International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

ISS-PKC: A Information Security Solution based on Public Key Cryptosystem

Duy-Hung Tran
Faculty of Information Technology
Hanoi Open University
Building B101, Nguyen Hien Street, Bach Mai Ward, Hanoi

Thanh-Tung Thai
Faculty of Basic Training
Hanoi Open University
Building B101, Nguyen Hien Street, Bach Mai Ward, Hanoi

Chi-Bang Duong
Faculty of Information Technology
Hanoi Open University
Building B101, Nguyen Hien Street, Bach Mai Ward, Hanoi

Minh-Tuan Luu*
Faculty of Information Technology, College of Technology
National Econmics University
207, Giai Phong Street, Bach Mai Ward, Hanoi

***Abstract* - The rapid development of information technology has brought useful values to the society - economy, as well as creating the complex issues about information security, especially the risk of the information loss. Recently, the types of illegal intrusion of the information technology systems at universities, colleges, research institutes, companies (are called organizations) steal the data to be increasingly and affected level is more serious. The information security is essential, plays an important role deciding on the organizations development. We found that information security at organizations is very urgent and necessary. One of the most effective information security solutions is the use of the cryptosystems to secure information and data. In this paper, we study to develop the information security solution based on the ElGamal public key cryptosystem to information security at organizations and apply for Hanoi Open University (HOU).**

Keywords—public key cryptosystem; ElGamal cryptosystem; information security; cyber security

I. INTRODUCTION

Information technology in general and information in particular had effected directly on the activities of the society – economy of the countries in the world. Information plays a very important role that securing information security and transparency, meaning that information is not changed, is not exposed by the others when transmitting from the the sender to the receiver. With the strong development of the internet, information is transmitted, the problem is how to secure information security, transmit to the right address. The information encryption is one of the methods that can solve given problem safely. If the information is encrypted, the hackers are very difficult to detect. Currently, Information security has been applied at many agencies and enterprises as: tax declaration, customs, securities, internet banking,...In the present context, the encryption has a very important role because it is a tool to secure information security. Users are quick to work, save money while securing information security. However, at present the application of encryption to secure information security in the fields is new and there are a few organizations which applying encryption in their activities.

The HOU's presidential board[1] has put forth the priorrity strategy of information technology application and information security in the management, training and scientific research activities to improve the training quality and competitiveness in the context of international integration. By the surveys, interviews which were interviewed directly with the officials and the lecturers of the departments at HOU, we found that:

- Most of users have not secured the data that was stored on the personal computers, information security is not important to them.
- Some users have secured the data following the way that "setting up password" for the personal computer in order to the others could not start up the computer, or "setting up password" for the data file in order to the others could not open the data file, they considered that it is absolute information security. Actually, there are many "password detecting" softwares which are free available on the internet so this method doesn't secure for the personal computer and the data files.
- In addition, the information communicates on the internet environment (such as email which has attached file, contract document, test document, exam document,... serving for training and management activities) between the staffs, the lecturers, the departments with the others are very much, always having risks but the information has not been encrypted before sending to the receiver.

II. BACKGROUND

According to [1,5], some mathematical background are presented below.

A. Mathematical background

Modulo expression's value: Let a natural number **n** and a random integer **a**. The value of modulo expression **a mod n** is the positive remainder value when dividing **a** by **n**.

Modulo equivalence: Let integers **a**, **b** and a positive integer **n**. If **a** and **b** have the same remainder value when dividing by n, we said that ***'a** is equivalent to **b** in modulo **n'***

Greatest Common Divisor: Firstly, recall that nonzero **b** is defined to be a divisor of **a** if **a = m.b** for some **m**, where **a**, **b**, and **m** are integers. We will use the notation **gcd(a,b)** to mean

This work is supported by Hanoi Open University (HOU) under grant number MHN2025-02.23

[1] https://hou.edu.vn/

* Corresponding author

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

the greatest common divisor of **a** and **b**. The positive integer **c** is said to be the greatest common divisor of **a** and **b** if:

- **c** is a divisor of **a** and of **b**;
- any divisor of **a** and **b** is a divisor of **c**.

Relatively prime: Two positive integers **a** and **b** have the only common divisor to be **1**, are called relatively prime.

Multiplicative inverse: Let a interger **a** $\in Z_n$, the multiplicative inverse of the **a mod n** *(denoted as* a^{-1}*)* is an integer **x** $\in Z_n$ such that **ax ≡ 1 mod n**. If x exists, **x** is unique.

