Unclassified computer data specify a cryptographic algorithm by the Federal Data Encryption Standard (FIPS)

[1]Priya Nalwaya , [2]Varun P Saxena

[1]Student M Tech, [2]Assistant Professor

Government women engineering college, Ajmer (India)

ABSTRACT

In this work we combine concept of running key cipher with ELGamal theory. so in this process we use two type of cryptography public key cryptography and private key cryptography by using single public private key pair. To do so we use Running Key Cipher followed by ElGamal in feedback mode. We construct a cryptographic scheme by using only single step of ElGamal providing security to the entire message blocks involved. We then analyze the performance and security of our proposal with respect to existing system.

Keywords: ***Running Key Cipher, El Gamal Cipher, Cipher Feedback Mode, Tabula Recta, One Time Pad.***

I INTRODUCTION

ElGamal encryption[1] is one of fundamental public-key cryptosystems. el gamal algorithm has simple and efficient but its chosen-plaintext security is clearly understood. Security overhead in terms of bandwidth, however, often becomes obstacles against its publicly wide use. ElGamal cipher texts are typically at least as many bits as the prime modulus p. If the plaintext size is small comparatively to the size of p, the relative size overhead becomes worse. For example, assuming p is a 2048-bit prime, in a hybrid encryption scenario where a symmetric key size is 256-bit, the size overhead of ElGamal is roughly ten times the plaintext size.in the future for larger public key size more powerful mathematical analyst and computational power method available. this situation become more and more harder.

More specifically, let consider the case where a server should receive from multiple clients each shared secret-key encrypted under hybrid encryption. If the number of clients grows linearly in the above example, the size overhead also increases linearly. Thus, efficiency can be improved if a router is given an accessory to compress multiple cipher texts[2].

II BACKGROUND RELATED WORK

A key agreement protocol establishes secret communication Key (s) among all parties involved. In 1976, Diffie and Hellman (DH) [3] proposed the well-known public-key distribution scheme, based on the discrete logarithm problem[4], to enable two parties to establish a common secret key based on their exchanged public keys. However, their scheme did not provide authentication mechanism for the exchanged public keys. In past years,

NIST has published a series of security standards under Federal Information Processing Standard (FIPS) [5]. FIPS 186-2 Digital Signature Standard (DSS) [6] introduces Digital Signature Algorithm (DSA) Series of security standards publish by the national institute and technology(NIST) under Federal Information processing Standard(FIPS). Standard for key agreement is still missing in the current standards. Arazi [7] proposed integrating Diffie–Hellman (DH) key exchange into the Digital Signature Algorithm (DSA).

As for the problem that ElGamal digital signature scheme's security [8] is constantly being challenged and increasingly becomes increasingly serious, an improved ElGamal digital signature algorithm is proposed. As the original ElGamal algorithm has its own security disadvantages that only one random number is used, in order to improve its security, the scheme presented in this paper improved this demerit by adding a random number to the original one and increasing difficulty of deciphering key[9].

For long enough messages the processing overheads are also involved. Let for example we have a message divisible into ten numbers of blocks near to identical size. Now if we may be able to secure all of ten message blocks with the same degree of security provided by efficient Public Key encryption schemes like ElGamal, by application of ElGamal process only once to single block of message, it will reduce the performance overhead. Federal Information Processing Standards Publication 81 (FIPS'81) describes some of the common standards for the Standard and Common modes for DES operations which is Private Key cryptosystem in nature. Idea behind this work presented here is to apply concept of feedback operation modes in Public Key encryption as well. A simplest approach to do so may be using Public key scheme in message feedback mode[10].

The main issue with message feedback approach which arrives is that it does not consider the frequency cryptanalysis of English alphabet. Furthermore most of the such application relies over XOR-ing the message block in feedback mode, which seems impractical in current scenario as any typical message pattern leaks the whole subsequent blocks. Further consideration of only the processing overhead may result into security compromises. Yet this idea laid down foundation for a novel approach of message feedback cryptology.

In this work we used an approach of symmetric cipher feedback into an asymmetric cryptographic scheme rather than simple message feedback. For the purpose of symmetric encryption we used Running Key Cipher and in asymmetric module we used ElGamal encryption in feedback mode. We have used *William Shakespeare's Othello* adopted as Unicode text format (Othello.txt) as our text, and we are using the *tabula recta* as our tableau for Running Key. Information about the start point of Running key is contained into ElGamal Public Key cipher part, so the exchange of the Running key is not explicitly required. Start point of Running Key is generated using the random numbers while encryption.

