Composite ElGamal Cryptosystem and An Application of The Cryptosystem to Asymmetric Cryptography

C. ÖZYILMAZ[1] and A.NALLI[2]

[1] Ondokuz Mayıs University, Samsun/Turkey, cagla.ozyilmaz@omu.edu.tr
[2]Karabuk University, Karabuk/Turkey, aysenalli@ karabuk.edu.tr

***Abstract* - In this paper, we have defined a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules and we have constructed a new ElGamal cryptosystem based on the a new discrete logarithm problem. We have called the new system as Composite ElGamal cryptosystem. Then we made an application of Composite ElGamal cryptosystem to asymmetric cryptography and finally we have compared that Composite ElGamal cryptosystem and ElGamal cryptosystem in terms of cryptography and we have obtained that Composite ElGamal cryptosystem is more advantageous than ElGamal cryptosystem.**

***Keywords* - Composite ElGamal cryptosystem, Asymmetric cryptography, Discrete Logarithm problem.**

I. INTRODUCTION

THE fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, can't understand what is being said. This channel could be a telephone line or computer network, for example. The information that Alice wants to send to Bob, which we call ‘ plaintext ’, can be English text, numerical data, or anything at all- its structure is completely arbitrary. Alice encrypts the plaintext, using a predetermined key, and sends theresulting ciphertext over the channel. Oscar, upon seeing the ciphertext in the channel by eavesdropping, can't determine what the plaintext was; but Bob, who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext.

These ideas are described formally using the following mathematical notation.

Definition 1.1. A crptosystem is a five–tuple (P,C,K,E,D) where the following conditions are satisfied:

1. P is a finite set of possible plaintexts;
2. C is a finite set of possible ciphertexts;
3. K is a finite set of possible keys;
4. For each $K \in K$, there is an encryption rule $e_K \in E$ and a corresponding decryption rule $d_K \in D$. Each $e_K : P \to C$ and $d_K : C \to P$ are functions such that $d_K(e_K(x)) = x$ for every plaintext element $x \in P$ [1].

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system

* Symmetric Cryptography (Secret key cryptosystems)
* Asymmetric Cryptography (Public key cryptosystems)

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key. Algorithms for symmetric cryptography, such as DES [2], use a single key for both encryption and decryption and algorithms for asymmetric cryptography, such as the RSA [3] and ElGamal cryptosystem[4], use different keys for encryption and decryption.

In this study, we have constructed a new ElGamal cryptosystem and a new Discrete Logarithm problem similar to the ElGamal cryptosystem and Discrete Logarithm problem to be used composite modules. So, firstly we will define Discrete Logarithm problem and ElGamal Cryptosystem based on the Discrete Logarithm problem which is only used prime modules.

Definition 1.2. Given a generator α of $\mathbb{Z}_p^*$ for most appropriately large prime p, $f(a)$ is easily computed given α , a, and p; but for most choices p it is difficult, given (y; p; α), to find an a in the range $1 \le a \le p-1$ such that $\alpha^a (\bmod p) = y$. The difficult direction is known as the **Discrete Logarithm problem**[5]

Now, we cite public-key cryptosystems based on the **Discrete Logarithm problem.** The first and best-known of these is the ElGamal Cryptosystem. ElGamal proposed a public-key cryptosystem which is based on the Discrete Logarithm problem in ($\mathbb{Z}_p^*$, .). The encryption operation in the ElGamal Cryptosystem is randomized, since ciphertext depends on both the plaintext x and on the random value k chosen by Alice. Hence, there will be many ciphertexts that are encryptions of the same plaintext.

Definition 1.3. Let p be a prime number such that the Discrete Logarithm problem in ($\mathbb{Z}^*_p$, .) is infeasible, and let $\alpha \in \mathbb{Z}^*_p$ be a primitive element. Let $P = \mathbb{Z}^*_p$, $C = \mathbb{Z}^*_p \times \mathbb{Z}^*_p$ and define $K = \left\{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \,(\mathrm{mod}\, p)\right\}$. The values p, α, β are the public key, and a is the private key. For $K = (p, \alpha, a, \beta)$, and for a (secret) random number $k \in \mathbb{Z}_{p-1}$, define $e_K(x, k) = (y_1, y_2)$, where

$$\begin{aligned} y_1 &= \alpha^k \,(\mathrm{mod}\, p) \\ y_2 &= x\beta^k \,(\mathrm{mod}\, p) \end{aligned}.$$

For $y_1, y_2 \in \mathbb{Z}^*_p$, define $d_K(y_1, y_2) = y_2 (y_1{}^a)^{-1} \,\mathrm{mod}\, p$ [1].

