*I.J. Mathematical Sciences and Computing,* **2017, 3, 39-49**
Published Online July 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2017.03.04

***Available online at*** ***http://www.mecs-press.net/ijmsc***

# Building Background to the Elgamal Algorithm

Toan Nguyen Duc [a], Hong Bui The [b]

[a] *Food industrial College,Viet Tri,Phu Tho, Viet Nam*
[b] *Hung Yen University of Technology and Education, Hung Yen, Viet Nam*

**Abstract**

In this paper, we develop a new encryption scheme based on the ELGAMAL encryption algorithm and the degree of difficulty of the discrete logarithm problem (DLP). In public key cryptography, a secret key is often used for a long period of time, thus expelling the secret key. Moreover, devices used to calculate cryptography can also be physically attacked, leading to the secret key being exposed. This paper proposes a new encryption scheme to reduce the risk of revealing a secret key.

**Index Terms:** ElGamal, discrete logarithm, secret key.



## 1. Introduction

In recent years cryptography uses and attaches more mathematics, encryption is more used in network security. This is a very important industry and has many uses in human social life. Along with the development of the Internet, cryptographic research has become increasingly diversified, opening up many areas of research in depth. Encryption applications not only encrypt and decode information but also cover a variety of issues that need to be investigated and resolved such as: authenticating the origin of information content, authenticating the owner of the lock code, The process of exchanging information securely online.

However, the security and coding time is the problem that algorithms tend to optimize in addition to the key exchange problem is also a general impediment to the algorithm. This issue may refer to two recent articles, one about the safety of Poincheval and Stern and the counterfeiting of Bleichenbacher's signature.

In order to overcome these obstacles, we propose to develop a new encryption scheme based on the ELGAMAL encryption algorithm and the difficulty of the discrete logistic problem (DLP).

The rest of the article is presented as follows. Part 2: Some basic concepts. Part 3: Eliminate the drawbacks of Elgamal; Part 4: Proposed new schema based on ElGamal ; Part 5: References.

* Corresponding author.
E-mail address: ductoanndt9@gmail.com, hongbuithe@gmail.com

## 2. Some Basic Concepts

### *A. ElGamal Encryption Definition [1,4]*

Elgama bile was proposed in 1984 on the basis of a discrete logarithm problem. Then, the US DSS [6] and GOST R34.10-94 [7] of the Russian Federation were developed on the basis of the digital signature algorithm of the cryptosystem, while the cryptographic algorithm The ElGamal public key has been used by the National Security Agency (NSA).

+) *Parametric and key shaping algorithms*

The members of the system want to exchange confidential information with Elgamma cryptographic algorithm, the key formation process is as follows:

1- Select prime numbers large enough $p$ so that the logarithm problem in $Z_p$is hard to solve.
2- Select $g \epsilon Z_p^*$ as the primitive element.
3- Select the secret key x as a random number such that: $1 < x < p$

Generic public key y according to the formula:

$$y = g^x mod p \tag{1}$$

+) *Encryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: $x_A$ and the public key is: $y_A$
The receiver B has a secret key of: $x_B$ and the public key is: $y_B$. Then, to send message M to B, with: $0 \leq M \leq p$, Sender A will perform the following steps:

1- Select the random number k satisfactory: $1 < k < p$. Calculate the R value by the formula:

$$R = g^k mod p \tag{2}$$

2- Use public key of B to calculate:

$$C = M \times (y_B)^k mod\ p \tag{3}$$

3- Send the code (C, R) to the receiver B.