Modulo equation: The modulo equation **ax ≡ b mod n** (with **b** $\in Z_n$) has the only one solution **x** $\in Z_n$ such that **gcd(a,n)** = 1.

Set Z_n *and* Z_n^**:*

- The set Z_n is the set of all equivalence classes on Z_n in modulo **n**, meaning that the set $Z_n = \{0, 1,..., n-1\}$. The addition, subtraction, and multiplication operations on the set Z_n are calculated similar to those for real numbers, but the results are reduced in modulo **n**.
- The set Z_n^* is set of integers **p** ($p \in Z_n$) that each element is relatively prime with **n**, meaning that $Z_n^* = \{p \in Z_n \mid gcd(n,p) = 1\}$. Every element of the set Z_n^* is called a primary element and Z_n^* is a cyclic group.

B. Related algorithms

1) The Euclidean and extended Euclidean algorithms

a) The Euclidean algorithm (Algorithm 1)

The Euclidean algorithm is used to determine the greatest common divisor (**gcd**) of two positive integers **a** and **b** as follows:

Algorithm 1. Euclidean algorithm

Input : Let two positive integers a, b (assuming that a >b> 0);

Output: Finding gcd(a, b);

1: While b ≠ 0 do

2: {

r ← a mod b;

a ← b;

b ← r;

}

3: return(a);

b) Extended Euclidean algorithm (Algorithm 2)

The Euclidean algorithm can be extended in order to find **d = gcd(a, b)** and the integers **x**, **y** satisfy a*x + b*y = d as follows:

Algorithm 2. Extended Euclidean algorithm

Input: Let 2 positive integers a, b (assuming that a > b > 0);

Output: Finding d = gcd(a, b) and the integers x, y satisfy a*x + b*y = d;

1: If b = 0 then

{

d ← a;

x ← 1;

y ← 0;

returrn(d, x, y);

}

2: Setting: {$x_2 \leftarrow 1$; $x_1 \leftarrow 0$; $y_2 \leftarrow 0$; $y_1 \leftarrow 1$;}

3: While b > 0 do

3.1: {

q ← a mod b;

r ← a - qb;

x ← $x_2 - q*x_1$;

x ← $y_2 - q*y_1$;

}

3.2: {

a ← b;

b ← r;

$x_2 \leftarrow x_1$;

$x_1 \leftarrow x$;

$y_2 \leftarrow y_1$;

$y_1 \leftarrow y$;

}

4: Setting: {q ← a; x ← x_2; y ← y_2;}

5: return(d, x, y).

2) The algorithm finding the multiplicative inverse (Algorithm 3)

Algorithm 3. Algorithm for finding the multiplicative inverse

Input: a $\in Z_n$.

Output: a^{-1} mod n (if existing).

1: Using the *extended Euclidean algorithm* in order to find the integers x, y satisfy ax + by = d, with d = gcd(a,n);

2: If d > 1 then message('a^{-1} *mod n does not exist!*');

3: else return(x).

3) The 'Square and Multiply' algorithm calculating the modulo expression's value (Algorithm 4)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

Algorithm 4. Algorithm "Square and Multiply" for calculating the modulo expression's value

Input: The modulo expression $\mathbf{A^k \bmod n}$.

Output: The value $\mathbf{f = A^k \bmod n}$.

1: Representing k in binary format: $b_l b_{l-1} \ldots b_1 b_0$, $b_i \in \{0, 1\}$, $0 \le i \le l$.

2: Initializing: {c ← 0; f ← 1};

3: for $i = l$ downto 0 do

{

(3.1) c ← 2*c;

(3.2) f ← (f*f) mod n;

(3.3) if $b_i = 1$ then

{

(3.3.1) c ← c + 1;

(3.3.2) f ← (f*a) mod n;

}

}

4: return(f).

C. The computational complexity

Following [1], the computational complexity is the number of memory cells or the number of operations performed during the computational process.

The computational complexity of an algorithm is considered as a function **f** such that f(n) is the maximum number of memory cells or the number of operations which the algorithm performs on the data, every n.

The computational complexity of a problem (or a function) is defined as the complexity of the best algorithm to solve the problem (or computing function).

III. THE ELGAMAL PUBLIC KEY CRYPTOSYSTEM

Following [2,3,4,5], the fundamental background of the ElGamal public key cryptosystem are presented as follows.

