Using El Gamal Cryptosystem in Message Feedback Mode for Computing Cost Reduction

Sohit Kumar
Scholar (Master of Technology)
Department of CS, SunRise University, Alwar
Rajasthan, India

Ashish Vashistha
Associate Professor
Department of CS, IET, Alwar
Rajasthan, India

ABSTRACT
This paper discuses comparatively more efficient and cost effective scheme of El Gamal Cryptosystem by introducing the concept of using the established cryptosystems into message feedback mode. The idea behind this is, "an established cryptographic scheme can be used to initiate any communication, and further users may switch to some lightweight process so that the degree of secrecy is maintained by means of the public key cryptosystem and the performance is achieved by using some other lightweight process. Approach discussed in this paper is of using message itself as One Time Pad (OTP), because any automation can't produce any random pad than a human being, and their messages posses same property. The length of Key used in El Gamal encryption and size of OTP determines the level of secrecy offered by the proposed system. Further a discussion is made upon the other dimensions of degree of security provided in such implementation. So as a result an applied approach is presented to design a data security mechanism for which users will use message itself as a One Time Pad and El Gamal Cryptosystem to initiate the operations and subsequent steps will involve simple XOR operations for cryptographic purpose.

General Terms
Cryptography, Network Security, Public Key Cryptosystem, El-Gamal Algorithm

Keywords
Discrete Logarithm , El Gamal Encryption, One Time Pad, Cipher Stream, Key Feedback, Message Feedback Mode.

1. INTRODUCTION
In 1984 Taher ElGamal who is also the inventor of SSL, presented a cryptosystem which is based on the Discrete Logarithm Problem. 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.

The basic idea behind the El Gamal Encryption [1] was that, it is possible to construct cryptosystems based on other difficult number-theoretic problems. Being more specific in El Gamal Encryption users deal with real numbers, like $log_a y$is the value x, so that$a^x = y$. One can define an analogous discrete logarithm [2] as El Gamal does. Let's have integers a and n, with a<n, the discrete logarithm of an integer y to the base a is an integer x, provide

$$a^x \equiv y \bmod n \qquad (1)$$

This is also referred to be index for which formula written

$$x = ind_{a,n} y. \qquad (2)$$

Users may efficiently raise numbers to large power modulo p by making a use of repeated squaring algorithm [3], its inverse computation is more complex so does El Gamal encryption relies on this complexity.

Here a model for Lightweight and computationally more cost effective scheme of El Gamal encryption's implementation is introduced which provide the level of security of the higher order of counterpart symmetric ciphers [4]. The private key is used of the form of One Time Pad and for each cryptographic step a new Key with automatic update is used through message feedback approach. Hence no Key exchange is required rather than the first step where users establish a session [5] by making use of El Gamal encryption.

This paper is divided into total of seven sections. This 1st section deals with introductory part. 2nd section describes terminology and definitions of frequently used key terms throughout the paper. 3rd and 4th section deals with the limitations associated with the stand alone implementations of public key cryptographic systems and One Time Pad respectively, which in terms also conclude that, there exists no specific mechanism or algorithms which implement One Time Pad. Section 5 describe proposed model which utilize conceptual parts of both public key cryptographic systems and One Time Pad. 6th section is about the results and discussion while the paper is concluded in 7th section.

2. TERMINOLOGY & DEFINITIONS

2.1 One Time Pad

In cryptography, the one-time pad (OTP) [6] is a type of encryption mechanism, which is already proved in various literatures to be impossible to crack if used properly. Every bit or bit-sequence from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or *pad*) of the same length as the plaintext, will produce a cipher text. If the pad or key is chosen randomly, and its length is equal to the length of plain text or is greater than the plaintext to be enciphered, and never used again neither in whole or partially and always kept secret, the cipher text will be impossible to decrypt or break without having knowledge about the key. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys.

2.2 Message feedback mode

In any cryptographic approach once session key is established by using any of existing public key cryptosystem and the first stream of message having sufficient number of bits is securely transferred, now in Message feedback mode [7] the message stream of previous cryptographic step is used as a Private Key of One Time Pad forms. Security [8] of such model is completely dependent over the public key cryptosystem used and session establishment mechanism

3. LIMITATIONS ASSOCIATED WITH STAND ALONE IMPLEMENTATION El GAMAL ENCRYPTION

Whenever a data is in transition over the network, its security is essential. To achieve security objectives users use cryptographic techniques in order to protect data from collision with other entities over the network. Processing of cryptographic approaches require numerous resources and many hosts or nodes will get significant benefits in their performance if the processing load [9] is reduced. In this context discussion is made upon El Gamal encryption in terms of its processing overhead [10], authentication and confidentiality. Cryptography also creates some drawbacks along with resolution of security issues [11]. Major part of these drawbacks is processing overhead. No perfect cryptosystem have been developed so far. So person concerned with higher degree of system security keep trying to make the encryption approaches more complex to make system rigid against security threats. Now these complex approaches take more time and resources to encipher a message as the complexity of the system is increased. As a result more security require more time on communication. Data overhead is also associated significantly.

