Volume 5, Issue 5, MAY 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancement of ElGamal Digital Signature Based on RSA & Symmetric Key

Yashpal Jitarwal, Pawan Kumar Mangal, Sunil Kumar Suman
Computer Science & Engineering, National Institute of Technology
Jalandhar, Punjab, India

Abstract- cryptography necessarily focus on various security goals such as availability,integrity and confidentiality.In today's day to day environment there are various types of attacks such as snooping,traffic analysis,modification,masquerading,replaying,repudiation and denial of service. This paper focus on satisfy the security issues using combined approach of RSA and symmetric key cryptography based on enhancement of ELGAMAL digital signature scheme. This scheme works by merging integer factorization problem and discrete logarithm problem. As a result it provides better computing speed and throughput compare to existing RSA-ELGAMAL algorithm.

Keywords – ElGamal algorithm,RSA, cryptography,Throughput,digital signature, SHA-512.

I. INTRODUCTION

In the current scenario of day by day increasing of internet over worldwide,we are moving towards the more secure systems. We expecting more and more secure systems and secure applications. Security is becoming crucial issue in day to day real world applications such as net banking, online shopping. One solution to this is achieved by using encryption and decryption approach. There are two types of cryptographic algorithms,first is asymmetric key cryptography or public key cryptography and second, symmetric key cryptography or private key cryptography.Initially wereferred to data as plain text. After applying certain cryptographic algorithms on the plain text encrypted data is known as cipher text. There are various algorithms exist for achieving encrypted data file or cipher text file based on various key size and some other parameterRSA algorithm is public key cryptographic algorithm means that sender encrypt with its receiver's public key and receiver decrypt with its own private key.ElGamal cryptosystem is another public key cryptosystem. In this paper we are presenting enhanced technique of ElGamal cryptosystem based on RSA algorithm and symmetric key cryptography algorithm .Here we are also using the concept of Digital signature for verification of integrity of the message using SHA-512.

This paper is organized as follows, In section 2 ,we are providing related work, section 3 consist of existing technique , section 4 consist of proposed scheme and implementation and section 5 providing the conclusion.

II. RELATED WORK

Cryptography is the technique for creating secret codes.Cryptanalysis involves to break these secure codes. There are various types of cryptanalysis attacks such as cipher text-only,known-plaintext, chosen-plaintext and chosen-cipher text. In symmetric key cryptography algorithm lot of computation is required for key generation and maintenance phase. Solution to this problem is given by using public key cryptography [1] or asymmetric key cryptographic algorithm. RSA algorithm , Rabin cryptosystem, ElGamal cryptosystem etc. are some well-known algorithm that are used for the purpose of encryption and decryption process and to send data or text files in secure manner[1].

RSA Algorithm

RSA algorithm is public key cryptographic technique, it involves key generation,encryption and decryption phase. RSA uses modular exponentiation for encryption and decryption process.

RSA key generation

- Select two large prime numbers n1 and n2.
- n←n1*n2.
- $\emptyset(n)$ ←(n1-1)*(n2-1).
- We are select e such that 1<e<$\emptyset(n)$ and e is coprime to $\emptyset(n)$
- (d*e)mod $\emptyset(n) == 1$
- Public key ← (n,e).
- Private key ←d

RSA_Encryption(p,e,n)

- C←(p^e)mod n

RSA_Decrytpion(c,d,n)

- P← (c^d)mod n

Diffie-Hellman key agreement protocol

This scheme was first published by Whitfield Diffie and Martin Hellman. Diffie-Hellman key agreement protocol is based on symmetric key cryptography algorithm[3]. In this cryptographic approach we are using same key for encryption and decryption purpose. This scheme was first published by Whitfield Diffie and Martin Hellman. Diffie-Hellman key agreement, itself is an anonymous (non-authenticated) key agreement protocol. An intruder in middle can establish communication between the two communicating parties.An standard methods is needed to prevent this type of attack between communicating entities. Diffie-Hellman algorithm is depend on difficulty of computing discrete logarithms.Diffie-Hellman protocol is used in secure shell(SSH),Internet protocol security (IPsec),public key infrastructure(PKI).