A. The public key cryptosystem

The public key cryptosystems use two different keys: private key and public key. These two keys are asymmetric so these cryptosystems are called asymmetric cryptosystems. The public key cryptosystems support solving some information security problems rather than substituting the secret key cryptosystems. The public key (everyone knows) is used to encrypt plain text or verify digital signature. Private key (the only receiver knows) is used to decrypt cipher text or signing a digital signature. The public key cryptosystems apply the results of number theory.

The general diagram of a public key cryptosystem is shown in Fig. 1.

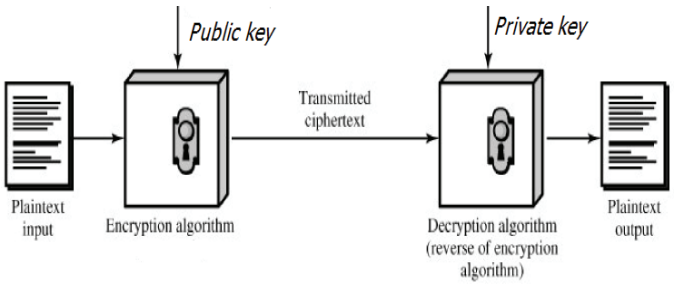

Fig. 1. The general diagram of the public key cryptosystem

B. The ElGamal public key cryptosystem

1) Discrete logarithm problem and the ElGamal public key cryptosystem

The characteristic of the discrete logarithm problem in set Z_p: $\mathbf{I = (p, \alpha, \beta)}$ where **p** is prime, $\alpha \in Z_p$ is the primary element, $\beta \in Z_p^*$. Finding the only integer **a** such that $0 \le a \le p-2$ which satisfies: $\alpha^a \equiv \beta \bmod p$.

The discrete logarithm problem is considered to be a nondeterministic problem (if p is chosen carefully) meaning that there is no polynomial time algorithm for solving the problem. To prevent from the detection method, choosing **p** has at least 150 digits and **(p-1)** has at least one large prime factor. The discrete logarithm problem is difficult to find discrete logarithms but the inverse problem (the exponentiation problem) has been computed by the *"squared and multiply"* algorithm, meaning that modulo exponentiation **p** is a one - way function with appropriate **p** prime.

The ElGamal public key cryptosystem is based on a discrete logarithm problem. This is a nondeterministic cryptosystem because the cipher text depends on the plain text and random integer **k** that was chosen by the sender so there will be many cipher texts from the same plain text [4,5].

2) The ElGamal cryptosystem

a) Key formation process

Assume that the sender and the receiver who would like to exchange confidential information by the ElGamal public key cryptosystem. First of all, the sender performs the key formation process as follows:

- Choosing a large enough prime number so that the discrete logarithm problem in Z_p is hard to solve.
- Choosing two random integers less than **p**: **α** (α is the primary element of Z_p^*) and **a** (**a** belongs to the receiver, is secret).
- Calculating the value of **β** expression according to the formula: $\beta = \alpha^a \bmod p$.
- Results: Secret key is **a**, public key is set **(α, p, β)**

b) Encryption process

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

To encrypt the plain text M (as an integer in Z_p) to cipher text C, the sender performs the steps following:

- Choosing a random number **k** less than **p** and computing the encryption key: $\mathbf{K=\beta^k \bmod p}$.
- Calculating: $\mathbf{C_1 = \alpha^k \bmod p}$.
- Using public key to calculate: $\mathbf{C_2 = (K*M) \bmod p}$.
- The sender sends cipher text C = (C_1, C_2) to the receiver, **k** is canceled immediately.

c) Decryption process

To decrypt the cipher text C to plain text M:

- Firstly, recalculating the K that used to encrypt the plain text according to the fomula: $\mathbf{K = (C_1^{(p-1-a)}) \bmod p = (\alpha^{k(p-1-a)}) \bmod p}$.
- Then, computing plain text M by solving the module equation: $\mathbf{M = (C_2. K) \bmod p}$.

IV. EXPERIMENTS

A. Developing the experimental application

In this section, we have developed function modules of the ElGamal public key cryptosystem using JAVA programming language. Then, we execute the system using the parameter's values of the cryptosystem, the experimental data and experimental results are shown in Fig2. below.

