www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-2, June- 2013
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security

V. Kapoor

Department of Information Technology
Institute of Engineering and Technology, DAVV, Indore, India

*vkapoor13@yahoo.com

Received: 03 May 2013 Revised: 17 May 2013 Accepted: 15 June 2013 Published: 30 June 2013

Abstract: Information is a valuable asset. As an asset information needs to be secured from cryptanalysis attacks. Security by encoding a message to make them non readable is the art and science of cryptography. Cryptographic algorithms are computationally rigorous function and guzzle a large amount of CPU time and space complication at the time of encryption. In this research paper we have proposed a reliable, an efficient and a more secure system by using our proposed algorithm for encryption and decryption. The Encryption key is long and consists of 128 bits. In cryptography, information should be confidential not only when it is stored in the computer, it should maintain its confidentiality when it is transmitted from one computer to another. For this purpose here we proposed an integrated cryptographic scheme. This scheme is based on a new cryptographic algorithm, message digest algorithm MD5 and RSA Algorithm. Proposed Encryption Algorithm is used to achieve confidentiality, whereas Message Digest Algorithm MD5 is used to verify the integrity of the message. RSA is adopted to encrypt the key of the encryption algorithm and to generate the digital signature. Four major security principles such as Authentication, Confidentiality, Integrity of Data and Non-Repudiation are achieved together using this scheme.

Keywords: Brute-force attack, Cryptography, Cryptographic algorithm, Encryption key, Information Security.

1 Introduction

Main Cryptography is the study of information hiding and verification. It is usually referred to as "the study of secret" when data exchanged over the internet or other media. It's the Art of protecting Information from unauthorized access by transforming it into a non readable format, called cipher text. Only those who possess a secret key can decipher the message into plain text. It includes the protocols, algorithms and strategies to secure and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

The original message from sender to receiver called Plain Text and the message that is sent through the channel is called Cipher Text. Cryptography has two processes; Encryption and Decryption. The process to create a plain text into cipher text called Encryption and reverse the process, to create a plain text from Cipher called Decryption. The encryption process consists of an algorithm and a secret key. The key controls the algorithm. Depending upon the secret key used, the algorithm will produce a different output. If the secret key is changed then the output of the algorithm is also changing.

Secret key used in the Encryption algorithm to create Cipher text from plain text called Encryption key and the key used in a decryption algorithm to create plain text from cipher text is called Decryption key. Cryptography is divided into two categories depending on what keys are used. First is Symmetric key cryptography (same key is used for encryption and decryption) and the second one is asymmetric key cryptography (two different keys are used as one for encryption and another for decryption).

Four chief principles of security are confidentiality, integrity of data, authentication and non-repudiation [2, 3, 18, 19, 20]. Confidentiality ensures that only authorized set of people can access the information. Authentication allows the recipient of information to confirm the sender's identity, that is, to determine its origin. Integrity provides a condition in which data has not been altered or destroyed in an unauthorized manner. Non-repudiation ensures that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. If any cryptographic algorithms providing security of information then they must be to satisfy the security principles.

The different types of information and their importance create the need for different types of encryption that could efficiently handle the transmitted data, so various encryption algorithms are presented, such as RSA, DES, AES etc. Due to lots of mathematical operations efficiency of existing algorithms has decreased [1]. The performance and security issues have considered in the proposed work.

© 2013, IJSRNSC All Rights Reserved

This paper is formatted as section II describes related work, section III describes proposed algorithm and scheme, section IV describes the future aspects related to this paper work and conclusion.

2 Related Work

Security issues are ubiquitous. Both senders as well as receiver faces the security issues. This section describes the existing work.

To achieve confidentiality encryption algorithms are used. Mathur [7] proposed an encryption and decryption algorithm based on the ASCII values of the plain text characters. These ASCII values are used to encrypt data. This is a symmetric key encryption algorithm as the same key is used for encryption and decryption , but this algorithm operates when the length of the input and the length of key are same. In this algorithm secret used will be modifying another string, then for encryption and decryption theses string is used as a key.

