Symmetric Encryption Algorithm for Data Security and Privacy using Linear Convolution Sum Technique

[1]Sangita Bhusare, [2]Dr. S B Thorat [3] G.B Chounste [4] Dr.P.A Kadam

[1] Assistant Professor, Department of Computer Science and IT, Yeshwant Mahavidyalaya, Nanded
[2] Director, Institute of Technology & Management, Nanded
[3]Assistant Professor, Department of Computer Science and IT, Yeshwant Mahavidyalaya, Nanded
[2] Assistant Professor, Institute of Technology & Management, Nanded

Abstract:
Security is major concern in data handling, communication, message transmission and electronic transaction on public network. Cryptography (secret writing) is the encryption process of transformation of messages to make information secure and resistant to attack. The idea of encryption algorithm which we can encode our data in secret code and not to be able readable by hackers or unauthorized person even it is hacked. Cryptography algorithms are two types such as symmetric and asymmetric key cryptography. This paper proposes a symmetric cryptographic algorithm to maintain Confidentiality of data from unauthorized person. The proposed algorithm is Symmetric Encryption algorithm which uses same key both for encryption and decryption. The proposed algorithm uses mathematical concept of convolution sum and deconvolution with the combination of Z-Transform for encryption and decryption.

Keywords: Encryption, Cryptography, Information Security, Decryption, Data Security.

1. INTRODUCTION

Security is major concern in data handling, communication, message transmission and electronic transaction on public network. Cryptography (secret writing) is the encryption process of transformation of messages to make information secure and resistant to attack. To protect valuable information from illegal access become evident. This is especially the case to maintain data confidentiality and privacy while transferring information on unsecured channel of public network.
The generic name for the collection of tools/algorithms designed to protect data and to prevent hackers is computer security.
Data security measures are needed to protect data during their transmission. One approach is to consider three aspects of information security: Security Attacks, Security Mechanism and Security service. [1]
In security attacks there is flow of information from a source, such as a file, or a region of main memory to a destination, such as another file or a user. Another part or attacks is Interruption, Interception, Modifications and Fabrication. These attacks are in terms of passive attacks and active attacks. Passive attacks are in the nature of eavesdropping on or monitoring of transmissions. The passive attacks are traffic analysis. Passive attacks are very difficult to detect because they do not involve any alteration of the data. Active attacks involve some modifications of the data stream. [2]
A cipher, or cryptographic algorithm, is the means of altering data from a readable form (also known as plaintext) to a protected form (also known as cipher text), and back to the readable form. Changing plaintext to cipher text is known as encryption, whereas changing cipher text to plaintext is known as decryption. [1,2]
A cryptographic algorithms is (also called encryption algorithms) a “mathematical algorithm, used in conjunction with a secret key, that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm. Such algorithms are also the basis for digital signatures and key exchange.”[1,2]

1.1. Cryptography Goals

Authentication: The authentication service is concerned with assuring that a communication authentic. The identity is not of the user, but of the cryptographic key of the user. Having a less secure key lowers the trust we can place on the identity.

Non-Repudiation: Non-repudiation prevents either sender or receiver from denying a transmitted message. Often, cryptographic tools are required to prove that a unique user has made a transaction request. It must not be possible for the user to refute his or her actions.

Confidentiality: Confidentiality is the protection of transmitted data from passive attack, with respect to the release of message contents, several levels of protection can be identified.

Integrity: As with confidentiality, integrity can apply to a stream of messages, a single messages or selected fields within a message.

Access Control: In the context of network security access control is the ability to limit and control the access to host systems and applications via communications links.

Availability: A variety of attacks can result in the loss of or reduction in availability.
The Cryptographic algorithms can be classified as Symmetric algorithms, asymmetric algorithms and hash algorithms.[1,2]
The proposed algorithm is Symmetric Encryption algorithm which uses same key both for encryption and decryption. The proposed algorithm uses mathematical concept of convolution sum and deconvolution with the combination of Z-Transform for encryption and decryption.

1.2. Symmetric Encryption

Symmetric encryption (see Fig.1) involves the use of a single secret key for both the encryption and decryption of data. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [1,2,21].
For example, a source produces a message in plaintext, X = [x_1,x_2,x_3,….,x_N]. For Encryption, a key is generated at the message source. Then the key is also provided to the destination by means of some secure channel. With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [y_1,y_2,y_3,…,y_N]. This may be written as Y = E_K(X).

