

# **AN EXTENSION OF ELGAMAL DIGITAL SIGNATURE ALGORITHM**

*A Thesis submitted in partial fulfillment  
of the requirements for the degree of*

**BACHELOR OF TECHNOLOGY  
IN  
COMPUTER SCIENCE AND ENGINEERING  
BY**

**BINAY PRAKASH DUNG DUNG (108CS025)**

**PRANAV KUMAR (108CS072)**

Under the Guidance of

**Prof. SUJATA MOHANTY**



**Department of Computer Science & Engineering**

**National Institute of Technology, Rourkela**

**Rourkela-769 008, Odisha, India**



## **CERTIFICATE**

This is to certify that the thesis entitled, “**AN EXTENSION OF EIGAMAL DIGITAL SIGNATURE ALGORITHM**” submitted by **Binay Prakash Dungdung (108CS025) & Pranav Kumar (108CS072)** in partial fulfillment of the requirements for the award of **Bachelor of Technology degree in Computer Science & Engineering** at National Institute of Technology Rourkela is an authentic work carried out by them under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any University/Institute for the award of any Degree or Diploma.

Prof. Sujata Mohanty

Department of Computer Science & Engineering

National Institute of Technology

Rourkela-769008



## ACKNOWLEDGEMENT

We avail this opportunity to extend our hearty indebtedness to our guide **Prof. Sujata Mohanty**, Computer Science Engineering Department, for her valuable guidance, constant encouragement and kind help at different stages for the execution of this dissertation work.

Binay Prakash Ddungdung (108CS025)

Pranav Kumar (108CS072)

Computer Science & Engineering, 2012

Computer Science & Engineering, 2012

NIT Rourkela

## ABSTRACT

As for the problem that ElGamal digital signature scheme's security is constantly being challenged and is becoming more and more serious, an improved ElGamal digital signature algorithm was 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 proposed scheme improved this demerit by adding a random number to the original one and increasing difficulty of deciphering key. The security of the improved signature scheme is the same with the ElGamal signature scheme which is based on the difficult computable nature of discrete logarithm over finite fields. Its time complexity is better than the original one but the issue is about the time complexity which is still high. So in order to improve the time complexity another improved ElGamal digital signature algorithm is proposed. The scheme presented in this paper after analysis showed that the security level is kept high by using two random numbers and the time complexity is reduced.

# Contents

<b>1. Introduction</b> .....	2
1.1 Digital Signature.....	2
1.1.1 Why Digital Signature Is Required?.....	2
1.1.2 Services Of Digital Signature.....	2
1.1.3 Digital Signature Schemes.....	2
<b>2. Objective</b> .....	5
<b>3. Cryptography</b> .....	7
3.1 Cryptographic Techniques.....	7
3.1.1 Symmetric Key Cryptography.....	7
3.1.2 Asymmetric Key Cryptography.....	7
3.1.3 Hashing.....	7
3.2 Cryptanalysis.....	8
3.3 Security Services.....	8
3.3.1 Authentication.....	8
3.3.2 Non-repudiation.....	9
3.3.3 Access Control.....	9
3.3.4 Data Confidentiality.....	9
3.3.5 Data Integrity.....	9
3.4 Security Mechanisms.....	9
<b>4. ElGamal Digital Signature Scheme</b> .....	12
4.1 Description.....	12
4.2 Attacks.....	13
<b>5. ElGamal Digital Signature Algorithm Of Adding A Random Number</b>	15
5.1 Description.....	15
5.1.1 Setup.....	15

5.1.2	Signature Generation.....	15
5.1.3	Signature Verification.....	16
5.2	Other Algorithms Used In This Scheme.....	17
5.3	Demerits Of This Algorithm.....	18
<b>6.</b>	<b>Proposed Scheme</b> .....	<b>20</b>
6.1	Description.....	20
6.1.1	Setup.....	20
6.1.2	Signature Generation.....	20
6.1.3	Signature Verification.....	21
6.2	Correctness.....	21
<b>7.</b>	<b>Results and Analysis</b> .....	<b>23</b>
7.1	Implementation Screenshot.....	23
<b>8.</b>	<b>Conclusion</b> .....	<b>26</b>
	<b>References</b> .....	<b>27</b>

## List of Figures

1. Algorithm Flow Chart.....	16
2. Output of Existing Scheme.....	23
3. Output of Proposed Scheme.....	24

# **CHAPTER – 1**

# **INTRODUCTION**



# 1. INTRODUCTION

---

## 1.1 Digital Signature

We all are familiar with the concept of signature. A person signs a document to show that it originated from her or was approved by her. In other words, signature is a method to authenticate any document. It is a proof to the recipient that the document comes from the correct entity (sender). In the present world most of the documents are electronic due to the cult usage of the computer and its applications like email, e-banking, e-voting, etc. Thus the message, data, documents or any other materials in electronic format has to be signed electronically. This signature that is done electronically is known as Digital Signature.