1) Calculating result of the module expression β (Beta)

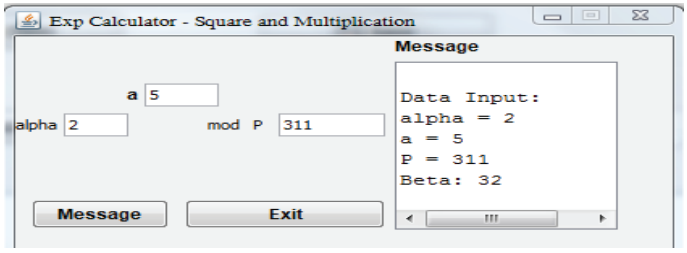

Fig. 2. Calculating result of the module expression β (Beta)

Choosing the values of the parameters to calculate the module expression β (Beta): α=2, a = 5 (a is secret), p = 311, calculating and getting β = 32.

The secret key a equals to 5, the public key (α, p, β) is a triple values (2, 311, 32).

2) Encryption and decryption results

a) Encryption result

- The parameter's values to encrypt: Choosing K = 7, α = 2, p = 311 and β = 32 (β calculated above). Attention: The secret key (a = 5) must be kept secretly.
- Original data (plain text): The exam document file (the content is displayed on the left hand of the function interface, we can understand).
- Encryption result: The encrypted exam document file (the content is displayed on the right hand of the functional interface, we can not understand).

b) Decryption result

- The parameter's values to decrypt: Secret key a = 5, α = 2, p = 311, β = 32 (β is recalculated automatically).
- Encrypted data (cipher text): The encrypted exam document file (the content is displayed on the right hand of the functional interface, we can not understand).
- Decryption result: The original exam document file (plain text) (the content is displayed on the left hand of the functional interface, we can understand).