The use of Running Key not selected by user and generated by random function result into One Time Pad.

III TERMINOLOGY AND DEFINITION

3.1 One Time Pad

In Cryptology, the one-time pad [11] is a type of encryption process. It has been proven to be impossible and infeasible to break if used properly. Each bit/character of the plain text is enciphered by a modular addition with bit/character from a randomly chosen private key (said to be PAD) having same length equal to the plain text, resulting in cipher. In the case the key is really random, meanwhile as large as / greater than the original plain text/message, further never reused wholly or partially, always kept private, the cipher will be impossible and

infeasible to decrypt or break without knowing the PAD or random secret key .In the one time pad or PAD we use the same requirement as cipher with the perfect security property. Furthermore, practical problems have always prevented OTP / PAD from being widely used generally.

3.2 Cipher Feedback

To used cryptographic protection of sensitive but unclassified computer data specify a cryptographic algorithm by the Federal Data Encryption Standard(FIPS)[5]. FIPS'81 defines four modes of operation for the DES which may be used in a wide variety of applications. The modes[12] specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). there are various modes are available we use this modes for encryption and decryption as a standards. there are four modes ECB,CBC,CFB,OFB here ECB stands for electronic code book , CBC for cipher block chaining CFB cipher feedback mode and OFB for output feedback mode.

The body of FIPS'81 standard provides specifications of the recommended modes of operation but does not specify the necessary and sufficient conditions for their secure implementation in a particular application. This standard specifies the numbering of data bits, how the bits are encrypted and decrypted, and the data paths and the data processing necessary for encrypting and decrypting data or messages. This standard is based on (and references) the DES and provides the next level of detail necessary for providing compatibility among DES equipment. This standard anticipates the development of a set of application standards which reference it such as communication security standards, data storage standards, password protection standards and key management standards. Cryptographic system designers or security application designers must select one or more of the possible modes of operation for implementing and using the DES in a cryptographic system or security application.

3.3 Running Key Cipher

In the running key cipher[13] text are used from the book, running key cipher is type of poly alphabetic substitution cipher. Usually used book are agreed ahead of time, while the passage to use should be chosen randomly each message are secretly indicated some where in the message Text.

Suppose we have agreed to use *The Programming Language* (1978 edition) as our text, and we are using the *tabula recta* as our tableau. Now suppose we want to send a message 'Flee at once'. For this we have to chose starting point. we have page and a line suppose we choose 63 as a page no and 1 as line no and our running key is error occur at serval place.

We write plaintext and running key just like:

Plaintext: f L e E A t o N c e

Running key: E R R O R S C A N O

Cipher text: J C V S R L Q N P S

And send the message 'JCVSR LQNPS'. In other type of cipher when we increase the size of message than we repeat the running key again and again but in this we doesn't repeat the running key we just continue the line from the book.

Now after sending the message we have to tall receiver about running key. for doing this we made fake block. in this example we make fake block of five cipher text character, where 3 denoting page number, 2 the line number using A=0,B=0etc.this block is called indicator block, and this indicator block is inserted at the second last position. now we encoded page and line in AGDAB(06301) form. here 63 is page number and 1 is line number.

3.4 Tabula Recta

In this method we shift previous row in the left, in this method we have table of alphabets. This table is know as square table and method is called tabula recta. In 1508 German author and monk Johannes invented trithemius and used as trithemius cipher.

3.5 Random Functions and random Numbers

There are various method to generate random number one method are called RNG[17] 'random number generator '.this method generate sequence of symbol and number that appears random.

There is different method to generate random number in old days. But now a days random number generator RNG as used to generate random number.

3.6 ElGamal Cipher

In 1984 Taher ElGamal [1] who is also the inventor of SSL, presented a cryptosystem which is based on the Discrete Logarithm Problem[17]. It relies on the assumption that the Discrete Logarithm cannot be found in feasible amount of time, while the reverse operation of the power can be computed efficiently. The original public key system proposed by Diffie and Hellman requires interaction of both parties to calculate a private key which is common for both the parties. This poses issues if the cryptographically designed system should be applied to communication systems where both parties are not able to interact in reasonable time due to delays in transmission or unavailability of the receiving party. Thus ElGamal simplified the Diffie-Hellman key exchange algorithm by introducing a random exponent k. This exponent is a replacement for the private exponent of the receiver. This simplification means the algorithm can be used to encrypt in single-direction, without having the necessity to the second party to actively participate. The main advance is that the algorithm can be used for encryption of electronic messages, which are transmitted by the means of public store-and-forward services.