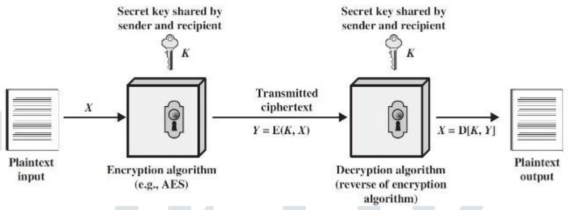
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1. Simplified Model of Symmetric Encryption [1]

Cipher text Y is produced by using encryption algorithm, where E indicates the encryption algorithm used and K indicates the key used for encryption. The receiver of this message should apply decryption algorithm with same key used for encryption to get the actual message X = DK[Y]. Here D indicates decryption algorithm.
Several symmetric encryption algorithms are available like Caesar Cipher, Playfair Cipher, Vigenere Cipher, Rail fence technique, Hill Cipher, Monoalphabetic ciphers, DES, AES, Feistel cipher and are used in information security. These algorithms can be categorized as Block and Stream cipher. These encryption algorithms are based on two general principles namely substitution cipher, in which each element in the plaintext is mapped into another element, and transposition cipher, in which elements in the plaintext are rearranged.[1,2]

2. Discrete Time Convolution

In mathematics and functional analysis convolution is a mathematical operation on two functions (f and g) to produce a third function that expresses how the shape of one is modified by the other. The term convolution refers to both the result function and to the process of computing it.
Generalizations of convolution have applications in the field of numerical analysis and numerical linear algebra, and in the design and implementation of finite impulse response filters in signal processing.
Convolution is a mathematical way of combining two signals to form a third signal. Computing the inverse of the convolution operation is known as deconvolution.[3]
Discrete time convolution is an operation on two discrete time signals defined by the integral

$$(f * g)(n) = \sum_{n=-\infty}^{+\infty} f(k)\, g(n-k) \quad \text{…..} \ (1)$$

for all signals *f*, *g* defined on Z. It is important to note that the operation of convolution is commutative, meaning that
$f*g=g*f$ …… (2)
for all signals *f*,*g* defined on Z. Thus, the convolution operation could have been just as easily stated using the equivalent definition

$$(g * f)(n) = \sum_{n=-\infty}^{+\infty} f(n-k)\, g(k) \quad \text{…..} \ (3)$$

for all signals *f*, *g* defined on Z.

3. Z-Transform and Inverse Z-Transform

In mathematics and signal processing, the Z-Transform converts a discrete-time signal, which is a sequence of real or complex numbers, into a complex frequency domain representation. It can be considered as a discrete-time equivalent of the Laplace transform. A special feature of the z-transform is that for the signals and system of interest to us, all of the analysis will be in terms of ratios of polynomials.
Given a finite length a discrete time signal x[n], the z-transform is defined as,

$$X(Z) = \sum_{n=0}^{N} X(n)\, z^{-n} \text{…..} \ (4)$$

Where the sequence support interval is [0, N], and Z is any complex number. This transformation produces a new representation of denoted by X(Z). Returning to the original sequence (inverse z-transform) requires finding the coefficient associated with the n^{th} power of Z^{-1}.

A sequence and its z-transform are said to form a z-transform pair and are denoted x [n] ^{Z} X (Z).
In the sequence or n-domain the independent variable is n. In the z-domain the independent variable is z. [3]

3.1. Convolution theorem for z transforms

The convolution theorem for z transforms states that for any (real or) complex causal signals x and y, convolution in the time domain is multiplication in the Z domain i.e.

If $x_1(n)\overset{z}{\leftrightarrow}x_1(z)$ and $x_2(n)\overset{z}{\leftrightarrow}x_2(z)$Then $x_1(n)*x_2(n)\overset{z}{\leftrightarrow}X_1(z)X_2(z)$ ……(5)

or

$$\boxed{x * y \;\leftrightarrow\; X \cdot Y}$$

or, using operator notation,

$$\mathcal{Z}_z\{x * y\} = X(z)Y(z),$$

[3]

4. PROPOSED ALGORITHM [25]

4.1. Encryption Algorithm

Followings are the steps in proposed encryption algorithm.

step 1. Read and Count the No. of character (N) in the plain text without space.

step 2. Convert the plain text into equivalent ASCII code. And form a one dimensional vector of size N.

i.e. X={x_1,x_2,x_3,….,x_N}

step 3. Read and convert key into equivalent ASCII code. Find length of KEY (M). Form a one dimensional vector of size M as above.

i.e. K={k_1,k_2,k_3,…,k_M}

step 4. Find the Z Transform of vector X.

i.e. $X(Z) = \sum_{n=0}^{N} X(n)z^{-n}$

step 5. Similarly Find the Z Transform of vector K.

i.e. $K(Z) = \sum_{n=0}^{M} K(n)z^{-n}$

step 6. Find the linear convolution sum of vector X and K by Z-Transform's "convolution property".

i.e. Y=X*K ^{Z} $Y(Z) = X(z).K(z)$

step 7. Find inverse Z-Transform of Y(Z) to get vector Y of size (N+M-1).

i.e. Y={y_1,y_2,y_3,…,$y_{(N+M-1)}$}.