### 1.1.1 Why Digital Signature Is Required?

When B sends a message to P, P needs to check the authenticity of the sender. He needs to be sure that the message comes from B and not S. It may happen that P modifies the message and claims that the message came from B, or B denies that the message was sent by him. To avoid all these things P needs to sign the message electronically. Hence, digital signature is required.

### 1.1.2 Services of Digital Signature

A digital signature provides:

- Message Authentication
- Message Integrity
- Non-repudiation

Non-repudiation can be provided using a trusted party. A digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

### 1.1.3 Digital Signature Schemes

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the

message was created by a known sender, and that it was not altered in transit. Digital signatures are used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. The various digital signature schemes are RSA digital signature scheme, ElGamal digital signature scheme, Schnorr digital signature scheme, Digital Signature Standard (DSS) scheme and elliptic curve digital signature scheme.

# **CHAPTER – 2**

## **OBJECTIVE**

## 2. OBJECTIVE

---

The objective of the proposed project is to design an ElGamal digital signature algorithm such that the time complexity of the algorithm is reduced and the security is kept high. Earlier improvement was made by adding a random number to the original algorithm because of which security was increased. But time complexity was still high.

# **CHAPTER – 3**

# **CRYPTOGRAPHY**

## 3. CRYPTOGRAPHY

---

Cryptography (covered text) is a technique of converting ordinary or plain text to cipher text. This is also called as encryption. In decryption the cipher text is converted back to the plain text. In earlier days cryptography referred to message encryption and decryption by using a common secret key. But in modern times the following mechanisms are proposed. They are

- Symmetric Key cryptography
- Asymmetric Key cryptography
- Hashing

### 3.1 Cryptographic Techniques

#### 3.1.1 Symmetric Key Cryptography

In this technique, the sender uses an encryption algorithm and a secret key known to both sender and receiver to encrypt the message. Then the receiver after receiving the message uses the decryption algorithm and the shared secret key to decrypt the message.

#### 3.1.2 Asymmetric Key Cryptography

This technique also known as public-key-cryptography involves the use of 2 keys - public key and private key. By using the public key the sender first encrypts the message and the receiver uses its private key to decrypt the message.

#### 3.1.3 Hashing

A fixed length message digest is created out of the variable length message in hashing. The digest is of very small size than that of the message(if the message is very large). Usually both the message and the digest are sent to the receiver. Hashing helps in providing check values for the message integrity. The hardware requirement for hashing is more than any operation. Compression function may be used by a set of cryptographic hash functions. These hash

functions include RSA, MD etc the most popular being MD5/SHA-1 algorithm for message compression which converts a message to a 128 bit/512 bit hexadecimal form.

## 3.2 Cryptanalysis

Cryptanalysis is the study of methods to obtain the meaning of encrypted information (cipher text), without requiring the access to the private parameters. Usually, this involves a pattern study of the working methodology of the system and hence deriving the secret key. "Cryptanalysis" is also used to refer to any attempt to overcome the security of any cryptographic algorithm and protocol in general, and not only encryption. However, cryptanalysis does not involve methods of attack that do not primarily target weaknesses in the actual cryptography. But these types of attack pose an important concern and often are more effective than traditional cryptanalysis.

## 3.3 Security Services

Some security services and some mechanism to implement those services are provided by the International Telecommunication union-Telecommunication standardization Sector. The security services include:

- Authentication
- Non repudiation
- Access Control
- Data Confidentiality
- Data Integrity

### 3.3.1 Authentication

This service gives a proof of authentication of the sender to the receiver or vice-versa. In peer entity authentication, during the connection establishment phase of connection oriented communication it provides the authentication of the sender or receiver. In data origin authentication i.e. in connectionless communication it authenticates the source of data.