3.6.1 Key Generation

As discussed above, the basic requirement for a cryptographic system is at least one key for symmetric algorithms and two keys for asymmetric algorithms. The key generation steps are similar to the general scheme explained above. With ElGamal, only the receiver needs to create a key in advance and publish it. Following our naming scheme from above, we will now follow Ron through his procedure of key generation.

Ron will take the following steps to generate his key pair:

1. Prime and group generation:

In this step we generate p and g .p is prime and g is generator. We select this from multiplicative group Z_{*p} of integer module p.

2. Private key selection:

Now Ron selects an integer b from the group Z by random and with the constraint $1 \leq b \leq p - 2$. This will be the private exponent.

3. Public key assembling:

From this we can compute the public key part $g^b \bmod p$. The public key of Ron in the ElGamal cryptosystem is the triplet (p, g, g^b) and his private key is b.

4. Public key publishing:

The public key may be published using some dedicated key server or other means, so that Henna is able to get hold of it.

3.6.2 Encryption Procedure

To encrypt a message M to Ron, Henna first needs to obtain his public key triplet (p, g, g^b) from a key server or by receiving it from him via unencrypted electronic mail. There is no security issue involved in this transmission, as the only secret part, b, is sent in g^b. Since the core assumption of the ElGamal cryptosystem says that it is infeasible to b compute the discrete logarithm, hence it is considered to be safe and secure.

For the encryption of the plaintext message M, Henna has to follow these steps:

1. Obtain the public key:

As described above, Henna has to acquire the public key part (p, g, g^b) of Ron from an official and trusted key server.

2. Prepare M for encoding :

Write M as set of integers (m1, m2, . . .) in the range of $\{1, \ldots, p - 1\}$. These integers will be encoded one by one.

3. Select random exponent:

In this step, Henna will select a random exponent k that takes the place of the second party's private exponent in the Di e-Hellman key exchange. The randomness here is a crucial factor as the possibility to guess the k gives a sensible amount of the information necessary to decrypt the message to the attacker.

4. Compute public key:

To transmit the random exponent k to Ron, Henna computes $g^k \bmod p$ and combines k it with the cipher text that shall be sent to Ron.

5. Encrypt the plaintext:

In this step, Henna encrypts the message M to the cipher text C. For this, she iterates over the set created in step 2 and calculates for each of the m_i:

$$c_i = m1 * (g^b)^\kappa$$

The cipher C is the set of all c_i with $0 < i \leq |M|$.

The resulting encrypted message C is sent to Ron together with the public key $g^k \bmod p$ derived from the random private exponent.

Even if an onset would attempt to listen to this transmission, and in a second step would also acquire the public key part g^b of Ron from a key server, he would still not be able to derive g^{b*k} as can be seen from the Discrete Logarithm problem.

For each message block this el gamal algorithm advise to chose new random value for k. This process enhances security because by knowing one block of message attacker doest get all the message block.

$$c1 = m1 * (g^b)^k mod P$$

$$c2 = m2 * (g^b)^k mod P$$

if we the value of m_1 then next block of the message that is m_2 can be calculated by using the following formula:

$$\frac{m1}{m2} = \frac{c1}{c2}$$

3.6.3 Decryption Procedure

After receiving the encrypted message C with randomized public key g^k, Ron has to use the decryption algorithm to be able to read the plaintext M . This approach may be divided in few steps:

1. Compute shared key:

The ElGamal cryptosystem helped Henna to define a shared secret key without Ron's interaction. This shared secret is the combination of Ron's private exponent b and the random exponent k chosen by Henna. The shared key is defined by the following equation:

$$(g^k)^{p-1-b} = (g^k)^{-b} = b^{-bk}$$

2. Decryption:

For each of the cipher text parts c_i Ron now computes the plaintext using

$$m_i = (g^k)^{-b} * c_i \, mod \, p$$

After combining all of the sub-parts m_i back to M Ron may read the message sent by Henna.

3.6.4 ElGamal Signatures

The ElGamal encryption scheme does not only support crypto-graphical steps encryption and decryption, but also the digital signing of messages M.

A signature scheme has following 3 main characteristics:

• Creation

Henna needs to be able to find the signature for M by using her private key a. She will then send the message together with the signature as the pair (M, S) to Ron.