4. LIMITATIONS ASSOCIATED WITH STAND ALONE IMPLEMENTATION OF ONE TIME PAD

There exists no specific mechanism or algorithms which implement One Time Pad. Basically One Time Pad is found more in literature and conceptual contexts than in any working model [12]. Further when users start working with the idea of making use of One Time Pad the very first question which arrives was that how he or she can implement a session establishment? Encryption was moon too far before resolving session establishment. But this dual problem was the actual solution. Proposed system combines both problems into one by making use of a compound system which on very first step establish session and message encrypted during this phase will be used as One Time Pad for next step [13]. Subsequent steps will use message encrypted on previous step and this leads to the idea of using established encryption algorithm into Message Feedback Mode

5. PROPOSED MODEL

The proposal is consisting of two step cipher scheme. Initially users establish and exchange the key element of the El Gamal Encryption, where the communication initiator device 'A' sends a communication request to device 'B'. Device 'B' responds with its public key triplet (p, g, y) of El Gamal Encryption. Now in the scenario where the flow of the data stream is from Device 'A' to Device 'B', i.e. Device 'A' acts as a sender and Device 'B' acts as a receiver. Now the cryptographic operations can be sought of a two step process;

1. El Gamal Encryption Mode
2. Message feedback mode

In El Gamal Encryption mode a session key is established and the first stream of message having 128 bits is securely transferred. In Message feedback mode the message stream of previous cryptographic step is used as a Private Key of One Time Pad forms. Security of the model is completely dependent over the El Gamal Encryption session establishment mechanism. The detailed operations are as:

1) El Gamal Encryption Mode:

   a) El Gamal Encryption Public key elements are shared between communicating devices, and after this Device 'B' having key elements (p, g, y) and (p, x) both. Device 'A' have public key element (p, g, y) only.

   b) Device 'A' encrypts the very first message stream M_0 having 128 bits into cipher stream c_0 using the public key (p, g, y) of Device 'B'.

   c) Device 'A' transmits c_0 to Device 'B'.

   d) On receiving of c_0 Device 'B' decrypts it using his own private key (p, x) and get m_0.

2) Message feedback mode: After El Gamal operations on very first message stream M_0 of 128 bit subsequent message streams M_n can be ciphered with the help of M_{n-1} using it as One Time Pad for X-OR operation.