+) *Decoding algorithms*

To retrieve the original message *(M)* from the ciphertext *(C, R)* received, the receiver B performs the following steps:

1- Calculate the Z value by the formula:

$$Z = R^{x_B} mod\ p = g^{k.x_B}\ mod\ p \tag{4}$$

2- Calculate the inverse of Z:

$$Z^{-1} = (g^{k.x_B})^{-1} \, mod \, p \; = \; g^{-k.x_B} \, mod \, p \tag{5}$$

3- Restore initial message (M):

$$C \; \times \; Z^{-1} \, mod \, p \tag{6}$$

+) *Correctness of Elgamal Cryptographic Algorithm*

Suppose the message received after decryption *(C, R)* is $\bar{M}$

$$\bar{M} \; = C \; \times \; Z^{-1} \, mod \, p \; = \; [(M \; \times (y_B)^k mod \, p) \times \; g^{-k.x_B} \, mod \, p] \, mod \, p$$

$$M \times g^{k.x_B} g^{-k.x_B} \; mod \, p = M \tag{7}$$

Thus, the message received after decoding *(M)* is the original message *(M).*

*B. Analyze and Reviews.*

+) *Analysis*

Let p be an element large enough: $p \; \geq 512 \; bits \; in \; size$
A is a primitive element in: $Z_p^* = \; Z_p/\{0\}$
A is a random integer number: $1 < a < p - 1$
The ELGAMAL secret system is a set of 5 components *(P, C, K, E, D);*
Where: $P = \; Z_p$, $C = \; Z_p \; \times Z_p$
Lock space $K = \{(p, \alpha, \beta, a)\}$ with $\beta = \; \alpha^a \; mod \; p$. For each: $k \; \in K \; ; k \; = (k_1, k_2)$
Where:
$k_1 = (p, \alpha, \beta)$ is the public key used to encrypt
$k_2 = a$ is the secret key used to decrypt and execute the digit.
E and D: For each $k \; \in K$, there exists a mapping $e_k \; \in E$
$E_k : P \; \rightarrow C$ and a mapping of $d_k \; \in D$ and
$d_k : C \; \rightarrow P$ such that $d_k \left(e_k(x)\right) = x \; for \; all \; x \in P$
In the ELGAMAL cryptosystem, the $e_k$coding function and decryption function are chosen as follows:
Let: $x \; \in P$ and select a random number (secret):

$$r \in \; Z_{p-1}^*; \; e_k(x) = \; y_1, y_2 \tag{8}$$

Where:

$$y_1 = \; a^r \; mod \; p \; and \; y_2 = \; x\beta^r \; mod \; p \tag{9}$$

Thus $y_1, y_2$ is the cipher block corresponding to the plain block *x*.
The decoding function:

$$d_k = \; y_2 (y_1^a)^{-1} \, mod \, p \tag{10}$$

It is easy to test that:

$$d_k\big(e_k(x)\big) = x \; for \; every \; x \in P \tag{11}$$

+) *Reviews.*

- Obviously, in the ELGAMAL code the length of each block would be twice the length of each block. Thus it occupies a lot of capacity and time to transmit ciphertext. The greater the length of the notice, the greater the amount of cached code and transmission time.
- If there are two identical blocks in the message, the two corresponding blocks of code are equal. This is a vulnerability for cryptographic analysts. Based on the above comment, the proposed ElGamal algorithm improvement could overcome these two disadvantages.

## 3. Eliminate the Drawbacks of Elgamal

To overcome weakness 2 of the above comment, we do the following:

Suppose we want to encode an X message with an ELGAMAL encryption algorithm. First of all, we use the displacement method with the displacement key:

$$k \in K = \{\pi: \{1,2,\dots,m\} \to \{1,2,\dots,m\}\} \tag{12}$$

Where: m is an arbitrary natural number but not too small.

Using the ek transformation algorithm we have: $e_k(X) = Y$

We then use the ELGAMAL password to encrypt the ciphertext instead of the plaintext X.

Thus, there is absolutely no code block in the Y code, and therefore there is no fear of duplication of blocks in the ciphertext of the ELGAMAL encryption algorithm.

Thus the second weakness of the ELGAMAL cryptosystem is overcome.

To overcome the first disadvantage, we do the following:

Given that p is a large prime number (larger than or equal to 512 bits) so that *p-1* has an elemental atom with a size greater than or equal to 160 bits, we denote the elemental nucleus as Q. Now consider the ELGAMAL cryptosystem with clear space $Z_q$ (not $Zp$).

The cipher space would be: $Zq \; x \; Zq$.