### 3.3.2 Non-repudiation

To avoid repudiation (denial) by either the sender or the receiver of the data non-repudiation service is advisable. The receiver of the data can later prove the identity of the sender along with help of the proof of origin in case of denial of service. In non-repudiation, the sender can confirm the delivery to the receiver with the real proof of delivery. This security service is extensively used in the verification phase of digital signatures.

### 3.3.3 Access Control

Access control enables an authority to gain control and access to areas and resources in an information system. An access control system provides security against unauthorized access and usage of data. The term access in this context can mean reading, writing, modification or execution of programs.

### 3.3.4 Data Confidentiality

International Organization for Standardization (ISO) in ISO-17799 defined confidentiality as "ensuring that information is accessible only to those authorized to have access" .In many cryptosystems confidentiality is one of the major design goals to protect data from disclosure attack. As defined by X.800 the service is very broad and includes confidentiality of the total message or part of a message and also ensures protection against traffic analysis. In other words it prevents traffic analysis and snooping.

### 3.3.5 Data Integrity

Data integrity is required to protect data from unauthorized insertion, deletion, modification and replaying by an attacker. It can protect the total message or the part of message.

## 3.4 Security Mechanism

Security mechanisms include:

- Encipherment



- Data Integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization
- Access Control
- Digital Signature

**CHAPTER – 4**

**ELGAMAL DIGITAL  
SIGNATURE SCHEME**

## 4. ELGAMAL DIGITAL SIGNATURE SCHEME

---

### 4.1 Description

ElGamal signature scheme was first introduced in 1985. In this signature scheme the public key is used for encryption and signature verification. For each user, there is a secret key  $x$ , and public keys  $\alpha, \beta, p$  where:

$$\beta = \alpha^x \text{ mod } p$$

The public keys  $\alpha, \beta, p$  are published in a public file and is known to everybody while the secret key  $x$  is kept secret.

$$\alpha^x = \beta \text{ mod } p \text{ -----} \rightarrow \text{DLP equation}$$

$(\alpha, \beta, p)$  - public key

$x$  - private key

The above things are performed once by the signer.

$p$  is a large prime.

Choose a random number  $k$  such that  $0 < k < p-1$  and  $\text{gcd}(k, p-1) = 1$ .

$$\gamma = \alpha^k \text{ mod } p$$

Signature of  $m$  is a pair  $(\gamma, \delta)$  where  $0 \leq \gamma, \delta \leq p-1$ , chosen such that

$$\alpha^m = \beta^\gamma \gamma^\delta \text{ mod } p \text{ ----- (1)}$$

$$\alpha^m = (\alpha^x)^\gamma (\alpha^k)^\delta \text{ mod } p$$

$$= \alpha^{x\gamma} \alpha^{k\delta} \text{ mod } p$$

$$= \alpha^{x\gamma + k\delta} \text{ mod } p$$

$$m = (x\gamma + k\delta) \text{ mod } (p-1)$$

$$\delta = (m - x\gamma)k^{-1} \text{ mod } (p-1)$$

Given  $m$ ,  $\gamma$  and  $\delta$ , it is easy to verify the authenticity of the signature by computing both sides of (1) and checking that they are equal.

## 4.2 Attacks on ElGamal Digital Signature Scheme

Main ways of attacks are:

1. A direct hack on the private key
2. Arbitrary forged signature attack
3. Substitution attack according to known signatures
4. The assault is homomorphism
  - a. Using the same random number  $k$
  - b. To use the relevant random numbers  $k_1, k_2, k_3$ .

**CHAPTER – 5**

**ELGAMAL DIGITAL  
SIGNATURE OF ADDING A  
RANDOM NUMBER**

## 5. ELGAMAL DIGITAL SIGNATURE ALGORITHM OF ADDING A RANDOM NUMBER

---

### 5.1 Description

Original Elgamal algorithm has its own security disadvantages, that is, only one random number is used. So in order to improve its security, one more random number is used due to which the difficulty of deciphering key increases.

#### 5.1.1 Setup

For each user, there is a secret key  $x$  which is selected by the signer, and public keys  $\alpha, \beta, p$  where:

$$\beta = \alpha^x \text{ mod } p$$

The public keys  $\alpha, \beta, p$  are published in a public file and is known to everybody while the secret key  $x$  is kept secret.

$$\alpha^x = \beta \text{ mod } p \text{ -----} > \text{DLP equation}$$

$(\alpha, \beta, p)$  - public key

$x (1 < x < \phi(p))$  is the signer's private key.