   a) Encryption at Device A

For M_n where n>0

$$C_n = M_n \oplus M_{n-1} \quad \ldots\ldots (3)$$

   b) Decryption at Device B

For C_n where n>0

$$M_n = C_n \oplus M_{n-1} \quad \ldots\ldots (4)$$

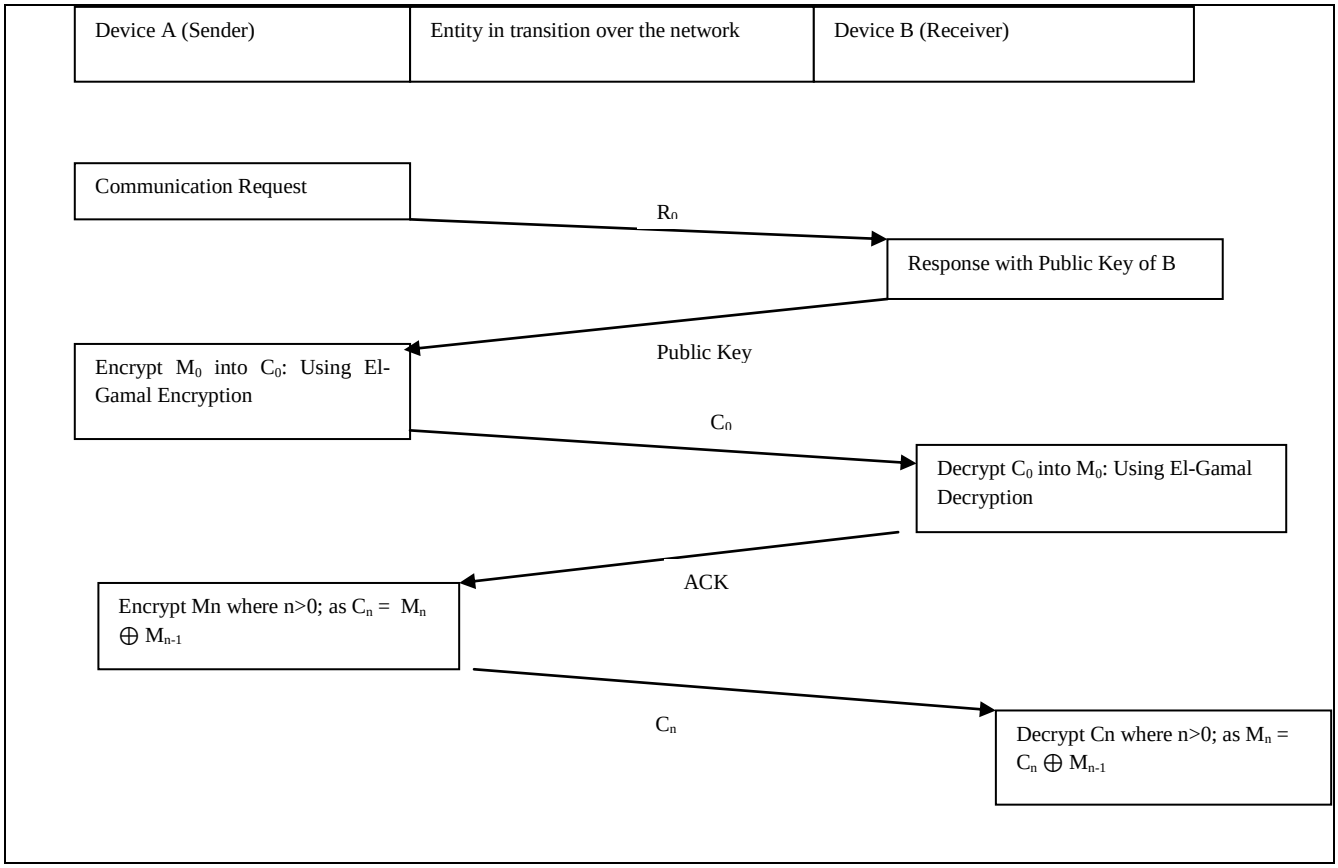

Fig. 1: Data Flow in proposed model

Now proof systems for cryptographic validation and significance for both the El Gamal Encryption and XOR operation is well established in various cryptographic literatures so these sections are eliminated, validation of this proposed scheme is done here via a working example carried out using the scheme proposed.

6. RESULTS AND DISCUSSION

To determine the correctness of working of proposed system let's have two communicating parties, Henna and Ron, where Ron wants to send some message to Henna using her public key. In order to calculate key for this system let Henna chooses

A Large Prime: $pA = 107$,

A Primitive root $\alpha A = 2$,

A Random Integer $dA = 67$,

And she computes $\beta A \equiv 2^{67} \ (mod\ 107) = 94$

Her public key is

$(pA, \alpha A, \beta A) = (107, 2, 94)$ And her private key is $dA = 67$.

Now let Ron wants to send following message to Henna

BEST WISHES FOR YOUR B'DAY

So starting the enciphering in El-Gamal mode, Ron will encrypt first object that is B using the El-Gamal Crypto system.

Now Ron wants to encrypt the message "B" (66 in ASCII) for Henna.

He chooses a random integer k = 45 and encrypts M = 66 as

$$(r, t) = (\alpha A^k, \beta A^k\ M) = 2^{45}, 94^{45}66)$$
$$= (\mathbf{28}, \mathbf{9})\ (mod\ 107)$$

He sends the encrypted message $(28, 9, 107)$ to Henna. So in simplest ASCII format first 24 bits of cipher will be interpreted as

Table 1: Sample Format of cipher message generated though El Gamal Approach

Place	Bit 1-8	Bit 9-16	Bit 17-24
Cipher Value	28	9	107
Binary	00011100	00001001	01101011

It is relevant to mention that increasing the size of block and / or key also enhances the secrecy of the overall system. Subsequent parts of the message will be encrypted in message feedback mode by simple X-OR as

$C_i = M_i \oplus M_{i-1}$

Table 2: Sample of a complete encryption process of proposed model

SENDER END			
TEXT	DECIMAL EQUIVALENT	ASCII	CIPHER GENEREATED
B	66	01000010	00011100000010010 1101011
E	69	01000101	00000111
S	83	01010011	00010110
T	84	01010100	00000111
<SPACE>	32	00100000	01110100
W	87	01010111	01110111
I	73	01001001	00011110
S	83	01010011	00011010
H	72	01001000	00011011
E	69	01000101	00001101
S	83	01010011	00010110
<SPACE>	32	00100000	01110011
F	70	01000110	01100110
O	79	01001111	00001001
R	82	01010010	00011101
<SPACE>	32	00100000	01110010
Y	89	01011001	01111001
O	79	01001111	00010110
U	85	01010101	00011010
R	82	01010010	00000111
<SPACE>	32	00100000	01110010
B	66	01000010	01100010
‘	39	00100111	01100101
D	68	01000100	01100011
A	65	01000001	00000101
Y	89	01011001	00011000