Ron Rivest, Adi Shamir and Leonard Adleman (RSA) Algorithm [2, 9, 18] is most common and proven asymmetric key cryptography algorithm. In asymmetric key cryptography two different key public key and private key are used for encryption and decryption respectively. Asymmetric key cryptography is also known as Public key cryptography. In RSA private and public keys are based on very large prime numbers [2]. Encryption and decryption use modular exponentiation. Modular exponentiation is feasible in polynomial time using the fast exponentiation algorithm. However, modular logarithm is as hard as factoring the modulus, for which there is no polynomial algorithm yet [9]. In other words, the sender uses a one-way function (modular exponentiation) with a trapdoor known only to the receiver. An attacker, who does not know the trapdoor, cannot decrypt the message.

Principal of Authentication is achieved by using the concept of Digital signature [2, 9]. Same as, signature on a document, if authentic, means that the document is probably authentic. The digital signature is used for the authentication of a digital data. A digital signature needs a public-key system to use the private and public key of the sender, while in the case of encryption and decryption private and public key of the receiver is used [9]. A digital signature is a means by which the sender can electronically sign the data by using a process that involves showing that sender owns a private key related to the public key that has been announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message [9].

Another security principle, named as non-repudiation, is also provided by the digital signature. Repudiation by either sender or the receiver of data is protected by the non-repudiation service. In non-repudiation with proof of the origin, the receiver of data can later prove the identity of the sender if denied [2, 9].

The message digest, also called as hash, is used to verify the integrity of data. A message digest is a fingerprint or a summary of a message [2]. Message digest takes an arbitrary block of data and return a fixed-size bit string, such that it is infeasible to recover a message from its hash [8]. Any accidental or intentional change to the data will return a totally different hash value and comparing this hash value with the hash value of the original data, the receiver can easily verify the integrity of receiving data.

3 Proposed Work

To achieve all four described security principle, this section proposed a new cryptography algorithm with an integrated scheme to improve data security. The cryptographic algorithm uses an integrated scheme to achieve authentication, integrity and non repudiation with improved confidentiality, when a given data is sent from sender to receiver. The proposed integrated scheme includes MD5, RSA with this new cryptography algorithm to strengthen the security of transmitted data. RSA is used to solve the key distribution problem and in addition to this, MD5 to verify the integrity of the message [11].

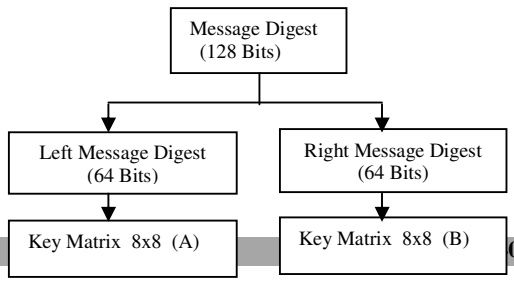
A. Keys Generation Module

This module includes MD5 algorithm and Key matrix generation process.

1. *MD5 Algorithm:* A truly safe system is "one time one key" but it is difficult to do so [12], but by using message digest we can create "one key for one message". A message digest algorithm MD5 is used to generate message digest of Plain Text. Message digests refer to the representation of a text in the form of a fixed size string and for each different message, there are totally different key pairs are generated in Key generation process. An input plain text to the MD5 algorithm generates a 128 bit output as a message digest.

2. *Key matrices generation process:* The output of MD5 is sent to the key matrices generation process. In this process, these 128 bits are divided into two equal halves, (A) and (B), of 64 bits. This first and second half, each of 64 bits, are organized in two matrices consist of size 8x8 and named as Key matrix (A) and Key matrix (B) respectively. The key matrices generation process is shown in figure 1.