4.2. Decryption Algorithm

To retrieve the original message, Decryption is necessary. Decryption is possible only with key values which are used for encryption. So key should have a vital role in encryption and decryption algorithm. Following steps illustrate the decryption algorithm.

step 1. Read encrypted text vector Y and KEY vector K.

i.e. Y={y1,y2,y3,…,y(N+M-1)} and K={k1,k2,k3,…,kM}.

step 2. Find the Z Transform of vector K.

i.e. $K(Z) = \sum_{n=0}^{M} K(n)z^{-n}$

step 3. Similarly Find the Z Transform of vector Y.

i.e. $Y(Z) = \sum_{n=0}^{(N+M-1)} Y(n)z^{-n}$

step 4. Find the deconvolution of vector Y and K by Z-Transform's "convolution property" as below.

i.e. X(Z)=Y(Z)/K(Z)

step 5. Find inverse Z-Transform of X(Z) to get vector X of size N.

step 6. Convert the ASCII code into character value.

Algorithm could be known to everyone but key should be known only to authorize user.

5. Implementation

We have implemented and compared DES, 3DES, AES and blowfish with proposed approach. We have implemented the algorithms in java using 'Net beans' IDE .We has used packages java security and java crypto. The packages java crypto and security provides security features like encryption, decryption, key generation, key management infrastructure, authentication and authorization features. We have used files of sizes 25KB, 50KB, 100KB consisting of text as input for encryption. The encrypted output of each file is saved as a file, which in turn is input for decryption. For sake of comparison we have used the same input files for all algorithms throughout the experiment. We have used a same system for all implementations and analysis work, so that memory and processor conditions remain same for all algorithms for comparison. Java crypto and security package contains the classes and interfaces that implement the Java security architecture. Using the libraries of these packages, we implemented and compared various cryptographic algorithms with proposed approach. The method of implementing algorithms using functions of java.security and javax.crypto package is as follows: Generate key using key generator class, create a cipher object with parameters algorithm name and mode, initialize the cipher created for encryption/decryption and perform encryption/decryption using doFinal() method.

6. Evaluation Parameters [22]

Each of the encryption techniques has its own strong and weak points. We compared and analyzed performance, strength and weakness of existing algorithms with proposed approach based on several features. Analysis is done with following metrics under which the cryptosystems can be compared are described below:

6.1. Encryption time

The time taken to convert plain text to cipher text is encryption time. In our experiment we have measured encryption time in milliseconds. Encryption time impacts performance of the system. Encryption time must be less making the system fast and responsive.

6.2. Avalanche effect

In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input the output changes significantly. This is also called avalanche effect. We have measured Avalanche effect using hamming distance. Hamming distance in information theory is measure of dissimilarity. We find hamming distance as sum of bit by bit XOR considering ASCII value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithm.

Avalanche effect = (hamming distance ÷ file size)

5.3. Entropy

Randomness is an important property in cryptographic processes because information should not be able to be guessed by an attacker. Entropy is measure of randomness in the information. It measures uncertainty in the information. In information security, we require security algorithms to yield high randomness in encrypted message, so that there is less or no dependency between key and cipher text. With high randomness, the relationship between key and cipher text becomes complex. This property is also called confusion. A high degree of confusion is desired to make it difficult to guess to an attacker. Entropy reflects performance of cryptographic algorithm. We calculate entropy using Shannon’s formula.

7. Results and discussions

Simulation results obtained after comparison for above parameters is shown in below tables. Table 1 shows encryption times (in Milliseconds) of Encryption Algorithms with different input file Size. The result shows that the proposed algorithm required less time. Table 2 shows Entropy values of Encryption Algorithms. The result shows that the proposed algorithm has good entropy. Table 3 shows the Avalanche effect of Encryption Algorithms. The result shows that the proposed algorithm has good avalanche effect also.

Table 1: Comparative encryption time (in Milliseconds) of Encryption Algorithms with Different input file size

Input size in (KB)	DES	3DES	AES	Blowfish	Proposed Approach
25 KB	206	219	213	194	121
50KB	218	223	234	206	143
100 KB	228	234	242	212	169

Table 2: Entropy values.

	DES	3DES	AES	Blowfish	Proposed Approach
Average entropy per byte of encryption	4	3.75	4	3.875	4

Table 3: Avalanche effect values.