• Verification

Ron has to be able to verify the signature by using the public key g^a. The verification of the signature assures Ron that Henna has signed the message as he received it. It does not deliver information about if Henna wrote the message herself or if she intended to send it at all. The second information Ron can draw from the verification is that the message has not been altered on the transmission path between him and Henna.

• Forgery prevention

It must be impossible for a unauthorised user to use the public key g^a of Henna to create a signature for an arbitrary message.

A signature in the ElGamal cryptosystem is the pair (r, s) with $0 \leq r, s < p - 1$ defined by the equation

$g^M \equiv (g^a)^r r^s \bmod p$

The procedure of digital signing follows same kind of steps as the encryption procedure:

1. Choose random k ϵ G
2. Compute $r \equiv g^x \bmod P$
3. Fill the signature equation from above as

$g^{M \equiv} g^{ar} gks \bmod P$

and solve it for s using

$m \equiv ar + ks \bmod (P-1)$

This has a solution for s if k is chosen such that $\gcd(k.p-1) = 1$ Ron received (M, r, s) and wants to verify the signature instantly. For this purpose, he only needs to compute both sides of the equation one and check it for equality of both sides.

3.6.5 El-Gamal Summary

As has been shown, the ElGamal cryptosystem is as secure as it is hard to solve the problem of Discrete Logarithm, specified none of the weak random exponents or prime numbers are chosen. Moreover it prevents a chosen plaintext onset by making usage of a randomized encryption exponent say, k. As this exponent k is chosen uniformly before the process of encryption, the same plaintext may result in (p – 1) different cipher values, one of these possible values is chosen uniformly by choosing a k.

One drawback of ElGamal is the Message size Expansion. The size of the cipher / transferred message doubles the original size. This increment comes from selection of a new random value k for each block of the plaintext message m_i. Public key derived from this k need to be sent together with the cipher c_i in the form of the pair (c_i , g^k), the set of all these pairs giving the cipher text k .

Another problem that can arise is that Henna relies on the authenticity of the public key she retrieves from Ron. This is a lesser problem if the public key is handed over in direct contact, meanwhile usage of the system over a larger network like the Internet other means need to be found Users send their public keys there after generation so others can download them and use them for encryption or validation of signature. In the case suspicious attacker managed to supply Henna with his key and make her believe it is the key of Ron, she would encrypt the message to the attacker and not to the intended receiver Ron. If the message is not signed, the attacker can then encrypt the message again, this time with Ron's key and send it to Ron. This attack is of the type Man-In-The-Middle. Here at least the man-in-the-middle might be detected if Henna would both sign and encrypt the message, since Ron would notice the changed contents when verifying the signature.

To overcome the problem of forged signatures, webs of thrust can be built up where users sign their keys against each other thereby assuring the authenticity of the key. Another possibility is a central certification authority that signs or even gives out the keys only after validating the owner of the key.

IV PROPOSED MODEL

Unlike the approaches described in FIPS'81 which describes the four modes of operations specifically for DES which is Private Key encryption in nature, we are going to design a cryptographic system for Public key cryptographic systems, which will be more efficient in terms of security.

We will introduce the concept of cipher Relay instead of using conventional phenomenon of cipher feedback. Cipher feedback is a mode defined for a single cryptographic algorithm; we will use hybrid cryptosystem by facilitating use of ElGamal Cryptosystem (Asymmetric Key) with Running Key Cipher (Symmetric Key) in a blended environment.

Cipher feedback approach when implemented alone on ElGamal encryption leaves the whole system to be a subject of frequency analysis. So we will first generated some cipher by making use of Running key encryption, then we will relay the output of it as input to ElGamal encryption. This prevents the frequency analysis of English alphabets and text strings of encrypted message. Further we will be able to use cipher feedback in ElGamal encryption.

4.1 Encryption in Proposed System

First we will encrypt the whole message at sender side by using Running Key with the help of some pre-agreed text and a Random function. Here Random function determines the start point of the Running key. This step will give us two entities namely

1. Running Key Cipher (C_r),
2. Running Key (K_r : random number used).

In next step we will restructure K_r and C_r into multiple fixed size cipher streams as

$$c_r = K_r + c_{r0} + c_{r1} + c_{r3} + c_{r4} + \cdots$$

Now encrypt K_r+C_{r1} using ElGamal encryption resulting to C_0 as

$$c_0 = E(ElGamal(K_r + c_{r0}))$$

And Encrypt rest part into Cipher feedback mode as

$$C_n = C_{rn} \oplus C_{r(n-1)}$$

4.2 Decryption

Decrypt very first ElGamal cipher part i.e. C_0 using ElGamal Decryption will result into C_{r0} and K_r.