The above things are performed once by the signer.

$p$  is a large prime.

#### 5.1.2 Signature Generation

Choose a random number  $k$  such that  $0 < k < p-1$  and  $\text{gcd}(k, p-1) = 1$ .

$$\gamma = \alpha^k \text{ mod } p$$

Choose a random number  $t$  such that  $0 < t < p-1$  and  $\text{gcd}(t, p-1) = 1$ .

$$\lambda = \alpha^t \text{ mod } p$$

$$m = (x\gamma + k\lambda + t\delta) \bmod (p-1)$$

Signature of  $m$  is  $(\gamma, \lambda, \delta)$ .

### 5.1.3 Signature Verification

$$\alpha^m = \beta^\gamma \gamma^\lambda \lambda^\delta \bmod p$$

Using this equation the receiver verifies the authenticity of the signature by computing both sides of the equation.

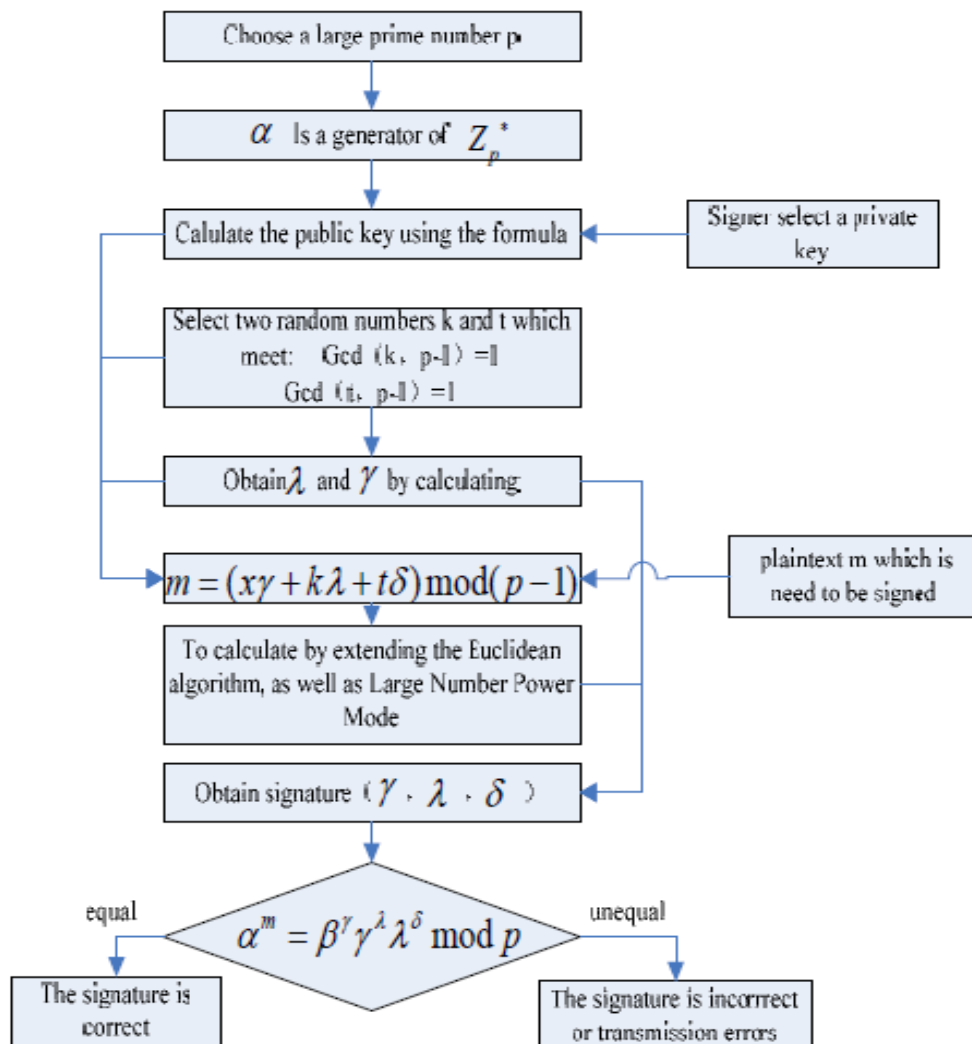


Fig. 1 Algorithm Flow Chart

## 5.2 Other Algorithms Used In This Scheme

In this algorithm, first of all a prime number is generated. Then to check whether it is prime or not, Miller-Rabin primality test is done. Calculation of  $\beta$ ,  $\gamma$ ,  $\lambda$  is done by using fast exponentiation method.

