security. The chaotic systems characteristics make it a robust cryptosystem against statistical attacks. It is difficult to handle bulk data capacity and high data redundancy related to some deferent types of content message such as image and video by traditional encryption methods [12]. In this paper we introduce a novel technique for enhancement security of PGP protocol based on chaotic systems (Lorenz). The paper is organized as follows: Section 2 introduces related work. Security of email, email protocols, email security protocol are introduced in Section 3. Chaotic cryptography and the proposed cryptosystem for encryption in PGP are introduced in section 4. Results and comparison with standard are given in section 5. Section 6 is the conclusion.

II. RELATED WORKS

In the recent years tremendous interest in the studies of chaos-based cryptography has been observed. These studies were greatly encouraged by the increasing number of applications that successfully utilize chaotic systems. Researchers proposed several designs for symmetric cryptosystems based on chaotic maps [7-11]. Various encryption algorithmic solutions have been proposed. The evaluation of encryption algorithm in general is performed by many researchers and statistical test suites are used to evaluate the randomness of these algorithms.

Others researchers propose several attacks on PGP protocol [1, 2]. In [20] an Enhanced Pretty Good Privacy (EPGP) System with mutual non-repudiation is presented and attempts to increase the degree of security and efficiency of e-mail message communication. In this research, a new cryptosystem based on chaotic system for encryption is presented then it is implemented in PGP protocol. NIST statistical analysis for randomness security is performed and the performance is measured based on encryption delay.

III. SECURITY OF EMAIL

Email is the one of most requested Internet services. Typical email architecture contains four elements which are post offices, message transfer agents, gateways and E-mail clients. The outgoing/incoming messages are temporally stored in post offices. Message transfer agents are used for

forwarding messages between post offices and to the destination clients. Gateways are used to translate between different e-mail systems, different e-mail addressing schemes and messaging protocols. E-mail clients connect to the post office. IETF publish RFCs about the format of mail messages, email protocols and email security protocols.

A. Email Protocols

The Simple Mail Transfer Protocol (SMTP) is used to transfer e-mail messages from one host to another, also is used to transfer e-mail messages among separate servers. SMTP is described in RFC 821, it is Internet standard and uses TCP protocol with port 25. RFC 1869 defines the capability for SMTP service extensions. Extended SMTP (ESMTP) allows new service extensions. SMTP traffic is secured by SSL protocol. The Multipurpose Internet Mail Extensions (MIME) is a standard described in RFC 1521 and RFC 1522. It defines the representation for "complex" message bodies. The "complex" message bodies include messages with embedded graphics or audio clips, messages with file attachments, messages in Japanese or Russian, or signed messages. SMTP cannot be used for languages that are not supported by seven-bit ASCII characters. The binary files, video or audio data cannot be used with SMTP. The Post Office Protocol is used to transfer e-mail messages from a permanent mailbox to a local computer. The POP client creates a TCP connection to a POP3 server on the mailbox computer. The messages are stored and transferred as text files in RFC 2822 standard format. The computers with a permanent mailbox must run two servers, the first server is a SMTP server that accepts sent mail and adds each incoming message to the user's permanent mailbox, and the second server is a POP3 server allows a user to extract messages from the mailbox and delete them. The Internet Message Access Protocol (IMAP) is a standard protocol for accessing email from your local server. IMAP requires continual access to the server during the time that client is working with its mail. In the (POP3), the mail is saved in mailbox on the server. It is immediately downloaded to your computer and no longer maintained on the server.

B. Email attack and defense

There are different types of attacks on email systems [1-2], the first is spoofing attack which can be used to enable one party to masquerade as another party. The defense for this attack is authentication. Through authentication only trusted users can engage in sessions. The second attack is man in the middle/session hijacking attack, in which an attacker inserts itself between two parties and pretends to be one of the parties, the solution is digital signatures. The third attack is an eavesdropping attack in which an attacker listens to a private communication. The defense for this attack is encryption. The fourth attack is data modification attack in which an attacker changes the data. The defense for this attack is an encrypted message digest. The fifth attack is a dictionary attack in which an attacker uses large set of common used passwords to guess the password. The defense is using strong passwords. The sixth attack is denial of service in which an attacker floods the network or computer with hundred or even million of messages or service request. The defense for this attack is authentication service filtering. Another risk of SMTP is the sending and receiving of viruses and Trojan horses. In this paper we focus on the eavesdropping attack so the vulnerability of secure encryption by PGP is related to the used algorithm. E-mail message includes different types of data such as text, image, and video. The used algorithms in PGP are vulnerable to eavesdropping attack when dealing with images or video.

