ISSN: 0975-766X
CODEN: IJPTFI

Available Online through ***Research Article***
www.ijptonline.com

MODIFIED ELGAMAL CRYPTOSYSTEM FOR PUBLIC-KEY ENCRYPTION AND DIGITAL SIGNATURE

Sandip Kumar Bhowmick[1], Sourav Kumar Das[2], Tamal Chakraborty[3], P.M.Durai Raj Vincent[4]
[1,2,3] 2nd year MCA Student, SITE, VIT University
[4] Associate Professor, SITE, VIT University
Mail: sandipkb922@gmail.com

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract:

The key exchange in cryptography is a major issue today for secured data transmission over thenetwork in which keys are exchanged between two parties for utilization of keys in acryptographic algorithm. This paper proposes a modified ElGamal cryptography scheme which will provide data secrecy as well as adigital signature with a high information rate. The security of ElGamal entirely depends on the complexity of factoring discrete logarithmic problems in which it is very difficult to figure out discrete logarithms over finite fields through brute force attacks or statistical attacks. As the ElGamal scheme's security is constantly being challenged, our proposed scheme enhances the algorithm by adding an arbitrary number and an extra key to the conventional one in order to increase deciphering complexity and reduce time complexity to decrypt themessage.

Keywords: Public key cryptography, discrete logarithm problem, multiplicative group.

I. Introduction:

Cryptography is thescience of hiding information from unauthorized persons mostly in the form of scrambled texts, numbers, pictures, audio and video to make the content imperceptible or unintelligible for serving its primary goal of confidentiality, integrity, authenticity and access control. The concept of public key cryptography or asymmetric key cryptography was first invented in 1976 by Diffie and Hellman.[3] The key concept behind the public key encryption is trapdoor functions. Thetechnique utilizes the usage of a couple of cryptographic keys such as public keys and private keys. The message sender encrypts its message with the public key which is freely distributable and whereas the receiver decrypts the message using its private key whichis kept thesecret to it.

After Diffie-Hellman key exchange algorithm, ElGamal algorithm became most well known public key cryptographic algorithm invented by Taher Elgamal in 1985 as the successful implementation of theDiffie-

Hellmanalgorithm. It is a modified Diffie-Hellman algorithm which not only allows exchange messages rather than just keys butalso provides adigital signature for message authentication.[4][5] The digital signature assures the recipient that the message came from intended sender without any alteration in transit. It also has the advantage of generating different cipher text from the same plaintext each time it is encrypted.[6] Now, let us review the ElGamal scheme.

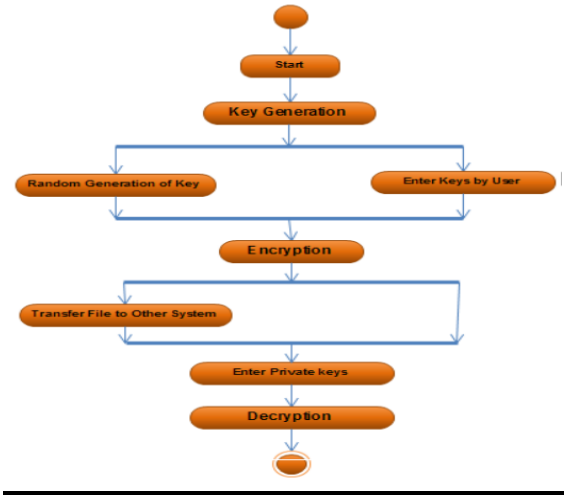

Fig.1 ElGamal Encryption Flowchart.