Miller-Rabin algorithm:

Miller-Rabin(n)

$n-1 = 2^k m$ , where  $m$  is odd (note that  $n-1$  is even)

choose a random number  $a$ ,  $1 \leq a \leq n-1$

$b = a^m \pmod n$

if  $b \equiv 1 \pmod n$

    then return (“n is prime”)

for  $i=0$  to  $k-1$

{

    If  $b \equiv -1 \pmod n$

    then return (“n is prime”)

    else  $b = b^2 \pmod n$

}

Return (“n is composite”)

Fast Exponentiation:

It is possible using the square-and-multiply method. Main idea behind this algorithm is to treat exponent as a binary number of  $n_b$  bits ( $x_0$  to  $x_{n_b-1}$ ). E.g.  $x=22=(10110)_2$

$y = a^x$

where  $x = x_{n_b-1} * 2^{n_b-1} + x_{n_b-2} * 2^{n_b-2} + \dots + x_1 * 2^1 + x_0 * 2^0$

E.g.  $y = a^9 = a^{1001} = a^8 * 1 * 1 * a$

Square\_and\_Multiply(a,x,n)

{

$y \leftarrow 1$



```
for(i←0 to nb-1)
{
    If(xi=1) y ← a * y mod n
    a← a2 mod n
}
Return y
}
```

### 5.3 Demerit of this algorithm

The complexity of this algorithm is high and there are some transmission errors due to which the signature obtained is incorrect. Because of the demerits, the verification equation and signature equation needs to be modified such that the time complexity will decrease and transmission errors will be reduced.

# **CHAPTER – 6**

## **PROPOSED SCHEME**

## 6. PROPOSED SCHEME

---

### 6.1 Description

#### 6.1.1 Setup

Here  $p$  and  $q$  are large primes, Compute  $n=pq$  such that

$$p=2p'+1 \text{ and}$$

$$q=2q'+1$$

where  $p', q', p$  and  $q$  are distinct primes.

Compute  $d$  such that  $ed \equiv 1 \pmod{\phi(n)}$  where  $e$  is co-prime to  $\phi(n)$ .

$g$  is a generator,  $g \in \mathbb{Z}_q^*$

Public parameter:  $n, g, h(m)$

#### 6.1.2 Signature Generation

Here the signer select a random number  $s_a \in \mathbb{Z}_n^*$  and computes.

$$y_a = g^{s_a} \pmod{n}$$

$$x = \text{ID} \cdot (y_a)^d$$

Where  $\text{ID}$  is the identity of the signer (public).

The signer choose a random number  $k \in \mathbb{Z}_n^*$  and computes,

$$r = g^k \pmod{n}$$

$$s = k + r \cdot x \cdot y_a^{-d} - s_a \pmod{n}$$

$$t = H(m, y_r^{s+s_a} \pmod{n})$$

$y_r$  is the public key of receiver.

The signature of the message  $m$  is

$$\sigma = (r, t)$$

### 6.1.3 Signature Verification

After receiving  $m$  and  $\sigma$  the verifier (R) checks the validity of the signature as

$$t = H[m, (r \cdot g^{r \cdot \text{ID}})^{x_r} \bmod n]$$

If the above satisfies, the signature is a valid one.

The receiver chooses  $x_r \in \mathbb{Z}_n^*$  in random and computes its public key,

$$y_r = g^{x_r} \bmod n$$

## 6.2 Correctness

$$s = k + r \cdot x \cdot y_a^{-d} - s_a \bmod n$$

$$s + s_a = k + r \cdot \text{ID} \bmod n; \quad (\text{since } x = \text{ID}, y^{d_a})$$

