An Enhanced Approach to Secure Message Using Combination of Symmetric and Asymmetric Cryptography and Triangulation Method

Tanusree Saha
Department of Information Technology
JIS College of Engineering, Kalyani, W.B, India

Abstract: Cryptography is the practice and study of Encrypting/Decrypting information. In this era of information processing where all transaction is digitized, information security becomes an essential issue for every aspects of digitization. The process of securing information means protecting the information from non-repudiation, maintaining its integrity and make it secure. Access to stored information on computer increased .hence there is a strong demand of securing information that is passing via network. The channel through which information is passing should be secured as well as the information itself should be strongly encrypted.

In this paper I have proposed an enhanced encryption algorithm which is the combination of both symmetric and asymmetric encryption techniques together with triangulation method through which each character of the message will be strongly encrypted by no. of steps such as substitution techniques, triangulation method and at the end with RSA text encryption algorithm, depending on the ASCII value of each character of the message so that its integrity and security will be maintained while it will transmit via some network channel. Our proposed method is easy to adopt the coding of advance language and is safe enough.

Keyword: Cryptography, RSA, Substitution, Triangulation, ASCII.

I. INTRODUCTION

Cryptography is the science of keeping data secure. Encryption is the process of using cryptography to encode data or information so that no unauthorized user can access the data .For ensuring the security; the plain text is converted to cipher text by the sender. This process is called encryption. Decryption is exactly reverse process of encryption by which intended user can decode the message to its original form .Now a day's Different mathematical schemes and algorithms are there to scuttle the content of the message. . In this paper, an enhanced multi-level encryption decryption algorithm is introduced which is a combination of exixting asymmetric encryption algorithm like RSA and Symmetric encryption technique like Substitution along with triangulation technique, so that it will more secure and protect the confidentiality and integrity of the information being transmitted.

II. RESEARCH and REVIEW

Cryptography is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Purpose of Cryptography:

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

*Confidentiality:-*Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

*Authentication:-*The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

Integrity: - Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

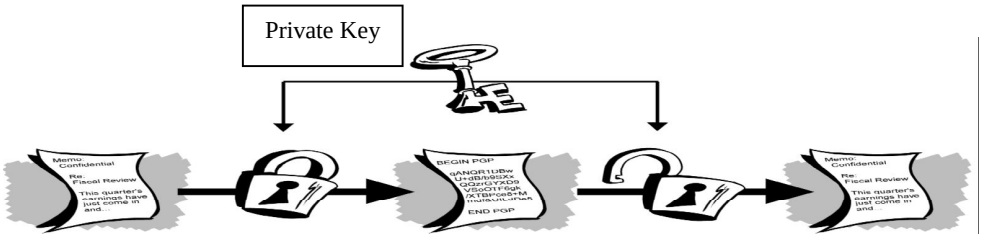
Non Repudiation: - Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control:- Only the authorized parties are able to access the given information.

Conventional Cryptography or Symmetric key Cryptography:

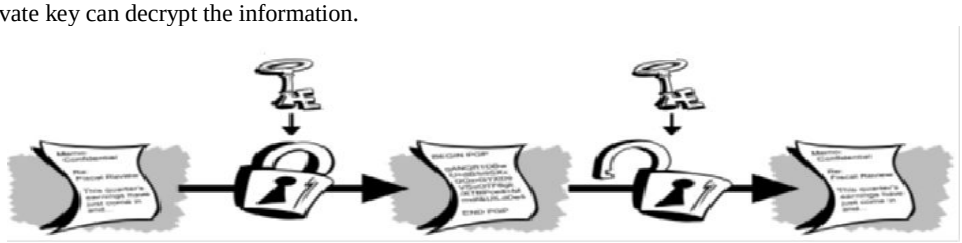
In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government.

Following figure is an illustration of the conventional encryption process:



Public key cryptography or Asymmetric key Cryptography:

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.



Existing Cryptographic Techniques/Method used :

- *Substitution Method:* In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution

  If key is three, then each character will substituted like following manner and we get cipher

plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

If key is four then it will be like this:

plain	a	b	c	d	e	f	g	h	i	j	k	L	m	N	o	p	q	r	s	t	u	v	w	x	Y	z
Cipher	e	f	g	h	i	j	k	l	m	n	o	P	q	R	s	t	u	v	w	x	y	z	a	b	C	d