C. Email Security Protocols

Email security protocol is responsible for protection email messages and passwords. Email security protocol ensures the privacy of clients. There are some email providers that support a secure mail protocol and others do not support such security protocol. Transport layer Security (TLS) prevent eavesdropping and spoofing between mail servers. It is used to provide endpoint authentication and privacy over the Internet. There are separate protocols which are used (by client) to provide security for email messages such as S/MIME and PGP.

1) Secure/Multipurpose Internet Mail Extension (S/MIME)

S/MIME is a security protocol which is designed to provide security for electronic mail. The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol. S/MIME is an IETF standards track and defined in several documents such as RFCs (3369, 3370, 3850, 3851, 6211, 5750, 5751, and 4262). S/MIME defines several cryptographic algorithms such as Triple DES (TDES), AES, RC2/40, RSA, Diffe-Hellman, SHA-1, and Digital Signature Standard (DSS). S/MIME version 3 encrypts message content using TDES algorithm in the cipher block chaining mode of operation. It uses the SHA-1 hash algorithm and the Digital Signature Algorithm (DSA) for generating digital signatures. Certificate information is secured with S/MIME to produce a public key cryptography standard (PKCS) object. S/MIME produces the hash value of the message content then it encrypts with the signer's private key.

2) Pretty Good Privacy PGP

Pretty Good Privacy (PGP) is an open source package used for e-mail security. PGP is an IETF standards track and defined in several documents. Table (I) shows the different RFC documents for PGP. The PGP protocol is described in RFC 1991 and expanded into OpenPGP in RFC 2440. RFC 2015 describes the different kinds of PGP message which is encapsulated using MIME.

TABLE I. THE DIFFERENT RFC DOCUMENTS FOR PGP

RFC	Title
1991	PGP Message Exchange Formats
2440 4880	OpenPGP Message Exchange Formats
2015	MIME Security with Pretty Good Privacy (PGP)
2726	PGP Authentication for RIPE Database Updates
3156	MIME Security with OpenPGP
5581	The Camellia Cipher in OpenPGP

PGP provides authentication using digital signature, confidentiality using symmetric block encryption, compression using ZIP algorithm and encoding using Rdic-64. Table (II) shows the different algorithms used for security in PGP.

TABLE II. THE DIFFERENT ALGORITHMS USED FOR SECURITY IN PGP [21]

Public-key algorithm		symmetric algorithm		Hash Algorithms	
ID	Description	ID	Description	ID	Description
1	RSA (encryption/signing)	0	No Encryption	1	MD5
2	RSA (encryption only)	1	IDEA	2	SHA-1
3	RSA (signing only)	2	Triple DES	3	RIPE-MD/160
16	ElGamal (encryption only)	3	CAST-128	4	Reserved(double with SHA)
17	DSS	4	Blowfish	5	MD2
18	Reserved (Elliptic Curve)	5	SAFER-SK 128	6	TIGER/192
19	Reserved (Elliptic Curve Digital Signature Algorithm)	6	Reserved (DES/SK)	7	Reserved (HAVAL)
20	ElGamal (encryption/signing)	7	Reserved(AES-128)	100-110	Private algorithms
21	Reserved (Diffie-Hellman)	8	Reserved(AES-192)		
100-110	Private algorithms	9	Reserved(AES-256)		
		100-110	Private algorithms		

PGP uses public key algorithms for key exchange. In e-mail security, the encryption/decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is encrypted with the public key of the receiver and is sent with the message. The packet tag denotes what type of packet the body holds. Table (III) shows some commonly used packet types.

TABLE III. COMMONLY USED PACKET TYPES [21].