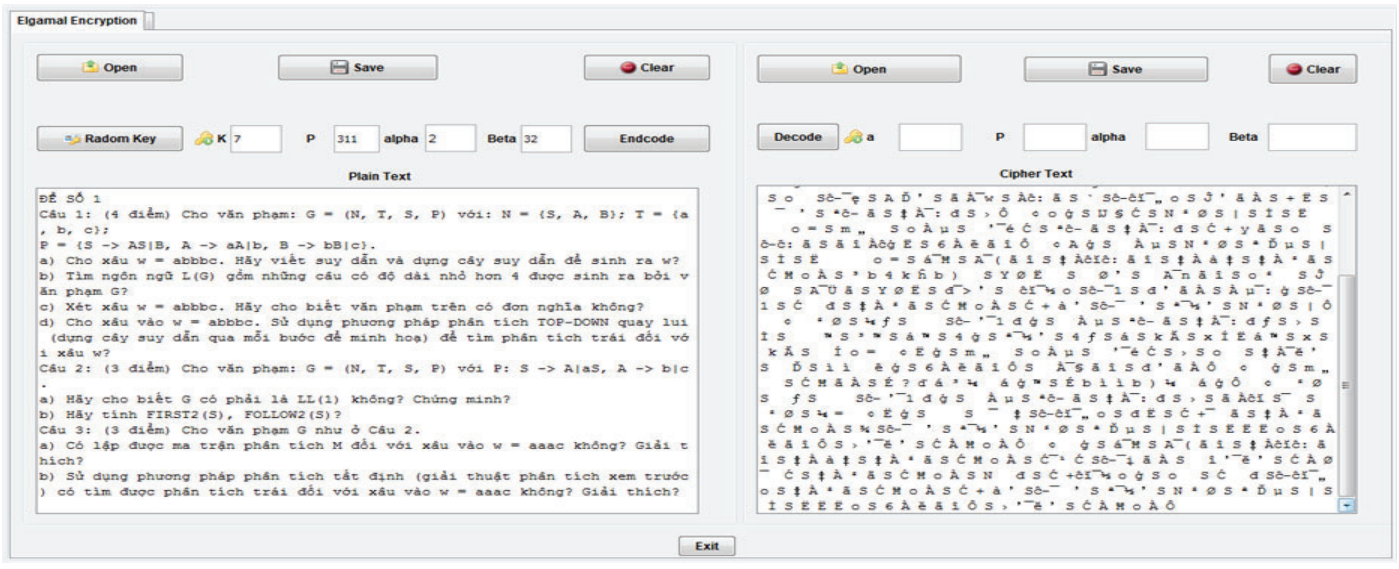

Fig. 3. Result of the encrypted exam document file

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

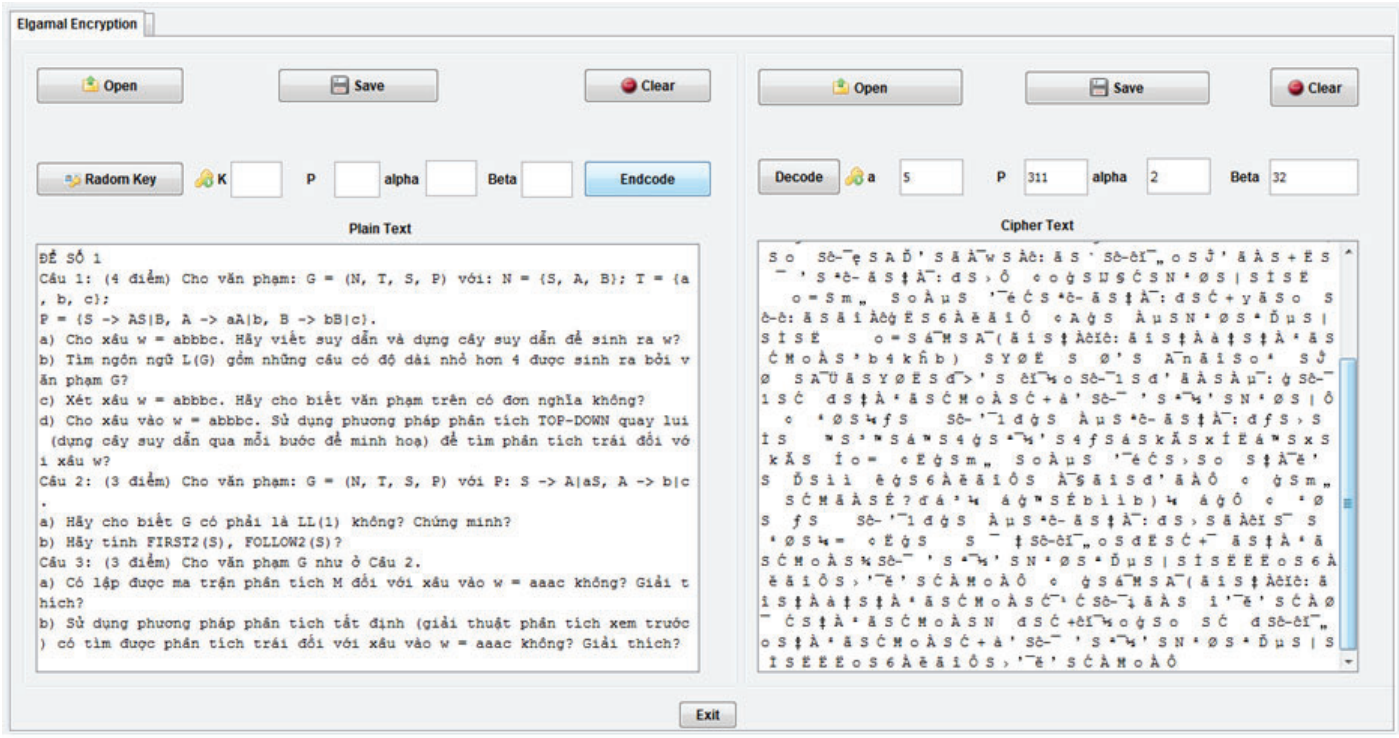

Fig. 4. Result of the original exam document file

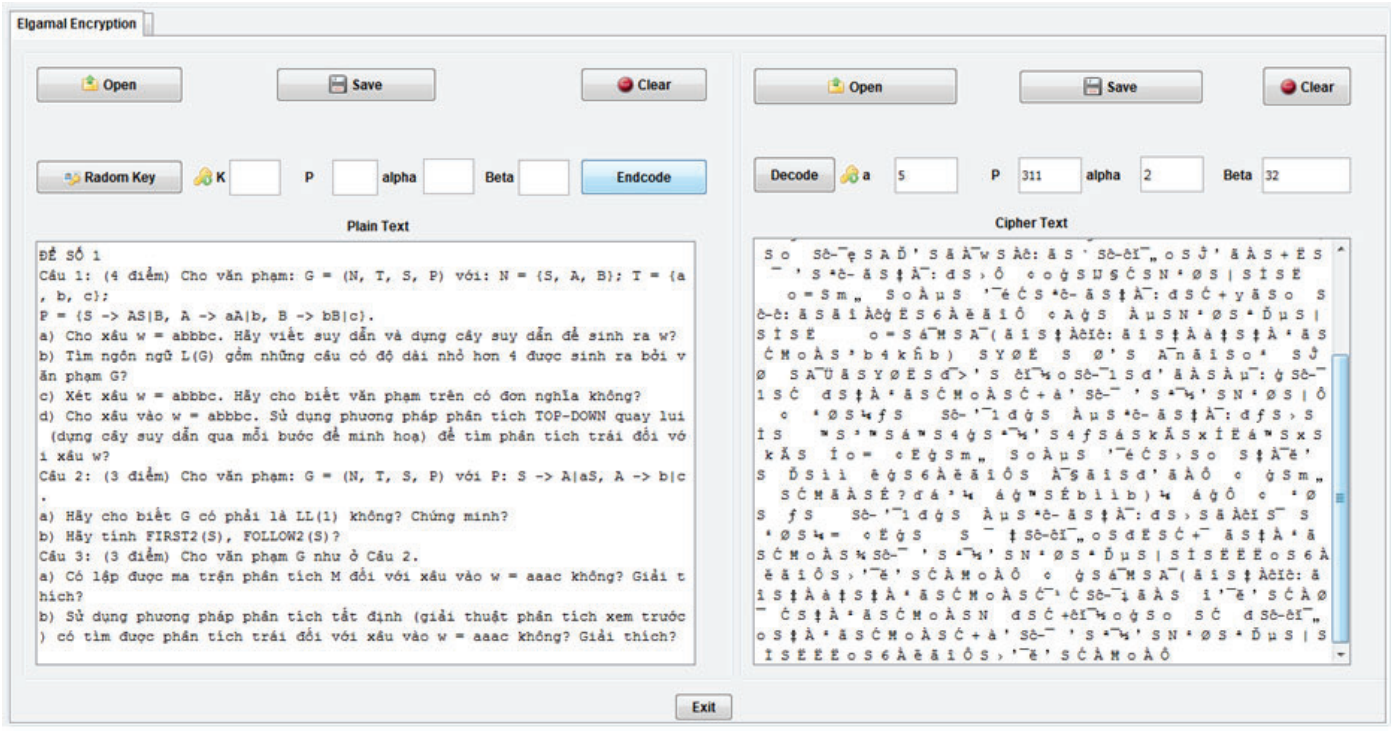

Fig. 5. Result of the original exam document file

B. Evaluating the experimental results

1) The advantages of the ElGamal cryptosystem

According to [2,5], the discrete logarithm problem can be solved by the brute force method with computational complexity **O(p)** (where **p** is the prime). Obviously, with large **p**, this time is very large so we can not solve the problem using this method.

As we know, the ElGamal cryptosystem is based on a discrete logarithm problem, so it is highly secure because the discrete logarithm problem has no effective information security solution yet.

With a large enough prime number **p**, the ElGamal cryptosystem hasn't been detected.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

The cipher text depends on the plain text and the chosen random integer value so we can encrypt the cipher text to many different cipher texts.

Besides, the copyright issue of the ElGamal cryptosystem is more flexible than the other public key cryptosystems (such as Rabin cryptosystem, RSA cryptosystem, Knapsack cryptosystem,…).

2) The disadvantages of the ElGamal cryptosystem

The encrypting and decrypting speed is slow because it must calculate with large prime numbers.

Key storage requires large memory.