El-Gamal digital signature scheme

Firstly, this scheme is described by TaherElgamal in 1984. This signature scheme is based on difficulty of computing discrete logarithms. This is another public key cryptography algorithm. Two attacks have been mentioned for the Elgamal cryptosystem based on low modulus and known plain text attacks[4]. Low modulus attack is applicable when value of modulus is low then it is difficult to solve the discrete algorithm. Known-plain text attack is applicable when we know plain text corresponding to cipher text, we can easily find out the key and attack becomes easier.

III. EXISTING SCHEME OF ELGAMAL DIGITAL SIGNATURE

The ElGamal algorithm can be described as follows-

Initialization

- select a large prime p
- select d to be member of group G =<Z*,X> such that 1<=d<=p-2
- select e1 to be a primitive root in the group G=<Z*,X>
- e2=(e1^d) mod p
- public key =(e1,e2,p)
- private key =d

Elgamal_encryption

- Select a random integer r in the group G=<Z*,X>
- C1=(e1^r)mod P
- C2=(p*(e2^r))mod p
- Cipher text c1 and c2 is transmitted

Elgamal_decryption(C2 , C1 , P)

- P=(c2(c1^d)^-1)mod p

IV. PROPOSED SCHEME

Proposed scheme of ElGamal variant scheme is make to it different from original scheme by key generation and encryption decryption process. In this technique we use two separate files are used for encrypted file and second for signing the digest of the message. We use symmetric key cryptography in enhancement of ElGamal cryptography. For signing of digest, we use efficient RSA algorithm. Various steps involves in this technique is follows.

A. Key_generation

- Sender and receiver both are agree on two prime numbers g and p.
- Sender choose its own secret number a and compute A=(g^a)mod p
- Transmit A to receiver.
- Receiver chooses its own secret number b and compute B=(g^b)mod p
- Transmit B to sender.
- Sender compute k1=(B^a)mod p
- Receiver compute k2=(A^b)mod p

  Here it is clear that k1=k2 means shared secret key is established between sender and receiver.
- Choose primitive finite field Fa and primitive root element belong to this field.

B. Encryption_phase

- Select another large prime q1 in such a way that 1<k1<q1.
- One time key otk=(a^k1)mod q1.
- Cipher text c=(m*otk) mod q1.

C. Decryption_phase

- compute otki=(a^-k2) mod p
- message text =(c*otki) mod p

Signature generation
firstly we will create digest or hashing of the message using SHA-512. In this technique the created digest is of size 512 bits. Then this 512 bit message digest is signed by using enhanced RSA algorithm.Here we use different algorithm for encryption and signing process to provide more security compare to existing system.

A. Key_signing

Message_digest=SHA_512(message size in multiple of 1024 bits, initial 512 bit message digest)

- Select two large prime numbers n1,n2,n3.
- n←n1*n2*n3.
- $\emptyset(n)$ ← (n1-1)*(n2-1)*(n3-1).
- We are select e such that 1<e<$\emptyset(n)$ and e is co-prime to $\emptyset(n)$
- (d*e)mod $\emptyset(n)$ == 1
- Public key ← (n,e).
- Private key ←d
- Sign s=(Message_digest^d) mod n

B. Verification

- Message_Digest=(s^e)mod n
- createMessage_digest from received message and compare it with step 1. If both are equal then message is valid.

V. IMPLEMENTATION PHASE

Implementation of the proposed algorithm is done in c++ code block programming software. Machine used for the programming is 2 GB RAM and intel i3 processor. Time comparison between various existing approaches and proposed approach is shown in following table.

Message size	RSA	Enhanced RSA	Elgamal	Proposed approach
1 KB	.00321 sec	.00154 sec	.02537 sec	.00602 sec
2 KB	.00344 sec	.00312 sec	.03456 sec	.02563 sec
3 KB	.00452 sec	.00438 sec	.03463 sec	.02589 sec
average encryption time	.01092 sec	.00320 sec	.03256 sec	.02137 sec
Throughput	4.00302	4.21593	.063791	.087923