	DES	3DES	AES	Blowfish	Proposed Approach
Average entropy per byte of encryption	7	8	16	8	12

CONCLUSIONS

The proposed algorithm uses mathematical concept of convolution sum and deconvolution with the combination of Z-Transform for encryption and decryption for providing strong security in message transmission by adding more complexity as compared to classical substitution and transposition cipher algorithms to increase Confusion and Diffusion in Cipher text. Proposed system will be an effective technique for the applications securing short messages while transferring it on internet.

REFERENCES

1. William Stallings, “Cryptography and Network Security: Principles & Practices”, Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.
2. Bernard Menezes, “Network Security and Cryptography”, Third edition, Cengage ISBN-13:9788131513491,2014.
3. Dimitris G Manolakis, John G. Proakis, “Digital Signal Processing : Principles, Algorithms, and Applications”, Fourth edition, PEARSON, ISBN: 9788131710005, 8131710009, 2007.
4. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)
5. Sharma, A., Singh, A.: Hybrid improved technique for data security and authentication for RDIF tags. In: IEEE International Conference on Signal Processing, Computing and Control (ISPCC2017)
6. Shahara Banu, T., Shajeesh, K.U.: Secure reversible data hiding technique on textures using double encryption. In: International Conference on Innovations in Information, Embedded and Communication System (ICIIECS 2017)
7. Tim Mather, Subra Kumaraswamy, and Shahed Latif “Cloud Security and Privacy”, O‟Reilly Media, Inc, pp 61-71, 2009.
8. Mohit Marwaha, Rajeev Bedi, “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, pp 367-370, 2013.
9. V.U.K. Sastry, N. Ravi Shankar and S. Durga Bhavani, “A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration”, International Journal of Network and Mobile Technologies, pp 45-53, 2010.
10. Quist-Aphetsi Kester, “A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher”, International Journal of Advanced Technology & Engineering Research (IJATER), Volume 3, Issue 1, pp 141-147, 2013.
11. Nagaraj, S., Raju, G., Srinadth, V.: Data encryption and authetication using public key approach. Procedia Comput. Sci. 48, 126–132 (2015)
12. Hellman, M.: A cryptanalytic time-memory trade-off. IEEE Trans. Inf. Theory 26(4), 401–406 (1980)
13. Lee, G.W., Hong, J.: Comparison of perfect table cryptanalytic tradeoff algorithms. Des. Codes Cryptogr. 80(3), 473–523 (2016)
14. Oyetola Oluwadamilola, K., Okubanjo Ayodeji, A., Osifeko Martins, O.: An improved authentication system using hybrid of biometrics and cryptography. In: International Conference on Electro-Technology for National Development (NIGRCON) (2017)
15. Harini, M., Pushpa Gowri, K., Pavithra, C., Pradhiba Selvarani, M.: A novel security mechanism using hybrid cryptography algorithm. (ICEICE2017) .
16. Rachmawanto, E.H., Amin, R.S., Setiadi, D.R.I.M., Sari, C.A.: A performance analysis Stego Crypt algorithm based on LSB-AES 128 bit in various image size. In: International Seminar on Application for Technology of Information and Communication (iSemantic2017)
17. D’souza, F.J., Panchal, D.: Advanced encryption standard (AES) security enhancement using hybrid approach. In: International Conference on Computing, Communication and Automation (ICCCA2017)
18. Ebrahim, M.A., El-Maddah, I.A.M., Mohamed, H.K.: Hybrid model for cloud data security using steganography. @2017 IEEE
19. Tian, Y., Gu, D., Gu, H., Ding, N.: Improved cryptanalytic of time-memory trade-off based on rainbow table. In: ICINS 2014, 2014 International Conference on Information and Network Security, Beijing, pp. 97–104 (2014)
20. Hong, J., Moon, S.: A comparison of cryptanalytic tradeoff algorithms. J. Cryptol. 26(4), 559–637 (2013)
21. Mohit Marwaha, Rajeev Bedi, “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, pp 367-370, 2013.
22. Priyadarshini Patila, Prashant Narayankar, Narayan D G, Meena S Md “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish”, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.
23. C. Giolli, A. Scrivani, G. Rizzi, F. Borgioli, G. Bolelli, and L. Lusvarghi, “Failure mechanism for thermal fatigue of thermal barrier coating systems”, Journal of Thermal Spray Technology,vol.18,pp.223–230,2009.
24. C. Zhou, Q. Zhang, and Y. Li, “Thermal shock behavior of nanostructured and microstructured thermal barrier coatings on a Fe-based alloy”, Surface & Coatings Technology,vol.2170–75,2013.
25. Sangita Bhusare, Dr.Suryakant Thorat,” Symmetric Encryption Algorithm for Data Security and Privacy using Linear Convolution Sum Techniques”, International Conference on Science, Technology ,Engineering and Management (ICSTEM), AE-ICSTEMBOSTON 16108-001.