Figure 1: Key matrices generation process



© 2013, IJSRNSC All Rights Reserved

B. Data Encryption/Decryption using Proposed Encryption/Decryption Algorithm

A new encryption and decryption algorithm are used to perform the encryption and decryption. This algorithm takes 128 bits plain text as input and generates 128 bits cipher text as output. In this encryption algorithm both, Key matrix (A) and Key Matrix (B) are used for encryption and decryption. The algorithm uses a series of logical operation like XOR, left circular shift and right circular shift. It already known that all the selected operation is very simple and very effective.

Decryption just reverses the process of encryption. In this algorithm, 128 bit cipher text is used as input to generate the 128 bits plain text as output by using the same Key matrix (A) and Key matrix (B) and the series of logical operation that are used in encryption.

C. Keys encryption using RSA

The RSA algorithm is the public key cryptographic algorithm. In Public key algorithm public-private key pair is used for encryption and decryption [11]. It can be used for data encryption, by using the key pair of the receiver, and also can be used for digital signature algorithm, by using the key pair of sender.

However, it is far slower and produces hug chunks of cipher text as compared to symmetric key cryptography [2], RSA is used to resolve the key distribution problem for the proposed encryption algorithm where same keys are used for encryption and decryption.

D. Integrated Scheme used in the algorithm

Three different encryption algorithms are used there in our proposed cryptosystem. By combining all in one it provides confidentiality with integrity, authentication and non-repudiation. Proposed encryption algorithm is used for encrypting the data to achieve confidentiality, whereas a wide key space (128 bits) is provided by using the message digest as a key and the second purpose is data integrity. Moreover, encrypting a message digest with a private key creates a digital signature, which is an electronic means of authentication [10]. Key distribution problem between sender and receiver is resolved by using the RSA algorithm in proposed integrated scheme.

E. Verification Process

This module performs the integrity verification of the received message. Checking of integrity is the important security service. In Integrated Encryption Scheme sender is A, the receiver is B. A's public key is A_p, and Secret key is A_s, B's public key is B_p and Secret key is B_s. (We assuming that the two sides of communication know each RSA public key A_p and B_p). RSA algorithm overcomes difficulty of key distribution/agreement. 128 Bit MD is encrypted by RSA Algorithm with receiver Public key and produces Cipher text of Key ($C_{k)}$.

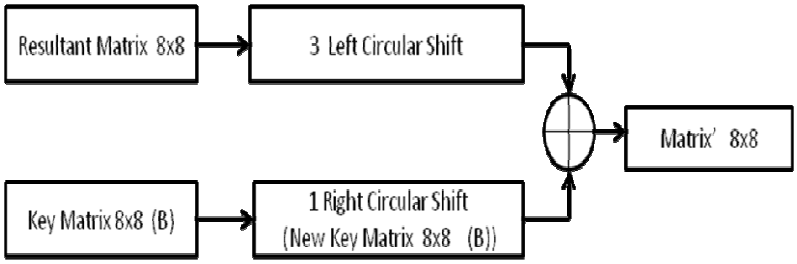
4 Research Methodology

This research methodology includes following processes.

A. Encryption process

To perform the encryption approach, an integrated hybrid scheme is used with encryption algorithm. 128 bit plain texts are displaced one by one and start performing the encryption.