For Example Plain Text JISCE

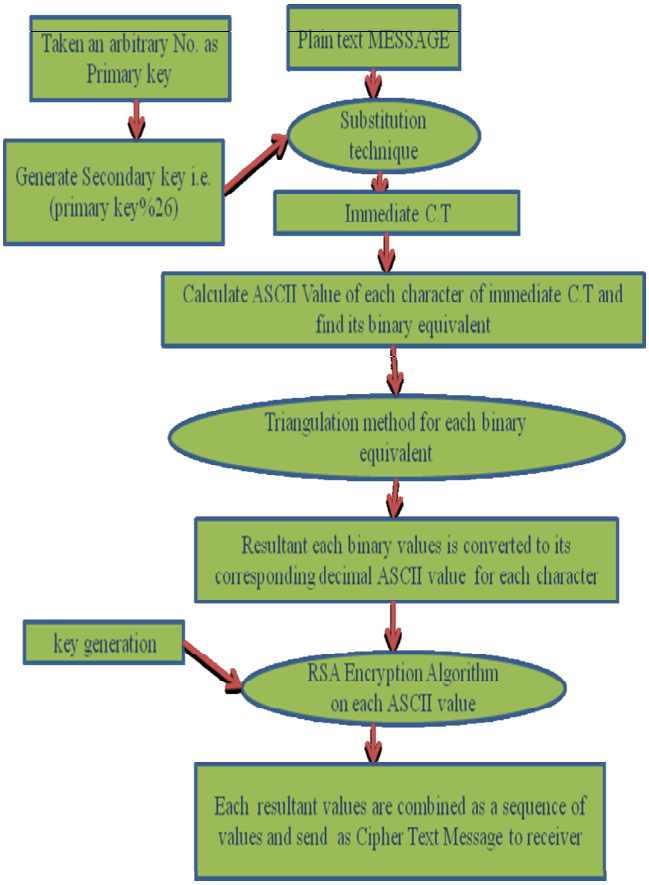
Cipher Text MLVFH

- *Triangulation Method:*Algorithm

Initially an n bit data string is taken. After this, we consider the steps discussed below.

1. The data string initialized is taken as it is.
2. Bit wise XOR operation is performed of all the bits; however, the MSB is not kept constant .This step is considered as the 1st iteration.
3. The iteration process is continued until the data string is reduced to a single bit.
4. The MSB's from the data string obtained from each of the iterations and are then joined together and taken as the new output.
5. If we take the new output as the data string, and perform the above mentioned steps, i.e, step1-step4, we get the original output.

The implementation of the above algorithm is shown
Using the previous data string example.
The data string taken is 1 0 0 0 1 1 0.
1 1 0 0 1 1 0
0 1 0 1 0 1
1 1 1 1 1
0 0 0 0
0 0 0
0 0
0
The output string obtained is 1010000.



Block Diagram Representation

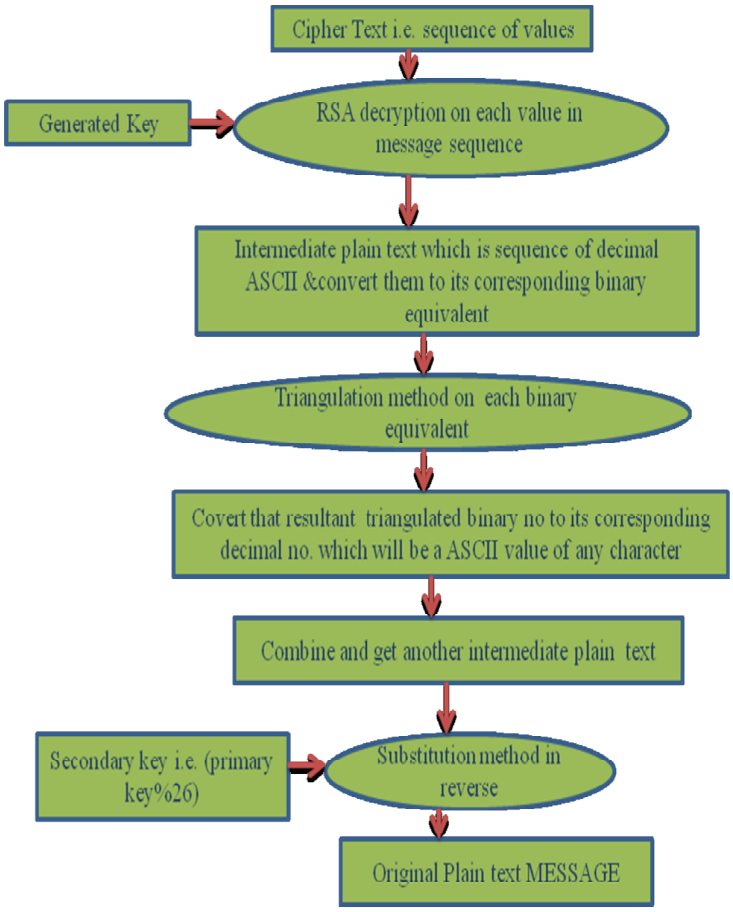
Now, this data string is taken as the new data string, and triangulation is performed on it.
1 0 1 0 0 0 0
1 1 1 0 0 0
0 0 1 0 0
0 1 1 0
1 0 1
1 1
0
The output data string obtained is 1100110,
which is the actual data string.
RSA Algorithm: The RSA public key cryptosystem was invented by R. Rivest, A. Shamir and L. Adleman. The RSA cryptosystem is based on the dramatic difference between the ease of finding large primes and the difficulty of factoring the product of two large prime numbers (the integer factorization problem).
RSA algorithm for encrypting and decrypting messages as follows:
Choose p = 3 and q = 11
Compute n = p * q = 3 * 11 = 33
Compute $\varphi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. Let e = 7
Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is d = 3 [(3 * 7) % 20 = 1]
Public key is (e, n) => (7, 33)
Private key is (d, n) => (3, 33)
The encryption of m = 2 is c = 27 % 33 = 29
The decryption of c = 29 is m = 293 % 33 = 2