The public key is $k_1 = (p, q, \alpha, \beta)$

The secret key is $k_2 = a \; (1 < a < q - 1)$

Encoding process:

Suppose $x \; \epsilon \; Z_q$ and the public key are $k_1 = (p, q, \alpha, \beta)$,

Randomize and keep some secret $r \; \epsilon \; Z_{q-1}$

Calculate $(x) = (y_1, y_2)$

Where: $y_1 = (\alpha^r mod p) \; mod q, y_2 = (x \; (\beta^r) \; mod p) \; mod q$.

Process decoding.

Put $(y_2 \; (y_1^a)^{-1} \; mod p) \; mod q = x$.

Prove

We have:

$$(y_2 \; (y_1^a)^{-1} \; mod p) mod q \tag{13}$$

Instead of $y_1$ and $y_2$ we have:

$$(x\ (\beta^r) mod p) mod q\big((\alpha r\ mod p) mod\ q_a\big) - 1\ mod)\ mod\ q \quad (14)$$

$$= (x(\alpha^{ra})(\alpha^{ra})^{-1} mod p) mod\ q = xmdp = x(x < q) \quad (15)\text{(Must prove)}$$

Swap key locks:

Depending on the length and shortness of the displacement key, we can divide it into one or two blocks of not more than 160 bits in size, which are then placed at the end of the transcript. Then the code is normal and informs the real destination first.

After receiving the ELGAMAL code, the receiver will decrypt normally and know that the last / last block is the transposition key, so that the receiver will solve the transposition code to find out the message from the person. sends.

## 4. Proposed New Schema based on ElGamal

+) *Parametric and key formation [2]*

- Choose a pair of prime numbers p and q with $(p - 1\ /\ 2q)$ as prime numbers.
- Select random primes $p_1$with length $\left|p\right| - \left|q\right| - 1$.
- Select g as the primitive element: $g \in Z_p$ Assuming the sender is A, the receiver is B. The key exchange on the DLP problem with general parameters is $(p, q, g)$. In which A has the secret key: $x_A \in [1, q - 1]$.

The public key is: $y_A . y_A = g^{x_A} mod\ p$
B has a secret key: xB, the public key is: $y_B$.

$$y_B = g^{x_B}\ mod\ p \quad (16)$$

- Choose hash function safe (Hash): $H\ \{0,1\}^* \rightarrow Z_q$ This algorithm can be attacked when reusing x. So we use the value $H\ (x \mid M \mid)$ instead of x.

Then the public key will be calculated according to the formula:

$$y_A = {g_A}^{H(x \| M)}\ mod\ p \quad (17)$$

$$y_B = {g_B}^{H(x \| M)}\ mod\ p \quad (18)$$

*A). Encryption and decryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: $x_A$ and the public key is: $y_A$
The receiver B has a secret key of : $x_B$ and the public key is: $y_B$. Then, to send message M to B, with: $0 \leq M < p$, Sender A will perform the following steps:

1. Select the random number k satisfactory: $1 < k < p$. Calculate the R value by the formula:

$$R = g^k\ mod\ p. \quad (19)$$

2. Use public key of B to calculate:

$$C = M \times (y_B)^k \bmod p \tag{20}$$

3. Send the code (C, R) to the receiver B.

+) *Decoding algorithms*

To retrieve the original message (M) from the ciphertext (C, R) received, the receiver B performs the following steps:

1. Calculate the Z value by the formula:

$$Z = R_B^{H(x\|M)} \bmod p \tag{21}$$

2. Calculate the inverse of Z:

$$Z^{-1} = (g_B^{H(x\|M)})^{-1} \bmod p = g_B^{-H(x\|M)} \bmod p \tag{22}$$

3. Restore initial message (M):

$$M = C \times Z^{-1} \bmod p \tag{23}$$

+) *Correctness of Elgamal Cryptographic Algorithm*

Suppose the message received after decryption (C, R) is $\bar{M}$

$$\bar{M} = C \times Z^{-1} \bmod p \tag{24}$$

$$= [(M \times (y_B)^k \bmod p) \times (g_B^{-k.H(x\|M)} \bmod p)] \bmod p$$

$$= M \times g_B^{k.H(x\|M)} \times g_B^{-k.H(x\|M)} \bmod p = M \tag{25}$$

Thus, the message received after decoding (M) is the original message (M).