<<Key generation procedure>>

p: *prime* number of large size(100-150 digits)

g: A generator function which belongs to the multiplicative group (Z^*_p % p)

a: Anarbitrary positive integer, such that 0<a<=p-2,

Calculate:g^a% p

Public Key for A: (p, g, g^a)

Private Key for A: a

<<Encryption Procedure>>

Sender B encrypts a message M :{ m0, m1…) to A. m in the range {0, 1… p-1}

Obtain A's public key: (p,g,g^a)

Select arbitrary positive integer k, such that k>0 and k<p-1

Calculate: $\gamma = (g^k \% p)$

$\delta = (m\ (g^a)^k) \% p$

Transmitencrypted text(cipher)c= (γ, δ) sends→A

<<Decryption Procedure>>

A receives ciphertext from B

Retrieve message m by calculating:

$m= ((\gamma^{-a})*\delta) \% p.$

<<Digital Signature Scheme>>

To sign, B takes a arbitrary positive number u, such that 0<u<p-1 and g.c.d (u, p-1) =1

Calculatew by: m=(b* γ)+(u*w) %(p-1); b: Private Key for B

Send (γ, δ, w) to user A

<<Signature verificationprocedure >>

If, $g^m= ((g^b \% p)^{\gamma})* (\gamma^w)\% p$: signature is verified.

Else, the signature is not verified.[7]

II. Literature Survey:

Cryptography is a mechanism that is used to provide security during data transmission over the network. There are many secure algorithms available in this regards. Among those algorithms, we need to select that particular algorithm which can meet all the conditions of authorization, authentication, integrity, confidentiality, Access control.[8] The main anxiety in the field of cryptography is to protect the information from the unauthorized access. In the field of public key cryptography, El-Gamal encryption is known as an asymmetric key encryption algorithm and is emerged on Diffie-Hellman (DH) key exchange algorithm.[9] Asymmetric or public key encryption technique is a kind of encryption technique in which two keys are used. In this pair of keys, one is used to encrypt the message and the decryption can be done by only the other. El-Gamal encryption technique can be narrated over G, Where G is a cyclic group.[10]Basically, El-Gamal is flourished on the Discrete Logarithm Problem. El-Gamal is used to simplify the DH Key exchange algorithm by presenting a random key K. Due to this alleviation, El-Gamal algorithm is mainly used to encrypt in one direction, except the requirement of active participation of thesecond party. The two biggest benefits of this algorithm are data expansion rate and unspecialized encryption for long messages. Slower speed is one of its main drawbacks. [11][12] The main purpose of this paper is to overcome this drawback and also proposed a modified version of El-Gamal.

Compute: $(\gamma^{p-1-a}) \% p= \gamma^{-a}= a^{-ak}$

III. Modified El-Gamal public key encryption scheme:

Now we modify the existing ElGamal encryption technique in the following way:

<<Encryption Procedure>>

Let B chooses an arbitrary positive Integer u, where: 0<u<=p-2 and g.c.d(u,p-1)=1

Compute: $v=g^u \% p$

Calculate w by, $m=(b* \gamma +u*w) \%(p-1)$; b: Private Key for B

Compute: (γ, δ, ε) as follows

$\gamma = v$

$\delta = w*(g^a \% p)^u \% p$

$\varepsilon = m*g^w \% p$

<Decryption Procedure>

A receives (γ, δ, ε) from B

Compute:

$\gamma^a =(g^u)^a \% p =(g^a)^u \% p = (g^u)^a \% p$

Where, a= private key of A

$(\gamma^a)^{-1} * \delta \% p = w \bmod p$

Recover actual message (m) by:

$((g^w)^{-1} * \varepsilon) \% p$

$= ((g^w)^{-1} * m * g^{w)} \% p$

$=m \% p$

<<Procedure for Signature Verification>>

If, $g^m= ((g^b \% p)^{\gamma})* (\gamma^w)\%(p)$: signature is verified.

Else, signatureis not verified.

The splitting property is retained in the modified algorithm. Assuming that the ciphertext is received in the same order as the sender sends, this modified algorithm generalizes the concept ofencipher and signing a plain text with higher information rate.

IV. Security Analysis: In our digital signature scheme, the arbitrary number 'u' shouldn't be used repeatedly as otherwise;a mathematical attack by interceptor can deduce the secret keys of the sending party. Let (γ1, δ, ε1)& (γ2, δ, ε2) are pairs of signature that utilized same arbitrary positive number 'u'. The relation be depicted as: $T_1= (k_b*r)+(u*w_1) \%(p-l) \rightarrow$(i)and$T_2= (k_b*r)+(u*s_{2)} \% p-1 \rightarrow$(ii) thus, k_b can be deduced from the above equations.