Tag Value	Packet type
1	Session key packet encrypted using a public key
2	Signature packet
5	Private-key packet
6	Public-key packet
8	Compressed data packet
9	Data packet encrypted with a secret key
11	Literal data packet
13	User ID packet

Figure 1 shows encrypted PGP message. Several packets are used to construct encrypted message. The public-key encrypted session key packet is used to ecrypte session key using public-key algorithm. The session key is used to encrypt a message.

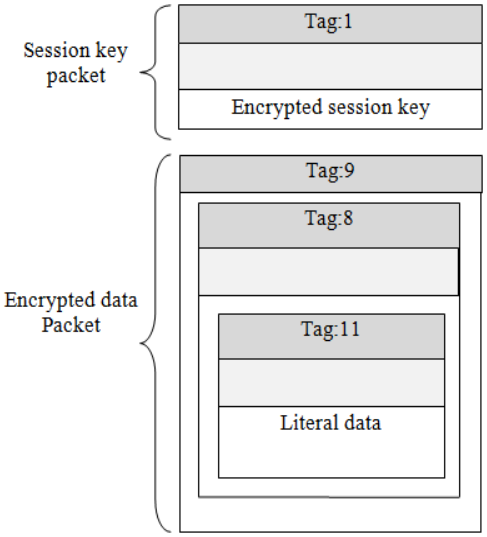


Figure 1. Encrypted message [21]

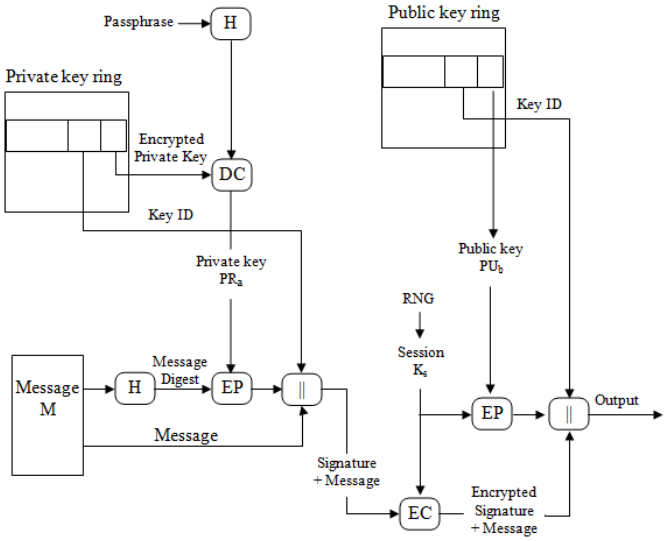
D. Confidentiality in Standard PGP Algorithm

Symmetric and asymmetric algorithms are used to provide confidentiality for PGP message. Confidentiality is achieved by encrypting the message with a randomly chosen session key and then encrypting the session key with the RSA public key of the recipient. Open PGP message format is described in RFC4880.

1) PGP Message Generation and Reception

Figure 2 shows the diagram for PGP message generation at sender side. PGP uses four types of keys which are one-time session conventional key, public key, private key, passphrase-based conventional key. Private and public keys are stored in two files at each client, these files are called keyrings. Private keys are stored in encrypted form. Decryption key is determined by user-entered passphrase. Random session key is used to encrypt the message. A new session key is required each time a message is encrypted. PGP uses the timing of key strokes and key patterns to generate random numbers. Session key is encrypted using receiver's public key and appended to message. The sending PGP entity performs the following steps:

- Signs the message:
  - PGP gets sender's private key from key ring using its user id as an index.
  - PGP prompts user for passphrase to decrypt private key.
  - PGP constructs the signature component of the message.
- Encrypts the message:
  - PGP generates a session key and encrypts the message.
  - PGP retrieves the receiver public key from the key ring using its user id as an index.
  - PGP constructs session component of message