*B). Encryption and decryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: $x_A$ and the public key is: $y_A$.
The receiver B has a secret key of : $x_B$ and the public key is: $y_B$. Then, to send message M to B, with: $0 \leq M < p$, Sender A will perform the following steps:

Step 1: Person A

1- Select the random number k satisfactory: $1 < k < p$.
2- Select : $K_A \in Z_q$

3- Calculating $R_A = g_A^{H(x \| M)} mod\ p$
4- Calculate $K_A = (R_B \times g_B)^{H(x \| M)} mod\ p$
5- Key function: $K = H(y_B^{K_A}, R_A, d)$, where d is the time of label
6- Calculate $C = M \times g_B^{H(x \| M)} mod\ p$
7- Send $R_A, d, C\ to\ B$

Step 2: Person B

8- Select $K_B \in Z_q$.
9- Calculate $K_B = (R_A \times g_A)^{H(x \| M)} mod\ p$
10- Calculate $R_B = g_B^{H(x \| M)} mod\ p$
11- Calculate $K = H(R_A^{H(x \| M}, R_A, d)$
12- Calculate $\bar{M} = C \times \overline{R_A})^{H(x \| M} mod\ p$
13- Testing: $E_A = E_A'$
14- If the wrong stop, the transaction fails
15- If true then the post-decrypt message is safe and is the original message

+) *Prove the correctness of the algorithm:*

If $K_A = K_B$

$$K_A = (y_B \times R_B)^{H(x \| M)} = g_B^{H(x \| M)} \times R_B^{H(x \| M)} \quad (26)$$

$$= g_A^{H(x \| M)} \times R_A^{H(x \| M)} = (R_A \times g_A)^{H(x \| M)} \quad (27)$$

Similarly we will prove: $\bar{M} = M$ when $g_A = g_B$
We have:

$$\bar{M} = C \times (\overline{R_A})^{H(x \| M)} mod p \quad (28)$$

$$= M \times (y_B)^{H(x \| M)} \times (\overline{R_A})^{H(x \| M)} \quad (29)$$

Which: $y_B = g_B^{H(x \| M)}$
That $R_A = g_A^{H(x \| M)}\ should\ \overline{R_A} = g_A^{H(x \| M)}$
replace the formula we have:

$$\bar{M} = M \times (y_B)^{H(x \| M)} \times (\overline{R_A})^{H(x \| M)}$$

$\bar{M} = M$ (Article must prove) (30)

*C). Encryption and decryption algorithms*

+) *Encryption algorithms*

Suppose the sender is A, the receiver is B. The sender A has the secret key: $x_A$ and the public key is: $y_A$.

The receiver B has a secret key of: $x_B$ and the public key is: $y_B$. Then, to send message M to B, with: $0 \leq M < p$, Sender A will perform the following steps:

1- Select the random number k satisfactory: $1 < k < p$.
2- Calculate the value of R according to the formula: $R = g^k mod\ p$ (31)
3- Calculate the value of E according to the formula: $E = H(R \| M)\ mod\ p$ (32)
4- Calculate the value of S according to the formula: $S = [k + x_A \times E]\ mod\ p$ (33)
5- Use public key of B to calculate C by formula: $C = M \times (y_B)^k\ mod\ p$ (34)
6- Sen to B (C,E,S)

+) *Decryption algorithms*

From the C code (C, E, S) received, B retrieved and checked the origin and integrity of the original M message as follows:

1- Calculate the value of R according to the formula: $\bar{R} = g^s \times (y_A)^E mod\ p$ (35)
2- Restore original message by formula: $\bar{M} = C \times (\bar{R})^{x_B} mod\ p$ (36)
3- Calculate the value of E according to the formula: $\bar{E} = H(\bar{R} \| \bar{M})\ mod\ p$ (37)
4- Check if: $\bar{E} = E\ then\ \bar{M} = M$ and M has a source from sender A