%p and $\varepsilon=m2.g^{w2}\%p$. But will not deduce g^s {s=signature} unless solving the DLP.

However, by introducing the non-commutative one-way function'F' before signature to the original text, this type of mathematical attack will be blocked asthe interceptor will not be able to find a sequence of messages (m0…mW) in reasonable time:

Hence the interceptors may find the signature,butthey would not be able to find the corresponding sequence of message blocks.

Also from the execution time analysis of the conventional ElGamal algorithm and the modified one, it clearly states that the speed of the algorithm has enhanced in creating and checking digital signature. Also, there is a slight increase in data rate for data encryption and decryption with preserving thecomplete security of the algorithm.

V. Conclusion:

This paper proposes a modified encryption and signature generation based on Elgamalcryptosystem with enhanced security and speed w/(w+2) {w= block of plaintext}. This proposed algorithm provides better information rate than the original ElGamal scheme and thus is expected to be secured in the digital data communications. The security of the modified algorithm entirely relies on the difficulty of finding the private keys as it is about factoring discrete logarithm problem and since the private keys are not known and are large, it is very difficult to factor large numbers to make theassumption of the private keys. Also, the inclusion of an extra key and extra random number in the public shared key adds to the security layer of the modified algorithm and makes it more resistant to attacks such as mathematical attack, brute force attack,and direct hack on theprivate key, etc according to known signatures. Thus we can say that the modified ElGamal cryptosystem for public key encryption and thedigital signature is a hard problem because by knowing ε, no one can derive g^w unless the DLP is solved. Nonetheless, the security of the scheme entirely depends on the hardness of solving the discrete logarithms.

References:

1. ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." *Workshop on the Theory and Application of Cryptographic Techniques*. Springer Berlin Heidelberg, 1984.
2. McEliece, R. J. "A public-key cryptosystem based on algebraic." *Coding Thv*4244 (1978): 114-116.
3. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.
4. Merkle, Ralph, and Martin Hellman. "Hiding information and signatures in trapdoor knapsacks." *IEEE transactions on Information Theory* 24.5 (1978): 525-530.

5. P.M.Durai Raj Vincent, Sathiyamoorthy E, " A Novel and efficient public key encryption algorithm" International Journal of Information and communication technology, Vol. 9, No. 2, pp 199-211, 2016.
6. ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." *Workshop on the Theory and Application of Cryptographic Techniques*. Springer Berlin Heidelberg, 1984.
7. Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." *Journal of computer and system sciences* 28.2 (1984): 270-299.
8. Li, Xiaofei, Xuanjing Shen, and Haipeng Chen. "ElGamal Digital Signature Algorithm of Adding a Random Number." *Journal of Networks* 6.5 (2011): 774-782.
9. P.M.Durai Raj Vincent "RSA Encryption Algorithm- A survey on its various forms and its security level" International Journal of Pharmacy and Technology Vol 8 No 2 12230-12240, 2016.
10. Sandhu, Ravinderpal S. "Cryptographic implementation of a tree hierarchy for access control." *Information Processing Letters* 27.2 (1988): 95-98.
11. Ingemarsson, Ingemar, and C. K. Wong. "A user authentication scheme for shared data based on a trap-door one-way function." *Information Processing Letters* 12.2 (1981): 63-67.
12. Sharma, Ankush, et al. "Implementation & Analysis of RSA and ElGamal Algorithm." *Asian J. of Adv. Basic Sci* 2.3: 125-129.
13. Burmester, Mike, et al. "A structured ElGamal-type multisignature scheme." *International Workshop on Public Key Cryptography*. Springer Berlin Heidelberg, 2000.
14. Vincent P.M.D.R, Sathiyamoorthy E, "A novel and efficient key sharing technique for web applications" in IEEE Fourth International Conference on Computing, Communications and Networking Technologies. 2013.