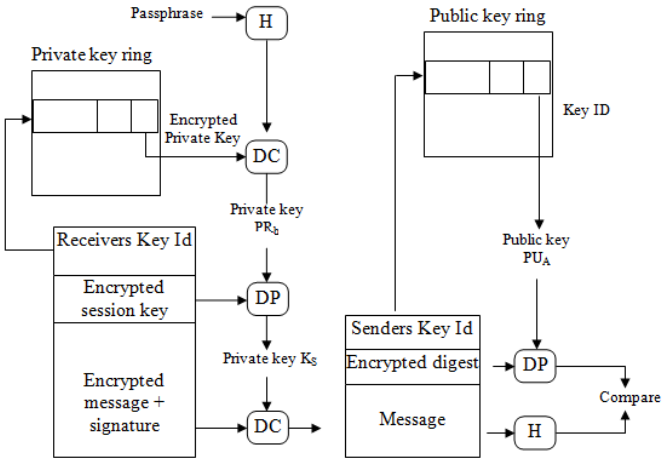


Where:
H: hash function;
DC: Symmetric decryption process;
EP: Public key Encryption process;
EC: Symmetric encryption process;

Figure 2. PGP message generation [23]

Figure 3 shows the diagram for PGP message generation at receiver side. Asymmetric and symmetric key cryptosystems are combined in this way to provide security for key exchange and then efficiency for encryption. The session key k is used only to encrypt message m and is not stored for any length of time. The schemes for authentication and confidentiality can be combined so that receiver can sign a confidential message which is encrypted before transmission. The receiving PGP entity performs the following steps:

- Decrypting the message: PGP get private key from private-key ring using Key ID field in session key component of message as an index then PGP prompts user for passphrase to decrypt private key. After that PGP recovers the session key and decrypts the message.
- Authenticating the message: PGP retrieves the sender's public key from the public-key ring using the Key ID field in the signature key component as index. Then PGP recovers the transmitted message digest. After that PGP computes the message for the received message and compares it to the transmitted version for authentication.



Where:
H: hash function;
DC: Symmetric decryption process;
DP: Public key decryption process;

Figure 3. PGP message reception [23]

IV. CHAOTIC CRYPTOGRAPHY (THE PROPOSED ALGORITHM)

In the recent years tremendous interest in the studies of chaos-based cryptography has been observed. These studies were greatly encouraged by the increasing number of applications that successfully utilize chaotic systems.

A. Chaotic Systems

Chaos Systems are nonlinear dynamical systems. Depending on the time range they are described by difference equations (discrete-time systems) or differential equations (continuous-time systems). Henon map [12], logistic map [13] and Couple Chaotic Systems Based Pseudo Random Generator (CCSPRBG) [14] are example of discrete-time systems. Rossler system [15] and the Lorenz system [16] are example of the continuous-time systems. Chaotic System is sensitive to initial condition, this means that the different initial condition produces different trajectory, the same conditions can produce the same trajectory. Lyapunov Exponents is used to define if the system has chaotic behavior or not, if the system is chaotic the difference between two trajectories with close initial condition will exponentially increase after a very short time. The difference is defined using the equation (1) [17]:

$$d_t = d_0 2^{\lambda t} \quad (1)$$

Where:

d_0: is initial distance.
d_t: is the distance at t time.
λ: is Lyapunov Exponents.

The value of Lyapunov Exponents (λ) is obtained by averaging the points, using the equation (2) [17]:

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})} \quad (2)$$

Where:

N: the number of points.
t_0: time at initial point.
t_N: time at point N.
$d(t_k)$: the distance at point k.
$d(t_{k-1})$: the distance at point k-1.

If $\lambda>0$ the system is considered as chaotic.

1) The Lorenz System

The purpose of Lorenz [1963] was to create and analyze a model for the unpredictable behavior of the weather. By greatly simplifying and truncating a set of nonlinear partial differential equations, he obtained the following system of ordinary differential equations (3) [16]:

$$\begin{aligned} x' &= \sigma (y - x) \\ y' &= \gamma x - y - xz \\ z' &= xy - bz \end{aligned} \quad (3)$$

A typical Lorenz chaotic attractor can be obtained by setting the parameters $\sigma=10$, $\gamma=28$, and $b=8/3$ with initial conditions $(x_0; y_0; z_0)=(1; 1; 1)$. Note that the Lorenz equation has three parameters and two nonlinearities (*xz* and *xy*), each of which is a function of two variables. The theoretical Lyapunov exponent for the Lorenz system is equal to1.5 [18].