Figure 1 : comparative analysis of encryption time and throughput

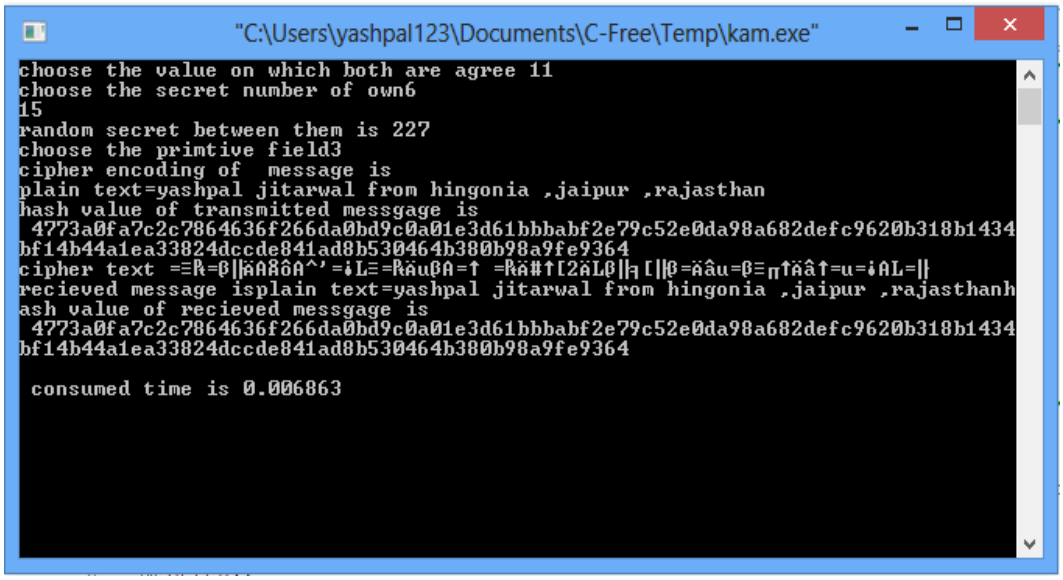

Figure 2. Result of encryption and decryption process

complexity of the given encryption and decryption process respectively is O $(\log n)^3$+ O(log n) + 2 O $(\log n)^3$, O (log n) + 3 O $(\log n)^3$. Complexity of signing the message digest using RSA algorithm is O(n) based on fast exponential algorithm.

VI. CONCLUSION

The encryption and decryption provide the solution to confidentiality,integrity and authentication of message. This paper present the various aspects of key generation based on symmetric key procedure. Proposed version of ElGamal cryptosystem provide the confidentiality to the message sufficiently with more efficiently compare to existing algorithm. It provides more throughput compare to ElGamal cryptosystem.

REFERENCES

[1] Ahmed J.M. ; Ali,Z,M,"*TheEnhancemnt of computation Technique By combining RSA and ElgamalCryptosystem*"IEEE, proc. Electrical Engineering and Informatics(ICEEI),2011,pp:1-5

[2] Shay Gueron , Simon Johnson , Jesse Walker " SHA-512/256" Security Research Lab, Intel Labs, Intel Corporation, USA. [3] MasoudNosratiRonakKarimi Mehdi Harir "Audio Steganography: A Survey on Recent Approaches" World

[3] DiaaSalamaAbdElminaam, HatemMdAbdual Kader, MohiyMdHadhoud, *"Evaluating the Performance of Symmetric Encryption Algorithms",* International Journal of Network Security, 2010, Volume 10, pp: 213-219.

[4] Rashmi Singh, Shiv Kumar, "*Elgamal's Algorithm in Cryptography",* International Journal of Scientific & Engineering Research,2012, Volume 3.

[5] William Stallings, Cryptography and Network Security-Principles and Practice, Fifth Edition,Pearson publication, pp. 259-262.

[6] Thomas H. *Cormen*. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein; Introduction algorithms; second edition; 2003;

[7] W. Mao, Modern cryptography: theory and practice: Prentice Hall Professional Technical Reference, 2003, pp. 294-296.

[8] TaherElGamal "*A public key cryptosystem and a signature scheme based on discrete locarithms*" 1998,Springer-Verlag.

[9] http://www.rsa.com/rsalabs/node.asp?id=2255

[10] http://x5.net/faqs/crypto/q29.html [12] [11]

[11] http://www.princeton.edu/~achaney/tmve/wiki100k/docs

[12] J. He and T. Kiesler. Enhancing the security of ElGamal's signature scheme. In Computers and DigitalTechniques, IEEE Proceedings-, volume 141, pages 249-252.

[13] ELGAMAL T. A public key cryptosystembased on discrete logarithms[J].IEEE Trans inform Theory.1985,31(4):469-472