V. CONCLUSION

The application of data security solutions is very essential in the digital age. The public key cryptosystems are are effective solutions for information security as well as data storage. In this paper, we have developed the information security solution based on the ElGamal public key cryptosystem to meet data security requirements. Our information security solution is applied at Hanoi Open University and achieved good results. However, our information security solution currently only secures document information data. In the future, we will research and expand our information security solution to provide security solution for other format data such as images and videos. Additionally, we will also research to implement the ElGamal public key cryptosystem in the form of *"hardening"* to increase processing speed and enhance further security.

REFERENCES

[1] Phan Dinh Dieu, “Cryptography theory and information security”, Hanoi National University Publishing House, 2002. [Phan Đình Diệu, Lý thuyết mật mã và an toàn bảo mật thông tin, Nhà xuất bản Đại học Quốc gia Hà nội, 2002].

[2] R. S. Douglas, “Cryptography Theory and practice”, *CRC Press*, 1995.

[3] G. Nik, I. Boris, M. Alex, and M. Nik, “Modern Cryptography-Protect Your Data with Fast Block Ciphers”, *A-LIST Publishing*, 2003.

[4] A. Menezes, P. VanOorschot, and S. Vanstone, “Handbook of Applied Cryptography”, *CRC Press*, 1996.

[5] S. William, “Cryptography and Network Security Principles and Practices”, *Prentice Hall*, 2006.