Figure 2: Function F used in Encryption Algorithm



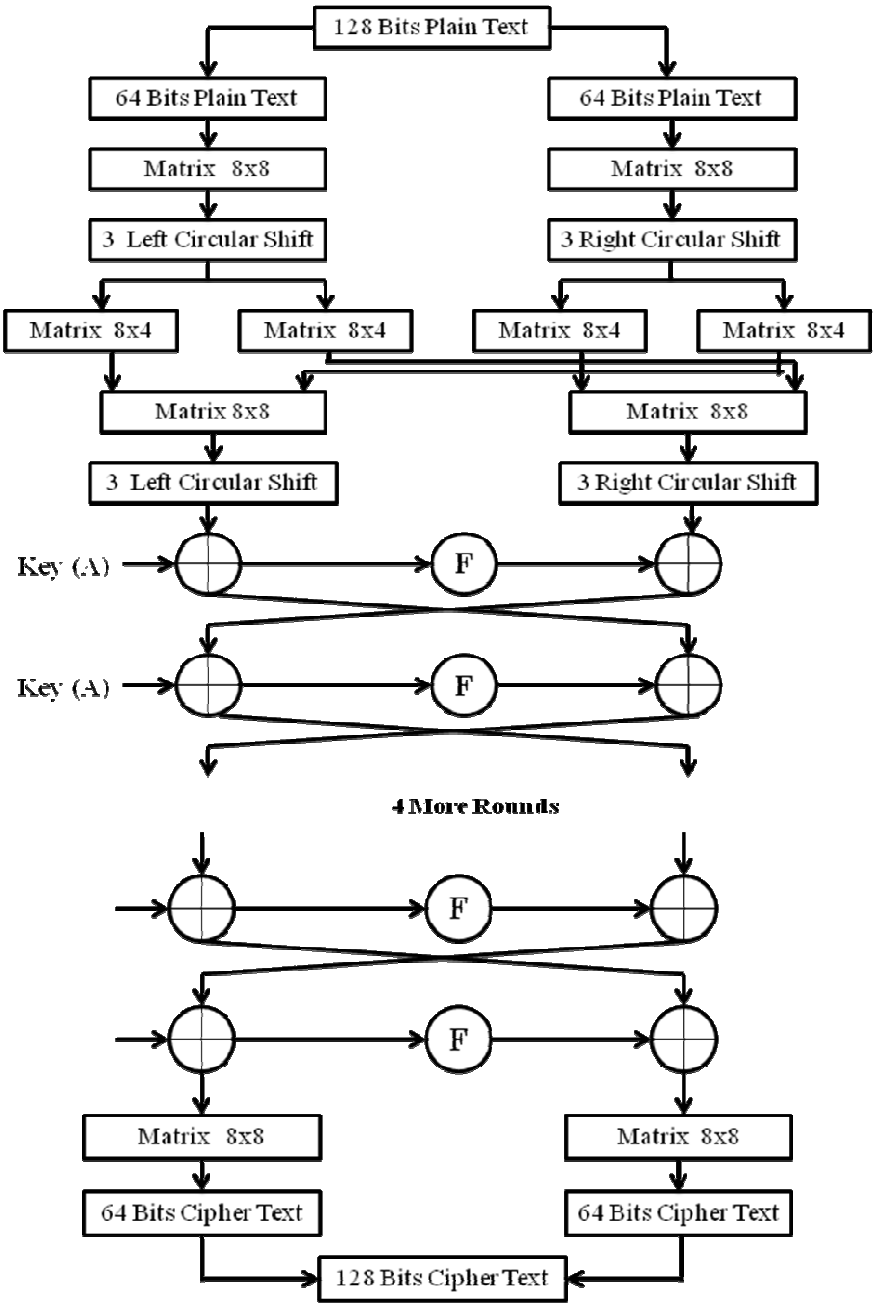
The block diagram of function F, used in encryption algorithm is depicted in figure 2. Function F performs logical XOR between 3 left circular shifts on an input matrix (8x8) and 1 right circular shift on key matrix (B), and generates a 8x8 matrix as output. In next round, before performing the XOR operation, we use this 1 right circular shifted key matrix (B) as a new key matrix (B), means next time again 1 right circular shift logical operation is perform on this right circular shifted matrix so total 2 right circular shift will be there on Key Matrix (B) in second round to perform the XOR operation and in third round one more XOR operation will be there on Key Matrix (B) and so on.