B. Proposed Chaotic Encryption system in PGP

Symmetric cryptosystem based on chaotic system needs defining the mapping scheme for trajectory, choosing valid initial condition and parameters then generating Random Number sequence and encrypting message based on stored Random Number sequence. Decryption process is started by using the same initial condition and parameters to generate the same PRN and then decrypting the cipher text. The initial condition and parameters are considered as keys. The chaotic system must pass NIST statistical test, the chaotic system is based on three dimensions chaotic system which is Lorenz system, but the normal three dimensions system doesn't pass NIST statistical tests [19]. The proposed modification in chaotic system is based on random initial conditions, and the good choice for initial condition is session key which is random number. Figure 4 shows Encryption/Decryption process that includes:

- Generate initial condition form private key.
- Generate PRN using chaotic system.
- Apply XOR function between PRN and content of message.

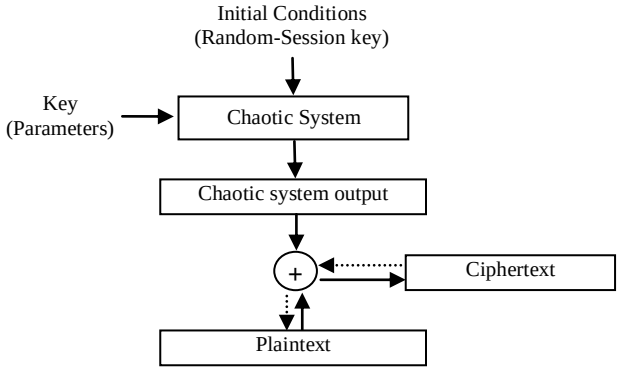


Figure 4. Chaotic encryption/decryption process

Table (IV) contains the common used symmetric key algorithm in PGP protocol and new identifier for symmetric chaotic encryption.

TABLE IV. CHAOTIC ENCRYPTION SYSTEM IN PGP

ID	Description
0	No Encryption
1	IDEA
2	Triple DES
3	CAST-128
4	Blowfish
5	SAFER-SK 128
6	Reserved for DES/SK
7	Reserved for AES-128
8	Reserved for AES-192
9	Reserved for AES-256
100	Chaotic encryption
101-110	Private algorithms

The session key packet contains an encrypted session key as shown in Figure 5. It is used to encrypt session key using public-key algorithm. The session key is used to encrypt a message. The session key is used as initial conditions for chaotic system.

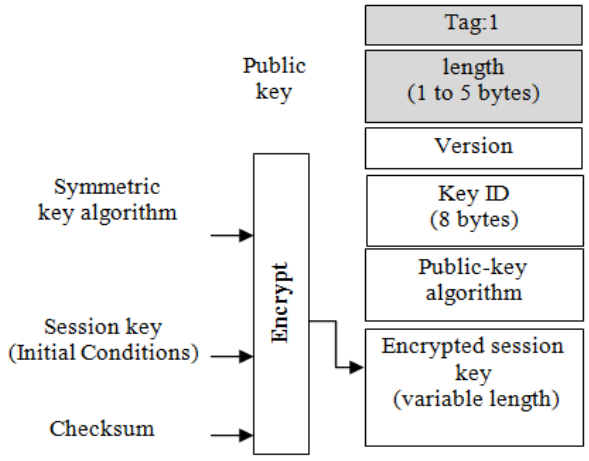


Figure 5. Session-key packet

Encrypted data packet is shown in Figure 6. The body of message is encrypted using chaotic system.

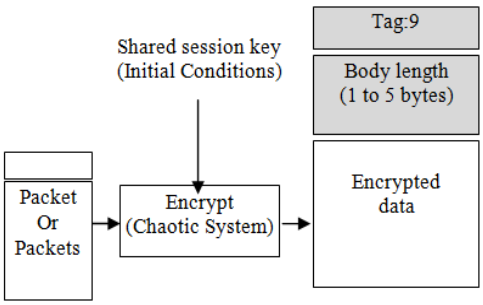


Figure 6. Encrypted data packet

The proposed chaotic encryption in PGP has the following features:

- The time required for encryption is less than in the default encryption.
- In default encryption the padding is needed when the length of payload is not multiple of block size of encryption algorithm. While in the proposed chaotic encryption there is no padding because the length of chaotic system output is variable.