$$(C_{r0}, K_r) = D(ElGamal(C_0))$$

Now we have C_{r0}, so we can easily decrypt cipher feedback part for $C_{r\,n}$ for all n>0 as:

$$C_{rn} = C_n \oplus C_{r(n-1)}$$

This will result into a stream of $C_{r\,n}$, recompose Cr by appending these streams of $C_{r\,n}$ in ordered way as

$$C_r = C_{r0} + C_{r1} + C_{r3} + \cdots$$

Now we have both C_r and K_r so we will be able to decrypt the Running Key Cipher by making use of pre-agreed text file.

4.3. Flow chart for encryption process in proposed system

In the fig1 we encrypt the message using first running key cipher and than using EL Gamal cipher M is over message and text Othello. text is over running key which we use to encrypt the message K_r is over running key that is random number. After encrypt the message we get the running key cipher C_r .Now we have $C_r + K_r$ in the next step we decompose C_r .Now we encrypt first block of message using EL Gamal algorithm and than encrypt rest part using x-or operation.

4.4 Flow chart in decryption of proposed system

In fig 2 show the decryption process, First we decrypt first block of message using EL Gamal algorithm. After that decrypt rest part using x-or operation. Now we get block cipher chain now we decrypt the cipher block and we gel over original message and text, Othello. text.

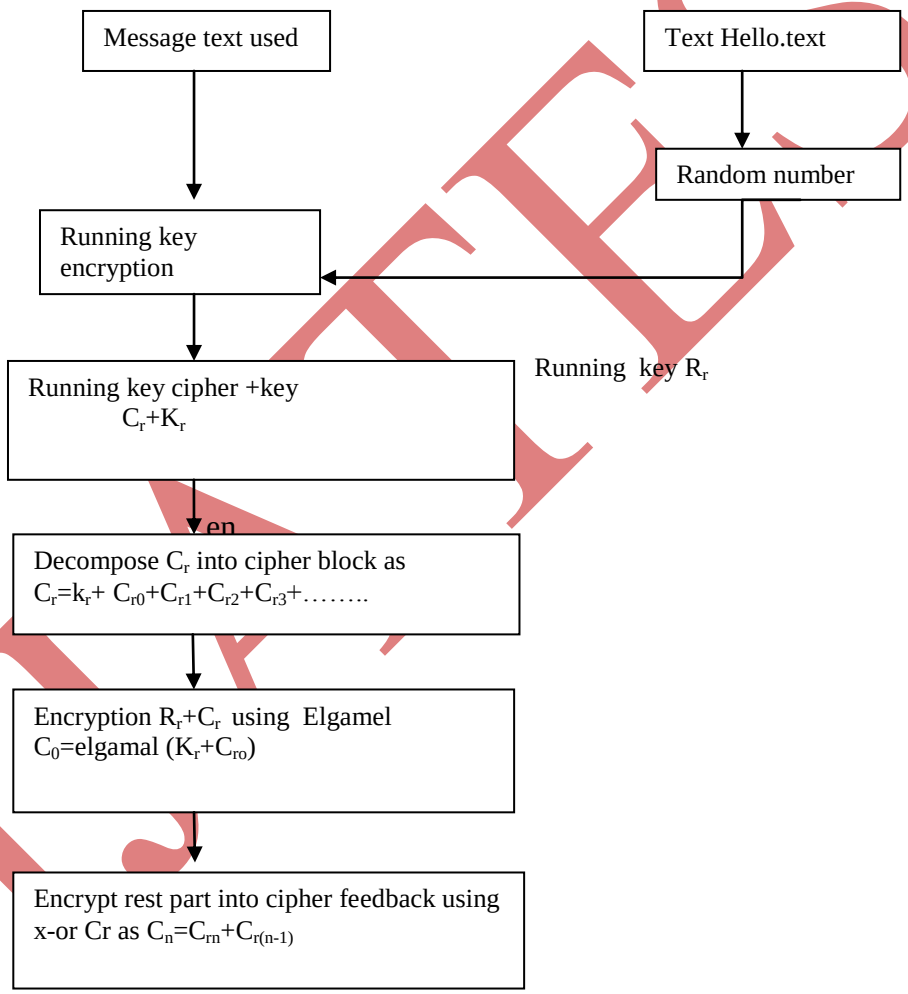
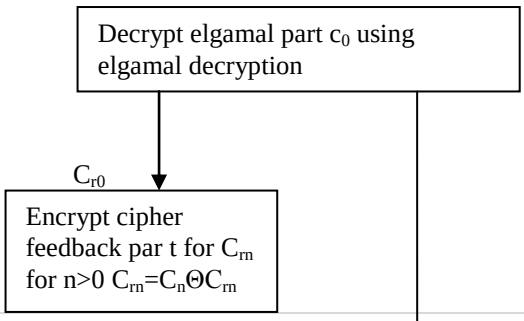