II. Composite Discrete Logarithm Problem and Composite ElGamal Cryptosystem

In this section, we will define a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules. To do this we need to following theorem.

Theorem 2.1. $\mathbb{Z}^*_m$ is cyclic and multiplicative group if and only if $m=2$, $m=4$ or $m=p^k$ or $m=2p^k$ such that $p \neq 2$ prime number [6].

Definition 2.1. Given a generator α of $\mathbb{Z}^*_m$ for most appropriately large m (m is one of the modulus which providing Theorem 2.1. and so we have found most appropriately large module m), $f(\lambda) = \alpha^\lambda \,(\mathrm{mod}\, m)$ is a one-way function. $f(\lambda)$ is easily computed given λ , α , and m ; but for most choices m it is difficult, given (y ; m ; α), to find an λ such that $\alpha^\lambda \,(\mathrm{mod}\, m) = y$. We have called difficult direction as the **Composite Discrete Logarithm problem**.

Now, we will obtain public-key cryptosystem based on Composite Discrete Logarithm problem. We have called the new cryptosystem as the **Composite ElGamal Cryptpsystem**.

Definition 2.2. Let m be a positive integer such that the Composite Discrete Logarithm problem in ($\mathbb{Z}^*_m$, .) is infeasible, and let $\alpha \in \mathbb{Z}^*_m$ be a primitive element(generator). Let

$P = \mathbb{Z}_m \backslash \{0\}$, $C = \mathbb{Z}^*_m \times (\mathbb{Z}_m \backslash \{0\})$

and define $K = \left\{(m, \alpha, \lambda, \beta) : \beta \equiv \alpha^\lambda \,(\mathrm{mod}\, m)\right\}$. The values m, α, β are the public key, and λ is the private key. For $K = (m, \alpha, \lambda, \beta)$, and for a (secret) random number $k \in \mathbb{Z}_{\varphi(m)}$, define $e_K(x, k) = (y_1, y_2)$, where

$$\begin{aligned} y_1 &= \alpha^k \,(\mathrm{mod}\, m) \\ y_2 &= x\beta^k \,(\mathrm{mod}\, m) \end{aligned}.$$

For $(y_1, y_2) \in C$, define $d_K(y_1, y_2) = y_2 (y_1{}^\lambda)^{-1} \,\mathrm{mod}\, m$.

Now, in this section, we illustrates some examples Composite ElGamal Cryptpsystem which we constitute above.

Example 2.1. Let m be 625 according to Theorem 2.1. $\mathbb{Z}^*_{625} = \left\{x \in \mathbb{Z}_{625} : (x, 625) = 1\right\}$. So, the primitive element $\alpha = 2$.

Let $a = 90$, so $\beta = 2^{90} \,(\mathrm{mod}\, 625) = 474$

Now, suppose that Alice wishes to send the message $x = 598$ to Bob. Say $k = 245$ is the random integer she chooses. Then she computes

$$\begin{aligned} y_1 &= \alpha^k \,(\mathrm{mod}\, m) = 2^{245} \,(\mathrm{mod}\, 625) = 332, \\ y_2 &= x\beta^k \,(\mathrm{mod}\, m) = 598.474^{245} \,(\mathrm{mod}\, 625) = 598.124 = 402 \end{aligned}$$

Alice sends $y = (y_1, y_2) = (332, 402)$ to Bob.

When Bob receives the ciphertext $y = (332, 402)$, he computes

$$\begin{aligned} x = y_2 (y_1{}^a)^{-1} \,\mathrm{mod}\, m &= 402.(332^{90})^{-1} \,\mathrm{mod}\, 625 \\ &= 402.\,(124)^{-1} \quad \mathrm{mod}\, 625 \\ &= 402.499 \quad \mathrm{mod}\, 625 \\ &= 598 \end{aligned}$$

which was the plaintext that Alice sent.

Example 2.2. Let m be 4418 according to Theorem 2.1. $\mathbb{Z}^*_{4418} = \left\{x \in \mathbb{Z}_{4418} : (x, 4418) = 1\right\}$. So, the primitive element $\alpha = 3$.