V. Analysis of The Proposed Chaotic Encryption Cryptosystem

The proposed Chaotic Encryption Cryptosystem is evaluated in terms of performance and randomness for current used (or reserved) symmetric algorithms in PGP vs. chaotic.

A. Test Environments

The implementation of proposed cryptosystem is tested on a test network. The network consists of three computers, two computers for email message transmission and the third for email server. Also the third computer is used for monitoring email message traffic.The test bed is composed of three endpoints:

- The first endpoint consists of 2.16 GHz (CPU) with 3 Gbytes RAM and 1 Giga Ethernet for network card, running Windows Vista operating system.
- The second endpoint consists of 3 GHz (CPU) with 1 Gbytes RAM and 1 Giga Ethernet for network card, running Windows Xp operating system.
- The third endpoint consists of 3 GHz (CPU) with 1 Gbytes RAM and 1 Giga Ethernet for network card, running Windows Xp operating system.

The proposed encryption system is implemented using sharp privacy project for open PGP, open source bccrypto-net-1.7 project and Visual C#.net 2008. The implemented software includes a set of modules; the modules are either COTS (Commercial Off-The-Shelf) or developed specially for the purpose of the tests.

- *COTS*: There are three modules which are symmetric module, asymmetric module, PGP module and Email packet module.

- Symmetric module: includes AES, DES, and TDES.
- Asymmetric module: includes RSA.
- PGP module: sending and receiving PGP packets.
- Email packet module: forming PGP packets.

- *Developed for the purpose of the tests*: Microsoft project doesn't contain the chaotic module. We implement the chaotic module and inserted it in the project. Chaotic module contains the following functions:

- Pseudo-Random Number Generator (PRNG).
- Chaotic encryption/decryption cryptosystem.

B. Performance Analysis of The proposed Chaotic Encryption Cryptosystem

The performance is evaluated in terms of encryption and decryption time for different symmetric algorithms vs. chaotic as shown in Figure 7.

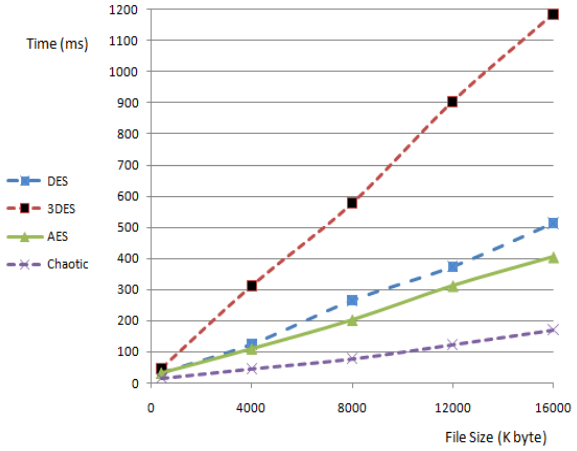


Figure 7. Encryption time for DES, 3DES, AES and Chaotic

C. Randomness Test using NIST for encryption system

In order to perform the randomness analysis of the implemented scheme the NIST tests must be applied [19]. There are various types of statistical test for randomness that have been proposed. Table (V) gives the P-value of NIST statistical tests for TDES and chaotic. The threshold level to pass test is P-value= 0.01.

TABLE V. P-value of NIST statistical tests for AES and chaotic

Test	TDES		Chaotic	
	P-Value	Result	P-Value	Result
Block frequency	0.455937	Passed	0.917870	Passed
Non–Overlapping Template Matching	0.992952	Passed	0.980883	Passed
Overlapping Template Matching	0.085587	Passed	0.282626	Passed
Universal Statistic	0.637119	Passed	0.975012	Passed
Approximate Entropy	0.041438	Passed	0.996335	Passed
Serial	0	Not Passed	0.534146	Passed
Linear Complexity	0.262249	Passed	0.971699	Passed
Frequency	0.474986	Passed	0.689019	Passed
Cumulative Sums (Forward) (Reverse)	0.911413 0.867692	Passed	0.410055 0.030806	Passed
Runs	0.023545	Passed	0.289667	Passed