Fig1 Encryption Scheme of Proposed System



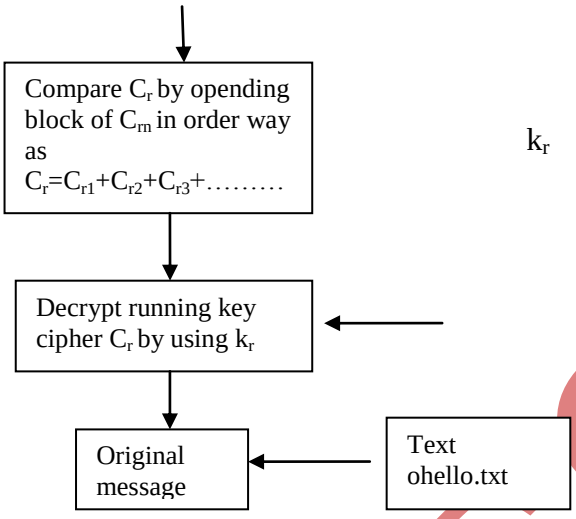


Fig 2 Decryption Scheme of Proposed System

V CONCLUSIONS

Higher level of security offered with lower processing overhead,.Advantages of Public key cryptography with simplicity of Private Key environment. A hybrid model which try to have advantages of both Public Key and Private Key cryptosystems The exhaustive operations of traditional private key algorithms are eliminated. The security lies totally on el gamal operations, which is approximately infeasible to break.terms of security has been greatly improved, which makes its scope of application even greater. The impact due to the increase of computation in the signature and verification operations will be weakened with the enhancement of the computing power of the processor.

The analysis of the improved algorithm modeled on the elgamel digital signature algorithm analysis is carrid out by comparsion .the new algorithm has its own characteristics ,especially after the increase in randam number ,there may be an attack methed which elgamal type digital signature it has not had .this is also the need of futher study.We also enhance the security by combining el g amal algorithm with any other algorithm.

REFERENCES

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[2] Myungsun kim, jihye kim, and Jung hee cheon "compress multiple cipher texts using elgamal encryption schemes" 2010 mathematics subject classification.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEETrans. Inform. Theory*, vol. IT-22, pp. 644–654, Nov. 1976.

[4] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," in Proc. 20th IEEE Symp. Foundations of Computer Science 1979, pp. 55-60.

[5] Federal Information Processing Standards Publication, National Institute of Standards and Technology. [Online]. Available: http://www.itl.nist.gov/fipspubs

[6] National Institute of Standards and Technology, Digital Signature Standard (DSS), "Federal Information Processing Standards Publication,",FIPS PUB 186-2, Reaffirmed, January 27, 2000.

[7] A. Arazi, "Integrating a key cryptosystem into the digital signature standard,"*Electron. Lett.*, vol. 29, no. 11, pp. 966–967, 1993.

[8] Yiannis Tsiounis, Moti Yung. On the Security of ELGamal Based Encryption[J]. Computer Science,1998.Vol.1431:117-134.

[9] Xiaofei Li, Xuanjing Shen and Haipeng Chen, ElGamal Digital Signature Algorithm of Addinga Random Number, IEEE 2011.

[10] *International Journal of Computer Applications (0975 – 8887) Volume 74– No.19, July 2013* Using El Gamal Cryptosystem in Message Feedback Mode for Computing Cost Reduction.

[11] Miller, Frank, *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. C.M. Cornwell. 1882

[12] Steven M. Bellovin , Matt Blaze Cryptographic Modes of Operation for the Internet, AT&T Labs Research.

[13]Wikimedia;"RunningKeyCipher",WikipediaTheEncyclopedia@ http ://en.wikipedia.org/wiki/Running_key_cipher retrieved Aug 2013.

[14] William Stallings; Cryptography and Network Security, Principles and Practice; Third edition; Pearson Education (Singapore), 2003.

[15]Steven M. bellovin ,problem area of ip security propocols,AT & T Labs Research.