III. PROPOSED ALGORITHM

Encryption Algorithm:

Algorithm Description

1. Take a random number as a primary key which is not a prime no.
2. A secondary key will be calculated as primary key%26.
3. Using secondary key every character of the plain text will be substituted by another character.
4. Determine ASCII value of the substituted character and find out their binary equivalent.
5. Use triangulation method i.e. bitwise XOR operation between bit of stream of ASCII value of each character of immediate cipher text, and result will be the leftmost bit of each step after XOR operation done with the bits
6. We convert the resultant triangulated binary number to decimal ASCII Value for each character of the message.
7. The ASCII value of each character of the 2nd immediate cipher text is further encrypted using RSA asymmetric key algorithm.
8. After encryption using RSA algorithm resultant encrypted ASCII's combine to get ultimate cipher text of the message and send to receiver.



Block Diagram Representation

Decryption Algorithm:

Algorithm Description

Decryption is the reverse process of above encryption process

1. Using RSA Decryption method we find out the immediate decrypted message, which are some ASCII values from final encrypted message.
2. All ASCII's are converted to its binary equivalent.
3. On each binary stream of ASCII value we use Triangulation method i.e. bit wise XOR operation and the result will be the leftmost bit of each step after XOR operation.
4. Covert that triangulated binary no to its corresponding decimal no. which is an ASCII value of any character and find out 1st immediate plain text.
5. Using secondary key (i.e. primary key %26) perform reverse substitution and each character will be substituted by another character.
6. Combine the character and finally get original plain text.

IV.CONCLUSION

I have proposed this method by using both symmetric and asymmetric encryption technique to ensure a secure, simple and fast cryptographic system for secure message. No doubt the security aspects to be examined thoroughly, but with the achieved efficiency if security measure is found adequate, it would enable us to secure message which is passing over a non-secure channel without considerable overhead. Thus it will provide efficient data security.

REFERENCES

[1] R. L. Rivest, A Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems, Communications of the Association for Computing Machinery, vol 21, no. 2, pp 120-126

[2] B.Scheier, Applied Cryptography : Protocols, Algorithms and Source Code in C,2nd ed.., John Wiley & Sons, 19995.

[3] B. Pfitzmann. Information hiding terminology. in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 347-350, 1996.

[4] W. Stallings, Cryptography and Network Security: Principles and Practices, 5th ed., Prentice Hall, 1999.

[5] Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhound — Performance Evaluation of Symmetric Encryption Algorithm —, IJCSNS, 2008

[6] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha — Performance Evaluation of Symmetric Cryptography Algorithms, IJECT, 2011.

[7] 2011-01-01 Cryptography and Steganography: New Algorithms and Applications Jonathan BlackledgeDublin Institute of Technology, jonathan.blackledge@dit.ie

[8] Vishwa gupta,. Gajendra Singh ,.Ravindra Gupta- Advance cryptography algorithm for improving data securityVolume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[9] K.S.S.Narayan,G.Veereswara Swamy- A Newly Established Symmetric Key Encryption Algorithm for Small Amount of Datahe IUP Journal of Information Technology, Vol. VIII, No. 4, pp. 60-65, December 2012

[10] Cryptography and network security-Atul Kahate ISBN 0-07-049483-5. Published by TaTa McGraw-Hill Publishing Co.Ltd.

[11] J. K. Mandal, S. Dutta, "A 256-bit recursive pair parity encoder for encryption", Advances D -2004, Vol. 9 nº1, Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE, France), www. AMSE-Modeling.org, pp. 1-14