Longest Runs of Ones	0.859637	Passed	0.842937	Passed
Discrete Fourier Transform	0.749884	Passed	0.236810	Passed
Random Excursions	0.900998	Passed	0.869014	Passed
Random Excursions Variant	0.930473	Passed	0.905843	Passed
Rank	0.207730	Passed	0.437274	Passed

Table (VI) gives the P-value of NIST statistical tests for AES and chaotic. The threshold level to pass test is P-value= 0.01.

TABLE VI. P-VALUE OF NIST STATISTICAL TESTS FOR AES AND CHAOTIC

Test	AES-key(256)		Chaotic	
	P-Value	Result	P-Value	Result
Block frequency	0.446556	Passed	0.917870	Passed
Non–Overlapping Template Matching	0.965019	Passed	0.980883	Passed
Overlapping Template Matching	0.073417	Passed	0.282626	Passed
Universal Statistic	0.544254	Passed	0.975012	Passed
Approximate Entropy	0.924076	Passed	0.996335	Passed
Serial	0.419021	Passed	0.534146	Passed
Linear Complexity	0.867692	Passed	0.971699	Passed
Frequency	0.465415	Passed	0.689019	Passed
Cumulative Sums (Forward) (Reverse)	0.678686 0.657933	Passed	0.410055 0.030806	Passed
Runs	0.102526	Passed	0.289667	Passed
Longest Runs of Ones	0.375313	Passed	0.842937	Passed
Discrete Fourier Transform	0.296834	Passed	0.236810	Passed
Random Excursions	0.969690	Passed	0.869014	Passed
Random Excursions Variant	0.901761	Passed	0.905843	Passed
Rank	0.311542	Passed	0.437274	Passed

The results indicate that the two methods AES and chaotic pass all tests but the P-value for chaotic based method is greater than the AES algorithm in most of tests which means more security. Also the results indicate that the chaotic encryption cryptosystem pass all tests but the TDES cryptosystem is not pass all test moreover the P-value for chaotic cryptosystem is greater than the TDES cryptosystem in most of tests which provides more security.

1) Image Encryption Quality Analysis

Email includes several types of data such as text, Image, Video. With the application of encryption to an image a change takes place in pixels values as compared to those values before encryption. Such change may be irregular. This means that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality. So the encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one. A measure for encryption quality may be expressed as the deviation between the original and encrypted image. The quality of image encryption may be determined as follows [22]:

Let F, F′ denote the original image (plain image) and the encrypted image (cipher image) respectively, each of size M*N pixels with L grey levels (each pixel is represented by an 8-bit). F(x, y), F′ (x, y) Є {0,.., L − 1} are the grey levels of the images F , F′ at position (x, y) , $0 \le x \le M-1$, $0 \le y \le N-1$. We will define HL(F) as the number of occurrence for each grey level L in the original image (plain image), and HL(F') as the number of occurrence for each grey level L in the encrypted image (cipher image). The encryption quality represents the average number of changes to each grey level L and it can be expressed mathematically as follows:

$$\text{Encryption Quality} = \frac{\sum_{l=0}^{255} | H_L(F') - H_L(F) |}{256}$$

Table (VII) gives the results of Encryption quality of TDES, AES and chaotic for an image file (Plain Image), from the results we can conclude that confidentiality in chaotic using Lorenz system is higher than confidentiality using AES and TDES algorithms.

TABLE VII. ENCRYPTION QUALITY OF TDES, AES AND CHAOTIC

TDES	AES- key(256)	Chaotic System
665.2	667.7	669.4

VI. CONCLUSIONS

This paper presents an alternative encryption technique to provide confidentiality for PGP. The proposed cryptosystem is based on Lorenz chaotic generator and using random initial condition. The chaotic system for encryption is implemented using C#.net, open source bccrypto-net-1.7 project and sharp privacy for open PGP. Evaluation and comparison with standard mechanism are achieved using statistical test suites (NIST) for randomness tests and Matlab for encryption quality. The performance is evaluated in term of encryption/decryption time using C#. The results obtained indicate that encryption/decryption time is less than the encryption/decryption time in standard encryption algorithm. Also the result shows that chaotic system has good randomness properties and high quality encryption. The conclusion is that chaotic system encryption using Lorenz with random initial conditions enhances performance and security.