+) *Prove:*

Replace 33 with 35 we have:

$$\bar{R} = g^s \times (y_A)^E mod\ p$$

$$= g^{k+x_A} \times (g^{-x_A})^E mod\ p \quad (38)$$

$$= g^k \times g^{x_A \times E} \times g^{-x_A \times E} mod\ p$$

$$= g^k\ mod\ p$$

From 38 it follows:

$$\bar{R} = g^k\ mod\ p \quad (39)$$

Replace 34, 40 with 36 we have:

$$\bar{M} = C \times (\bar{R})^{x_B} mod\ p$$

$$= \{M \times (y_B)^k mod\ p \times (g^k)^{x_B}\ mod\ p\} mod\ p \quad (40)$$

$$= M \times g^{-kx_B} \times g^{kx_B}\ mod\ p = M$$

From 38 it follows:

$$\bar{R} = R$$

Replace 40, 41 with 37 we have:

$$\bar{E} = H\,(\bar{R} \,\|\, \bar{M})\ mod\ p$$

$$= H\,(R \,\|\, M)\ mod\ p\ = E\quad (Article\ must\ prove)$$

+) *Improved algorithm security:*

1. Antispam capabilities
2. The ability to prevent spoofing of the origin and content of the newsletter.

The article proposes a new encoding scheme based on the *ELGAMAL* encryption algorithm and the difficulty of the discrete logarithm problem *(DLP).* However, with prime q of size 160bit to solve the discrete Logarithm problem $y_A = g^xA\ mod\ p$, where $g$ is an element of $q$ in $Z_p$, it should use $O\ (2^{80})$ operations, with the current methods post This math is very difficult to solve. The proposed encryption scheme addresses the disadvantages of revealing a secret key for a period of time, and the applicability of the advanced algorithm is fully applicable in practice.

## 5. Concude

This article proposes improvements to the ELGAMAL encryption algorithm. The proposed encryption algorithm has solved the disadvantages of the ELGAMAL algorithm and the application capabilities of the advanced algorithm are fully applicable in practice.

Ciphertext size has been significantly reduced: each code block has been reduced to 2.3 times. Thus, each code block of normal ELGAMAL cryptography is about 1024 bits in size, now it is reduced to only 320 bits. Since then, the first weakness has been resolved. Here, we need to take note of the prime number p. In order to obtain the prime factor q of 160 bits, the prime number p must not be large enough, but also prime numbers. There is now an algorithm for finding large and strong prime numbers [3].

The article proposes a new encoding scheme based on the ELGAMAL encryption algorithm and the difficulty of the discrete logarithm problem (DLP). However, with prime q of size 160bit to solve the discrete Logarithm problem yA = gxA mod p, where g is an element of q in Zp, it should use O (280) operations, with the current methods post This math is very difficult to solve. The proposed encryption scheme addresses the disadvantages of revealing a secret key for a period of time, and the applicability of the advanced algorithm is fully applicable in practice.

## References

[1] Nguyen Binh, Nguyen Minh Trung, *"Some Modified Forms of the ELGAMAL Cryptosystem on Discrete Logical Problem"*, Institute of Technology, Post and Telecommunications, 2016.

[2] Nguyen Quoc Toan, Do Dai Chi, Trieu Quang Phong *"On a parameter standard for discrete logarithm problem"* Journal of Information Security, Government Cipher Board, (2016).

[3] Luu Hong Dung, *"Development of public key cryptography algorithm based on ElGamal Cryptosystem"*, Specialized Research, Development and Application of Information and Communication Technology, Journal of Science and Technique Institute of Psychology), No. 149 (08-2012).

[4] D. Pointcheval, J. Stern. *"Security proofs for signature schemes"*, EUROCRYPT'96, vol. 1070, pp. 387-398, 1996.

[5] D. Bleichenbacher, *"Generating ElGamal Signatures Without Knowing the Secret Key"*, EUROCRYPT'96, vol. 1070, pp. 10-18, 1996.

[6] National Institute of Standards and Technology, NIST FIPS PUB 186-3. Digital Signature Standard, U.S. Department of Commerce, 1994.

[7] GOST R 34.10-94. Russian Federation Standard. Information Technology, "*Cryptographic data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm"*, Government Committee of the Russia for Standards, 1994 (in Russian).