Like key generation process, in proposed algorithm first half and second half of plain text bits are converted into two 8x8 matrices. Three left circular shift and three right circular shifts operation is performed, on each and every row, of first and second matrix respectively. Now, as shown in the figure 3, last four columns of each matrices are swap with each other and again three left circular shift and three right circular shift operation is performed, on each and every row, of first and second matrix respectively.

© 2013, IJSRNSC All Rights Reserved

Then it uses 8 rounds to generate, two 8x8 cipher text matrices (each of 64 bits) as first and second half of 128 bits cipher text.

Figure 3: Block Diagram of Proposed Encryption Algorithm

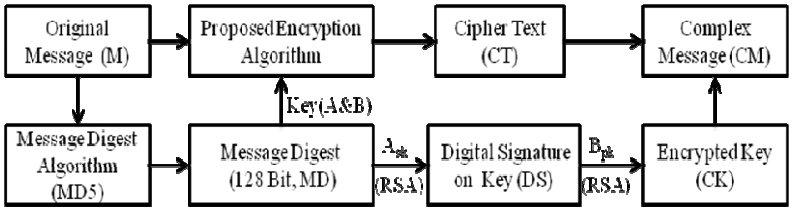


An integrated hybrid approach is performs on the output of 128 bit cipher text as following:

1. MD5 algorithm computes the 128 bits Message Digest (MD) of plain text.
2. Proposed encryption algorithm encrypts the original message (M) with the help of MD as symmetric key used in algorithm and then produce a cipher text (CT).
3. The MD encrypted by RSA Algorithm with sender's secret key A_{sk} to generate digital signature (DS) on key.
4. Now, DS is again encrypted by using RSA algorithm with receiver's public key B_{pk} and produce cipher text of Key (CK).
5. Combine a Cipher Text (CT) and Cipher text of Key (CK), produces a Complex Message (CM). Complex Message (CM) is sent to Receiver B.

Figure 4: Block diagram of sender side encryption process

© 2013, IJSRNSC All Rights Reserved



a) Sender Side Encryption Algorithm

1. Take Text Message M as input.
2. Compute MD
   MD5 (M) = MD
3. MD = K
4. $E_k(M) = CT$
5. Encrypt Key K with RSA
   $E_{Ask}(K) = DS$
6. Encrypt DS with RSA
   $E_{Bpk}(DS) = CK$
7. CK + CT = CM
8. Send CM to Receive.
9.

B. Decryption Process

To perform the decryption approach, an integrated hybrid scheme is used with decryption algorithm.

Decryption process is just reverse of encryption, and Function F' is used instead of function F. Function F' performs logical XOR between 3 left circular shift on an input matrix (8x8) and key matrix (B) to generate a 8x8 matrix as output. After the XOR operation 1 left circular shift is perform on key matrix (B) and then this new 1 left circular shifted key matrix work as Key matrix (B) for next round and so on. Block diagram of function F' is shown as following in figure 5.

Figure 5: Block Diagram of function F'