REFERENCES

[1] K. Jallad, J. Katz, and B. Schneier, "Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG," In Proceedings of the 5th International Conference on Information Security, pp. 90-101, 2002.

[2] J. Katz and B. Schneier, "A Chosen Ciphertext Attack against Several E-Mail Encryption Protocols," InProceedings of the 9th USENIX Security Symposium pp. 241-246, 2000.

[3] FIPS PUB197 "Advanced Encryption Standard (AES)," Federal Information Processing Standard (FIPS), Publication 197, National Institute of Standards and Technology, US

Department of Commerce, Washington D.C., November 26, 2001.

[4] X. Lai, J. L. Massey and S. Murphy, "Markov Ciphers and Differential Cryptanalysis", Advances in Cryptology– EUROCRYPT '91, Lecture Notes in Computer Science, Springer-Verlag, 1991:17-38.

[5] FIPS PUB 46-3, "Data Encryption Standard (DES)", Federal Information Processing Standards (FIPS), Publications (46-3), National Institute of Standards and Technology, US Department of Commerce, Washington D.C., October 1999.

[6] ANSI X9.52 – 1998, "Triple Data Encryption Algorithm Modes Of Operation", American National Standards Institute, July 29, 1998.

[7] L. Kocarev, S.Lian (Eds.), "Chaos-Based Cryptography-Theory, Algorithms and Applications", Studies in computational Intelligence vol. 354, Springer, 2011.

[8] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview," IEEE Circuits and Systems Magazine, vol. 1, pp. 6-21, 2001.

[9] M. Harada, Y. Nishio and A. Ushida, "A Cryptosystem Using Two Chaotic Maps," Proceedings of NOLTA'99, vol. 2, pp. 609-611, 1999.

[10] N. Masuda, K. Aihara, "Cryptosystems with discredited chaotic maps," IEEE Trans. Circuits and Systems I, vol. 49, pp. 28-40, 2002.

[11] R. Bose, "Novel public key encryption technique based on multiple chaotic systems," Phys. Rev. Lett., vol. 26, 2005.

[12] J. C. Sprott, "High-Dimensional Dynamics in the Delayed Hénon Map", Electronic Journal of Theoretical Physics 3, pp. 19-35, 2006.

[13] J. M. H. Elmirghani, R A. Cryan and S. H. Milner, "Performance of a novel echo cancellation strategy based on chaotic modulated speech," Proc. SPIE (special issue for chaotic circuits for communication), Oct. 1995.

[14] Sh. Li, X. Mou and Y. Cai, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", INDOCRYPT 2001, LNCS, Springer-Verlag, Berlin, 2001.

[15] O. E. Rossler, "An Equation for Continuous Chaos," Phys. Lett. A, vol. 57, no. 5, pp. 397-398, 1976.

[16] C. Sparrow, "The Lorenz Equations in Chaos," V. Holden. Princeton. University Press, Princeton, 1986.

[17] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series", Physica D 16 (1985) 285.

[18] T. Kilias, K. Kelber, A. Mogel and W. Schwarz, "Electronic chaos generators- Design and applications," Int. j. Electron. ,1995.

[19] The NIST Statistical Test Suite," URL:http://csrc.nist.gov" , 2005.

[20] Gregory Vert and Manaf Alfize, "An Enhanced Pretty Good Privacy (EPGP) System with Mutual Non-Repudiation", Security and Management CSREA Press (2006) , p. 364-370

[21] Behrouz A. Forouzan, "Cryptography and Network Security", McGraw-Hill Higher Education, 2008.

[22] Krishnamurthy G N, Dr. V Ramaswamy, "Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm using digital images", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009

[23] William Stallings, "Cryptography and Network Security Principles and Practice Fifth Edition", Prentice Hall, 2010.