Let $a = 786$, so $\beta = 3^{786} \,(\mathrm{mod}\, 4418) = 2901$

Now, suppose that Alice wishes to send the message $x = 3974$ to Bob. Say $k = 1223$ is the random integer she chooses. Then she computes

$$\begin{aligned} y_1 &= \alpha^k \,(\mathrm{mod}\, m) = 3^{1223} \,(\mathrm{mod}\, 4418) = 4217, \\ y_2 &= x\beta^k \,(\mathrm{mod}\, m) = 3974.2901^{1223} (\mathrm{mod}\, 4418) \\ &= 3974.361 = 3182 \end{aligned}$$

Alice sends $y = (y_1, y_2) = (4217, 3182)$ to Bob.

When Bob receives the ciphertext $y = (4217, 3182)$, he computes

$$
\begin{aligned}
x=y_2(y_1^{a})^{-1} \bmod m &= 3182.(4217^{786})^{-1} \bmod 4418\\
&= 3182.\,(361)^{-1} \quad \bmod 4418\\
&= 3182.4161 \qquad \bmod 4418\\
&= 3974
\end{aligned}
$$

which was the plaintext that Alice sent.

III. CONCLUSİON

In this study, we have defined a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules. To do this we will use a theorem and by means of the theorem we have obtained a cyclic and multiplicative group whose order is $\varphi(m)$. So, we have obtained that we are able to reconstitute Discrete Logarithm problem by using the theorem 2.1. Then, we have constructed a new cryptosystem based on the new problem similar to ElGamal Crptosystem, and we called the new cryptographic system as Composite ElGamal Cryptpsystem.

In addition one of two limits in the ElGamal cryptosystem is that the plaintext must be less than $p-1$ [7]. We have compared that ElGamal Cryptpsystem and Composite ElGamal Cryptpsystem in terms of this limit and we have obtained that while $\alpha\in\mathbb{Z}_p^*$, the plaintext must be less than $p-1$ ($P=\mathbb{Z}_p^*$) in the ElGamal cryptosystem, $\alpha\in\mathbb{Z}_m^*$, the plaintext must be less than $m-1$ ($P=\mathbb{Z}_m\backslash\{0\}$) in Composite ElGamal Cryptpsystem. Moreover, we know that if in ElGamal Cryptpsystem p is a large prime number, in Composite ElGamal Cryptpsystem, m is more large number($m=p^k$ or $m=2p^k$, for p is large prime number). That is, if we choose m a composite number by using the theorem, we obtained that this limit decrease as m increases.

So, by means of the new cryptosystem, we have made that the cryptosystem which is used only in prime modulus is also usable for composite modulus and also the new cryptosystem which we defined is more advantages than ElGamal Cryptpsystem in terms of crptography. Because, while number of data which must try to understand the message for one who doesn't know the private key is $\varphi(m)=p^k-p^{k-1}$ (for p is large prime number) in Composite ElGamal Cryptosystem, $\varphi(p)=p-1$ in ElGamal Cryptosystem. That is, in comparison with ElGamal Cryptpsystem, for one who doesn't know the private key the number of data which must try to understand the message increase in Composite ElGamal Cryptpsystem.

REFERENCES

[1] D. R. Stinson, *Cryptography Theory and Practice*. New York: Chapman & Hall / CRC, 2002.

[2] National Bureau of Standard, Data Encryption Standard, Federal İnformation Processing Standards, NBS, 1977.

[3] R.L. Rivest, A. Shamir and L. Adleman, ‘‘Method for Obtaining Digital Signatures and Public Key Cryptography’’, *Comm. ACM*, vol.21, no.2,pp. 120-126, 1978.

[4] T. ElGamal,. ‘‘A Public-Key Cryptosystem and a Signature Scheme Based on Discreate Logarithms’’. *IEEE Trans. Information Theory*, vol.31,no.4,pp. 469-472, 1985.

[5] H. Zhu. ‘‘Survey of Computational Assumptions Used in Cryptography Broken or Not by Shor’s Algoritm,’’ Master Thesis, McGill University School of Computer Science, Montreal, 2001.

[6] G. Yeşilot, and M. Özavşar, *Soyut Cebir Çözümlü Problemleri*, Ankara: Nobel Akademy , 2013.

[7] M.S. Hwang, C.C. Chang, K.F. Hwang, ‘‘An ElGamal-Like Cryptosystem for Enciphering Large Messages’’, *Transactions on Knowledge and Data Engineering*, vol.14, no.2,pp. 445-446, 2002.