$$\text{So now, } y_r^{s+s_a} \pmod n = g^{x_r(s+s_a)} \pmod n$$

$$= g^{x_r(k+r \cdot \text{ID})} \pmod n$$

$$= g^{x_r k} \cdot g^{r \cdot \text{ID} \cdot x_r} \pmod n$$

$$= (g^k)^{x_r} \cdot g^{r \cdot \text{ID} \cdot x_r} \pmod n$$

$$= r^{x_r} \cdot g^{r \cdot \text{ID} \cdot x_r} \pmod n$$

$$= (r \cdot g^{r \cdot \text{ID}})^{x_r} \pmod n$$

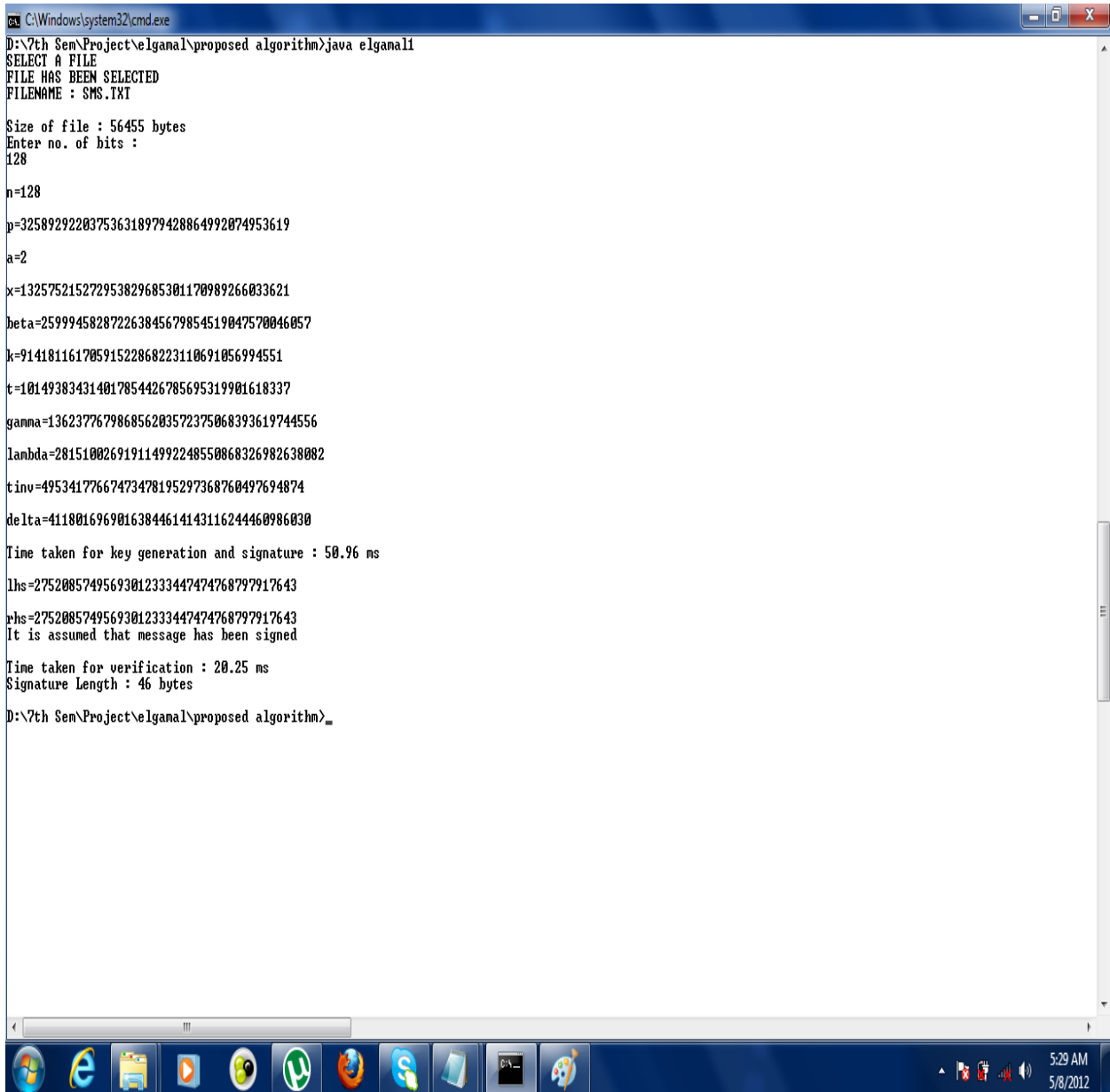
$$\text{Hence, } H[m, (y_r^{s+s_a}) \bmod n] = H[m, ((r \cdot g^{r \cdot \text{ID}})^{x_r}) \bmod n]$$

