A Novel Method for Cryptography

Gunjan Sahni, Ravindra Gupta, Gajendra Singh

Abstract— In this paper, we are presenting a modern technique for the encryption and decryption**.** This review research paper concentrates on the different kinds of encryption techniques that are existing. It is more secure also time efficient. Aim an extensive experimental study of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques, double encryption and Chaos-based encryption techniques. This study extends to the performance parameters used in encryption processes analyzing on their security issues.

Index terms— Cryptograpy, Integrity, Confidentiality, Non-deterministic, Equi-probable, Repudation, Private key

1 INTRODUCTION

1.1 Definition of Cryptography [1]

"Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack".

1.2 Cryptographic Goals

However, there are other natural cryptographic problems to be solved and they can be equally if not more important depending on who is attacking you and what you are trying to secure against attackers. The cryptographic goals covered in this text (in order of appearance) are privacy, integrity, authentication, and no repudiation.

These three concepts form what is often referred to as the CIA triad. The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

2 PROPOSED ALGORITHEM:

The proposed algorithm is as follows:

Input: 1. keys p and q

2. M i.e. message to be encrypted

Output : Secured sending of message from A to B

Procedure:

1. Generate_key(B)
2. Transmit public key to A
3. Select the message M to be transferred by A to B, call it as P
4. N is the product of two prime numbers in the form that if they are divided by four, the reminder remains 3.
   // n used in step 4 is same as n used in generate_ key(B) in step 1
5. Now A sends a message to B by using the following encryption equation

- *Author name is currently pursuing masters degree program in Information Technology inSssist College , RGTU University,Bhopal,India, E-mail: gunjan22aug@gmail.com*
- *Co-Author name is currently Assosiate Professor in Computer science and IT department in Sssist College,RGTU University,Bhopal, india,. E-mail: ravindra_p84@rediffmaill.com*

$C = P^2 \bmod N$
// This encryption is in $<Zn^*,*>$

6. At the receiver side B, the decryption is performed. The decryption is non deterministic. It creates four equally probable plaintexts.
7. Now B uses P and Q again which was used in step2 while generating keys i.e. P & Q are private keys for B
   $X1 = + C^{(P+1)/4} \bmod P$
   $X2 = - C^{(P+1)/4} \bmod P$
   $Y1 = + C^{(Q+1)/4} \bmod Q$
   $Y2 = - C^{(Q+1)/4} \bmod Q$
8. Now Chinese remainder theorem is called for generating four equi probable Plaintexts
   P1 = CRT (X1,Y1,P,Q)
   P2 = CRT (X1,Y2,P,Q)
   P3 = CRT (X2,Y1,P,Q)
   P4 = CRT (X2,Y2,P,Q)
9. Now B choose one of the P1,P2,P3,P4 as the final answer.

Generate_Key(USER)
{
1. Choose P and Q two large prime numbers of the form 4K + 3 and P != Q
2. Calculate N = P * Q
3. Public key = N
4. Private key = (P,Q)
5. public key and private key

}

3 COMPLEXITY ANALYSIS OF THE PROPOSED METHOD:

Encryption Complexity : $O(M^2)$, where M is the message

Decryption: O(M)

Key generation: O(1)

4 CONCLUSION

Contributions:

Advantages of the proposed method are as follows:

1. Encryption complexity is less in comparison to present system
2. Decryption complexity is also less
3. Key generation complexity is constant
4. There is no need of randomness
5. More secure against common modulus attack
6. Size of the message remains same during the encryption.

In future, our proposed method can be upgraded for digital signaling.

REFERENCES:

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004

[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.

[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[4] Ramesh G, Umarani. R, " Data Security In Local Area Network Based On Fast Encryption Algorithm",International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.

[5]Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.