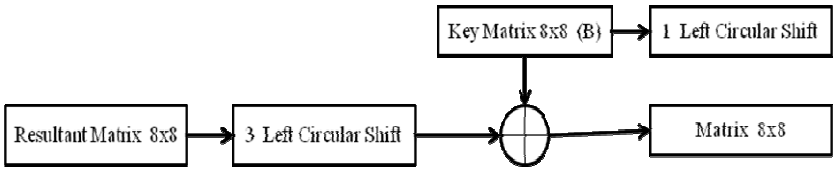
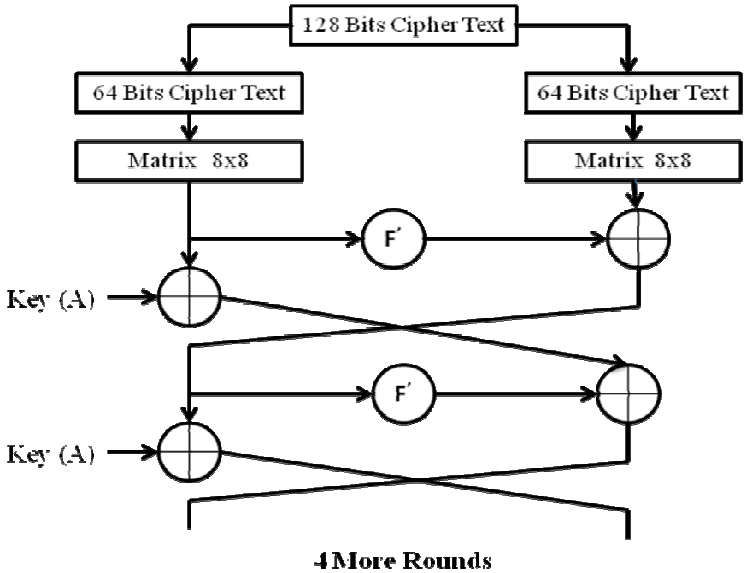
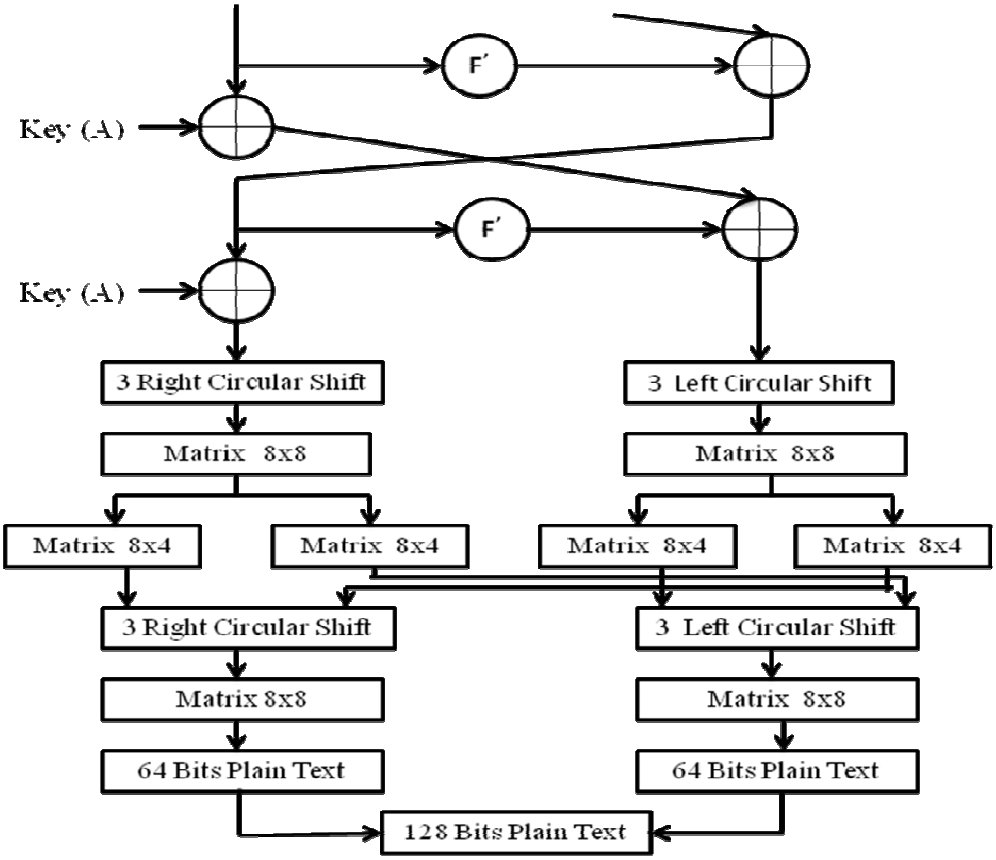