# **CHAPTER – 7**

## **RESULTS AND ANALYSIS**

## 7. RESULTS AND ANALYSIS

### 7.1 Implementation Screenshot



```
C:\Windows\system32\cmd.exe
D:\7th Sem\Project\elganal\proposed algorithm>java elgamall
SELECT A FILE
FILE HAS BEEN SELECTED
FILENAME : SMS.TXT

Size of file : 56455 bytes
Enter no. of bits :
128

n=128
p=325892922837536318979428864992874953619
a=2
x=132575215272953829685381170989266833621
beta=259994582872263845679854519047570046857
k=91418116170591522868223110691056994551
t=101493834314017854426785695319901618337
gamma=136237767986856203572375068393619744556
lambda=281510026919114992248550868326982638082
tinv=49534177667473478195297368760497694874
delta=41180169690163844614143116244460986030

Time taken for key generation and signature : 50.96 ms

lhs=27520857495693012333447474768797917643
rhs=27520857495693012333447474768797917643
It is assumed that message has been signed

Time taken for verification : 20.25 ms
Signature Length : 46 bytes

D:\7th Sem\Project\elganal\proposed algorithm>_
```

Fig.2 Output of existing algorithm

```
C:\Windows\system32\cmd.exe

D:\7th Sem\Project\elganal\proposed algorithm>java proposedalgo
SELECT A FILE

FILE HAS BEEN SELECTED

FILENAME : SMS.TXT

Size of file : 56455 bytes

n = 37b25e8ca94aa9456adaf8af2cde94456e0eea66

Enter no. of bits : 128

nb = 128

n = 241729937833713328690716461739832985373072971100039072271172581192232615620501
phi = 241729937833713328690716461739832985372088768404327558528726897716377326171212
e = 339443657483064332931943005768717790343
d = 54030051470129595008656025122954103409413546082489926414673495027613798533091
g = 2

xr = 319842632095121212269463821645747485657
yr = 27215720939723647407486680753658053302162785517612629848352257093425935973945

SA = 229760377021682438466931123719607060441
yA = 43723500981390456794109640466767595541726349697132576972922313736469206143210

ID = 100660985252279897913612961870229767257
x = 23720319003006019020984520168932470058995492035575609224780611257772780084291

k = 306515257912505162245487095226005802157
r = 99419198407799574518063502242850661492462426954384843329105173703613782407071

s = 2107626548676200208249632250069763571619195340787736824183212547197370131579186
m1 = 37b25e8ca94aa9456adaf8af2cde94456e0eea66178756967316623481129422413612532165913388491838021089400802432974159495156530
t = 7b315e2a8ab64d59b32bf73379401dcac483065e

Time taken for key generation and signature : 36.93 ms

m2 = 37b25e8ca94aa9456adaf8af2cde94456e0eea66178756967316623481129422413612532165913388491838021089400802432974159495156530
t1 = 7b315e2a8ab64d59b32bf73379401dcac483065e

Signature is correct

Time taken for verification : 12.66 ms

Signature Length : 52 bytes

D:\7th Sem\Project\elganal\proposed algorithm>java elganal1
SELECT A FILE
FILE HAS BEEN SELECTED
FILENAME : SMS.TXT

Size of file : 56455 bytes
FILENAME : SMS.TXT
```

Fig. 3 Output of Proposed algorithm

# **CHAPTER – 8**

# **CONCLUSION**



## 8. CONCLUSION

---

After analysis, we can conclude that the time complexity of the proposed algorithm is better than that of the existing algorithm.

## REFERENCES

---

1. William Stallings, "Cryptography and Network Security: Principles and Practice", Second Edition.
2. J.Orlin Grabbe, "Cryptography and Number Theory for Digital Cash".
3. T. ElGamal, "A public key cryptosystem and a signatures scheme based on discrete logarithms", IEEE Trans. Inform. Theory.
4. Cryptography and network security by Behrouz A. Forouzan, 2<sup>nd</sup> edition.
5. Xiaofei Li, Xuanjing Shen and Haipeng Chen, "ElGamal Digital Signature Algorithm of Adding a Random Number", Journal of Networks, Vol. 6, No. 5