Henna receives the message$(r, t) = (28, 9, 107)$, and using her Private Key $d_A = 67$she decrypts to

$$tr^{-dA} = 9 * 28^{-67} \equiv 9 * 28^{106-67} \equiv 9.43 \equiv \mathbf{66}\ (mod\ 107)$$

Subsequent parts of the message will be decrypted in message feedback mode by simple X-OR as

$M_i = C_i \oplus M_{i-1}$

Table 3: Sample of a complete decryption process of proposed model

RECIEVER END			
CIPHER RECEIVED	DECRYPTED AS	DECIMAL EQUIVALENT	TEXT
000111000000100 101101011	01000010	66	B
00000111	01000101	69	E
00010110	01010011	83	S
00000111	01010100	84	T
01110100	00100000	32	<SPACE>
01110111	01010111	87	W
00011110	01001001	73	I
00011010	01010011	83	S
00011011	01001000	72	H
00001101	01000101	69	E
00010110	01010011	83	S
01110011	00100000	32	<SPACE>
01100110	01000110	70	F
00001001	01001111	79	O
00011101	01010010	82	R
01110010	00100000	32	<SPACE>
01111001	01011001	89	Y
00010110	01001111	79	O
00011010	01010101	85	U
00000111	01010010	82	R
01110010	00100000	32	<SPACE>
01100010	01000010	66	B
01100101	00100111	39	‘
01100011	01000100	68	D
00000101	01000001	65	A
00011000	01011001	89	Y

7. CONCLUSION

The main results drown from this work include in the form of both simplicity and security. Using the proposed system higher level of security can be achieved with lower processing overhead. The security level of proposed model has the same level of security to offer as El Gamal cryptosystem does. Further in message feedback mode user can easily increase the size of One Time Pad to enhance the security of lightweight process. Advantages of Public key cryptography with simplicity of Private Key environment is presented, where public key cryptographic approach is used to simply initiate the communication and once it is done a symmetric approach is adopted to enhance the speed of the operations, so in overall this is a hybrid model which try to have advantages of both Public Key and Private Key cryptosystems. This approach tries to eliminate the exhaustive operations of traditional private key algorithms. Message feedback ensures the data integrity while communication over a communication medium in Public domain. The half part of security lies on El Gamal operations, which is approximately infeasible to break, and the other half is dependent upon the size of the pad selected. Quite attractive feature of pad is that it uses simple bitwise XOR so allow user to increase the pad size without any processing overhead. Running time of proposed scheme is reduced as in message feedback mode users are applying XOR operations which have no doubt faster operational speed than El Gamal encryption.

8. ACKNOWLEDGMENTS

We heartily acknowledge our gratitude and thanks to the family, friends, faculties of IET group and all those who directly or indirectly contributed towards conceptualization of this paper.

9. REFERENCES

[1] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms". In Proceedings of CRYPTO 84 on Advances in Cryptology, pages 10–18, New York, NY, USA, Springer-Verlag New York, Inc. 1985.

[2] A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance", AT&T Bell Laboratories Murray Hill, New Jersey, APR 1998

[3] Cohen, H., Frey, G. (editors): Handbook of elliptic and hyper elliptic curve cryptography. Discrete Math Appl, Chapman & Hall/CRC (2006)

[4] Delfs, Hans & Knebl, Helmut. "Symmetric-key encryption", *Introduction to cryptography: principles and applications*. Springer, ISBN 9783540492436, 2007

[5] Wikipedia, "Session (computer science)", http://en.wikipedia.org/wiki/Session_(computer_science) Ret. May 2013

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

[7] J. Kowalchuk, B. P. Schanning, and S. Powers, Communication privacy: Integration of public and secret key cryptography, *NTC Conference Record*, Vol. 3, pp. 49.1.1-49.1.5, Dec. 1980.

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

[9] D. E. Knuth, *The Art of Computer Programming: Vol. 2*, Semi numerical Algorithms, 2nd ed. Addison-Wesley 1981.

[10] David D. Clark, Van Jacobson, John Romkey, and Howard Salwen, "An analysis of TCP processing overhead" IEEE Communication, MIT, 1984, @ groups.csail.mit.edu/ana/Publications/PubPDFs/An%20 Analysis%20of%20TCP%20Processing%20Overhead.pdf

[11] R. Merkle, Secrecy, authentication, and public key systems, Ph.D. dissertation, Dept. of Electrical Engineering, Stanford Univ., 1979

[12] Shannon, Claude E. (October 1949). "Communication Theory of Secrecy Systems", *Bell System Technical Journal* (USA: AT&T Corporation) 28 (4): 656–715. Retrieved June 2013

[13] Sohit Kumar, Praveen Kr. Vishnoi, Rahul Yadav, Dhirendra Yadav, "A Lightweight Stream Cipher for Mobile Devices Using RSA & Message Feedback", in the proceedings of IGTT' 2011, IET Alwar, Dec 2011.