Figure 6: Block Diagram of Proposed Decryption Algorithm



© 2013, IJSRNSC All Rights Reserved



128 bit cipher texts are displaced one by one and start performing the decryption. Figure 6 is showing the block diagram of proposed decryption algorithm.
An integrated hybrid approach is performs on the output 128 bit plain text as following:

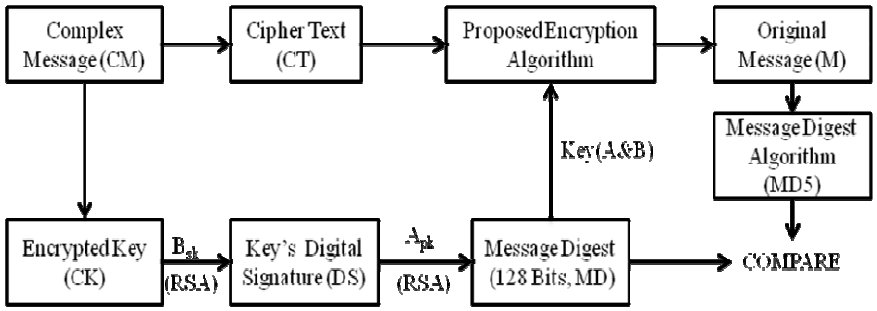
1. The receiver B received Complex Message (CM) in two parts, one is cipher text CT from proposed encryption algorithm and the other is cipher text of Key (CK) from the RSA algorithm encryption.
2. The receiver B decrypts cipher text of Key (CK) by their own private key B_{sk} and receives the digital signature (DS).
3. Now, DS is again decrypted by RSA Algorithm with sender's public key A_{pk} and receives the key (MD).

Decrypt the cipher text (CT) to obtain the original message (M) by using the MD as symmetric key in proposed decryption algorithm.

b) Receiver Side Decryption Algorithm

1. Receive CM
2. D_{Bsk} (CK) = DS
3. D_{Apk} (DS) = K = MD
4. D_K (CT) = M

Figure 7: Block diagram of receiver side Decryption process



© 2013, IJSRNSC All Rights Reserved

C. Verification Process

1. Calculate the MD of Original Message (M) by using MD5 algorithm.
2. Cipher text of Key (CK) decrypts by RSA algorithm with the help of Receiver's secret key B_{sk} to receive the digital signature DS.
3. Now, DS is again decrypted by using RSA algorithm with sender's public key A_{pk} and produce a secret key, it is also a MD.
4. Compare both MD.

c) Integrity Verification Algorithm

1. MD5 (M) = MD
2. MD = K
3. Compare Step 2 with decrypted key from decryption algorithm i.e. both MD.
4. If found equal.
5. Then accept
   Else;
   Reject message.

5 Conclusion and Future Work

Proposed algorithm uses a series of very simple and efficient logical operation like XOR, Left circular shift, Right circular shift, so it is less multifarious and expected to be more efficient. Due to less convolution and simple substitution and transposition techniques it may consumes less time to generate the cipher from plain text and vice versa. It is already known that as key size increases time for brute force attack also augment exponentially. A sufficient long symmetric key makes the line of brute-force attack impractical [21]. There are total 2^n keys are possible with a key of size n bits. As n increases, 2^n grows very exponentially. According to Moore's law, in every 18 to 24 months computing power doubles roughly but currently the larger security key lengths consider satisfactory well out of reach from this doubling effect. Avalanche effect and wholeness are two desired property of block cipher [9]. Using the message digest as key and logical operation like circular shift (left & right) provides Avalanche effect and wholeness to the algorithm. One more advantage of implementing this research work is that it achieves all four main security principles i.e. Confidentiality, Authentication, Integrity and Non-repudiation, in a single cryptographic scheme.