[8] Luu Hong Dung, Nguyen Duc Thuy, Le Dinh Son and Nguyen Thi Thanh Thuy, *"A method for constructing a digital signature scheme based on discrete logarithms"*, the IXth National Conference on Basic Research and Applications (FAIR 2016). ISBN: 978-604-913-397-8., Page 6, 01/10/2016.

[9] [9] Hoang Van Viet, Bui The Truyen, Tong Minh Duc and Luu Hong Dung, *"Разработка алгоритма определения новых ключей для симметричной ключевой криптосистемы/ New key established algorithms for symmetric key cryptosystems, Журнал «Наукоемкие технологии»* №1 за 2016 г. Издательство "Радиотехника": научно-техническая литература., pp. 8, 01/03/2016

[10] Luu Hong Dung, Le Dinh Son, Ho Nhat Quang and Nguyen Duc Thuy, *"DEVELOPING DIGITAL SIGNATURE SCHEMES BASED ON DISCRETE LOGARITHM PROBLEM"*, The 8th National Conference on Fundamental and Applied IT Research (FAIR 2015). ISBN: 978-604-913-397-8., pp. 8, 05/01/2016.

[11] Nguyen Duc Toan, Nguyen Van Tao, *"Design of pseudo-random maximal sequence generators"*, Journal of Science and Technology, Specialist in Natural Science and Technology - Thai Nguyen University, Vol. 159, No. 14, pp. 115-118, ISSN 1859-2171, 2016.

[12] Nguyen Duc Toan, Bui The Hong, Nguyen Van Tao, Tran Manh Huong, *"Encryption and message authentication using cryptographic algorithms with one-time keys"*, Basic Research and Application of Information Technology "( FAIR'9), Natural Science and Technology Publishing House ISBN 978-604-913-472-2, tr 284-289, in Cantho, April 4-5, 2016.

[13] Nguyen Duc Toan, Nguyen Van Tao, *"Combining OTP code and block coding to encode and decode message"* National Conference on Electronic Communications and Information Technology REV / ECIT 2016, Industrial and Commercial Publishing House, Topic: 4-1, Hanoi, 23-24 December 2016.

[14] Nguyen Duc Thuy, Nguyen Tien Giang, Le Dinh Son and Luu Hong Dung, *"A Design Method of Digital Signature Scheme Based on Discrete Logarithm Problem*", IJCSNS International Journal of Computer Science and Network Security. Vol. 17 No. 2 pp. 214-218, February 2017. ISSN: 1738 - 7906., pp. 6, 11/03/2017

[15] Nguyen Duc Thuy and Luu Hong Dung, *"A New Construction Method of Digital Signature Algorithms"*, IJCSNS International Journal of Computer Science and Network Security. Vol. 16 No. 12 pp. 53-57, December 2016. ISSN: 1738 - 7906., pp. 6, 13/01/2017

[16] Nguyen Duc Toan, Nguyen Van Tao, Bui The Hong *"A pseudorandom bit pattern evaluation"*, Journal of Science and Technology, Journal of Natural Science and Technology - Thai Nguyen University, ISSN 1859-2171. 2017.

[17] Nguyen Duc Toan, Bui The Hong, Nguyen Van Tao, *"Some Statistical Standards Applied in Cryptography"*, Journal of Science and Technology, Volume 46, Hanoi University of Pedagogy, ISSN 1859-2325, 2017.

**Authors' Profiles**

**Toan Nguyen Duc**, Graduated Master Degree in 2015. Current College of Food Industries. Studying for PhD in Thai Nguyen University. Research area: Security and confidential information. Email: *ductoanndt9@gmail.com*

**Hong Bui The**, Graduated from Hanoi University. Associate Professor Ph.D. Show art at Hung Yen University of Technical Education. Areas of Study: Password Security and Security, Cryptography, Machine Learning. Email: *hongbuithe@gmail.com*

**How to cite this paper:** Toan Nguyen Duc, Hong Bui The,"Building Background to the Elgamal Algorithm", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.3, No.3, pp. 39-49, 2017.DOI: 10.5815/ijmsc.2017.03.04