One of the strongest security solutions for confidential information is cryptography, but developing a cryptosystem must take many factors into consideration. Various issues of implementing text encryption are examines in this research work and recommendations have been made. Moreover, by combining to all three different encryption algorithms in one, this work presenting a common next of kin between them. Proposed encryption schemes preserve the Integrity, Authentication, Non-repudiation and Confidentiality of data. It uses a series of very simple and effective logical operation, so it is less complex and expected to more efficient. Using the message digest as key provides a wide key space and integrity for the message. Longer key length will always support to good security features, 128 bits key are used there to provide too much security in proposed algorithm.

In our future work there are other important issues related with research: first, Comparing results of proposed system with the results of existing system using traditional algorithms, second improvement in the present cryptosystem to achieve the better results i.e. less encryption/decryption time, efficient etc. in performance and security perspective, third, using the methods for access control and availability to control the access and availability for all parties using the information; and finally indexing and joining between different information. This proposed work would be inspiring for secure transmission of PDF file, video file, image file, etc.

References

[1] Bhatele, K. Sinhal, A.; Pathak, "A novel approach to the design of a new hybrid security protocol architecture" Advanced Communication Control and Computing Technologies (ICACCCT), **2012** IEEE International C0nference on page(s): 429-433 Print ISBN; 978-1-4673-2045-0

[2] Atul Kahate, Cryptography and Network Security Second Edition.

[3] Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh, "Efficient and High Performace Parallel Hardware Architecture for the AES –GSM" IEEE Transaction On Computers, vol.61,no.8, August **2012**.

[4] Introduction of cryptography by H. Delfs and H. Knebl springer Verlag berlin Heidelberg **2007**.

[5] Henry Beker & Fresd piper, "Cipher System, the protection of communications", A willey inter-science publication **1982.**

[6] El-Mageed, T., Hamdy, N., Amer, F., and Kerisha, Y.,"Cipher System and Cryptanalysis Techniques: An overview of the basic principles". The Egyptian Computer Journal, ISSR, Cairo UNIV, VOL (28), No.1,**2000.**

[7] Akanksha Mathur, "A Research paper: An ASCII value based datta encryption algorithm and its comparision with other symmetric data encryption algorithms", International journal on Computer Science and Engineering (IJCSE). Vol. 4 No. 09. Pp. 1650-1657, September **2012**.

[8] http://en.wikipedia.org/wiki/Cryptographic_hash_function

[9] Behrouz A. Forouzan: "Cryptography and Network security" McGraw Hill companies (special indian edition, Science, **2011**)

[10] http://www.webopedia.com/TERM/M/message_digest.html

[11] Trishna Panse, V. Kapoor, "An Integrated Scheme based on Triple DES, RSA and MD5 to Enhance the Secutity in Bluetooth Communiation", International Journal of Computer Applications, Vol. 50- No.7, July **2012**

[12] Zhao Yong-Xia, Zhen Ge, "MD5 Research" Multimedia and Information Technology (MMIT), Second International Conference on (Volume:2) **2010**.

[13] .Vishwa gupta,. Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advance Research in Computer Science and Software Engineering, Vol.2-Issue 1, January **2012**

[14] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[15] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, **1994**.

[16] Dorothy Elizabeth, "Cryptography and Data Security", Addison-Wesley, **1982.**

[17] Donghua Xu, Chenghuai Lu, and Andre D. Santos, "Protecting Web Usage of Credit Cards Using One-Time Pad Cookie Encryption", Proc. Annual Computer Security Applications Conference (ACSAC), **2002**.

[18] William Stallings "Cryptography and Network Security", 3rd Edition, Prentice-Hall Inc., **2005.**

[19] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C", John Wiley and Sons, Inc., **1996**.

[20] B. Schneier ,Applied Cryptography, John Wiley &Sons, New York, **1994**.

[21] Rivest, R.L., Robshaw, M.J.B., Sidney, R., & Yin, Y.L(**2000**). "The Case for RC6 as the AES." AES Round 2

© 2013, IJSRNSC All Rights Reserved

Public Comments. URL: http://csrc.nist.gov/CryptoToolkit/aes

/

© 2013, IJSRNSC All Rights Reserved