An Encryption and Decryption More Secure Elgamal Cryptosystem

Mr. Jaydip Thakkar
Department of Computer Science and Engineering
Nar Narayan Shastri Institute of Technology, Jetalpur

Abstract

Encryption and Decryption are two fundamental approaches in network security and cryptography. Both of these tools or we can say techniques are most commonly used nowadays. If we want to perform secure communication between sender and receiver than encryption and decryption are very useful. For this purpose, public key cryptography and private key cryptography is used. Here we present, we present an overview of the existing cryptographic system and will see some of the problems that arise in the existing cryptosystem. Then after we present the proposed system and provide advantages and implementation of our proposed system.

Keywords: Elgamal Cryptosystem, Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP)

I. INTRODUCTION

A. Definition of Cryptography

“Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack”.

B. Cryptographic Goals

However, there are other natural cryptographic problems to be solved and they can be equally if not more important depending on who is attacking you and what you are trying to secure against attackers. The cryptographic goals covered in this text (in order of appearance) are Confidentiality, Integrity, and Availability[7].

These concepts form what is often referred to as the CIA triad. These concepts embody the fundamental security objectives for both data and for information and computing services. A useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

C. Confidentiality:

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

D. Integrity:

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

E. Availability:

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad[7] to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

F. Authenticity:

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission of a message, or message originator.
G. Accountability:

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

II. RELATED WORK

An encryption scheme based on the integration of Enhanced RSA and Elgamal algorithm is introduced. Enhanced RSA algorithm is based on Integer Factorization Problem (IFP). On the other hand, Elgamal algorithm is based on Discrete Logarithm Problem (DLP). A combination of IFP and DLP is proposed. A comparison has been conducted for different public key encryption algorithms at different data size [5][6][9]. The encryption time and throughput of the naive scheme is computed and compared with the hybridized system of RSA and Elgamal algorithm. The aim of this paper is to make the novel algorithm efficient than the existing system as described above. As a result, the proposed algorithm holds an increased throughput and decreased encryption time as compared to the Elgamal and existing hybridized system of RSA-Elgamal.

Key generation, Encryption and decryption are performed in the following way:

![Diagram of key generation, encryption, and decryption processes]

<table>
<thead>
<tr>
<th>Message Size</th>
<th>RSA</th>
<th>Enhanced RSA</th>
<th>Elgamal</th>
<th>RSA-Elgamal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 KB</td>
<td>0.00326 sec</td>
<td>0.00157 sec</td>
<td>0.02697 sec</td>
<td>0.00778 sec</td>
</tr>
<tr>
<td>2 KB</td>
<td>0.00346 sec</td>
<td>0.00323 sec</td>
<td>0.03959 sec</td>
<td>0.01428 sec</td>
</tr>
<tr>
<td>3 KB</td>
<td>0.00479 sec</td>
<td>0.00450 sec</td>
<td>0.04763 sec</td>
<td>0.02177 sec</td>
</tr>
<tr>
<td>4 KB</td>
<td>0.00759 sec</td>
<td>0.00724 sec</td>
<td>0.05606 sec</td>
<td>0.02867 sec</td>
</tr>
<tr>
<td>5 KB</td>
<td>0.00829 sec</td>
<td>0.00786 sec</td>
<td>0.06758 sec</td>
<td>0.03862 sec</td>
</tr>
<tr>
<td>10 KB</td>
<td>0.01669 sec</td>
<td>0.01532 sec</td>
<td>0.12194 sec</td>
<td>0.07409 sec</td>
</tr>
<tr>
<td>20 KB</td>
<td>0.03186 sec</td>
<td>0.03122 sec</td>
<td>0.23498 sec</td>
<td>0.16017 sec</td>
</tr>
<tr>
<td>Average Time</td>
<td>0.01085 sec</td>
<td>0.01013 sec</td>
<td>0.06908 sec</td>
<td>0.04934 sec</td>
</tr>
<tr>
<td>Throughput (Megabytes/sec)</td>
<td>4.05069</td>
<td>4.33859</td>
<td>0.63622</td>
<td>0.89076</td>
</tr>
</tbody>
</table>

Fig. 1: Encryption time and Throuput for each method
III. EXISTING SYSTEM

- The Elgamal system is a public key cryptosystem based on the discrete logarithm problem.
- It consists of both encryption and signature algorithms.
- The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol [6].

A. Key Generation

Receiver A must do the following:
1) Generate a large random prime number \( p \)
2) Choose a generator number \( a \)
3) Choose an integer \( x \) less than \( p - 2 \), as a secret number.
4) Compute \( d \) where
\[
d = a^x \mod p
\]
5) Determine the public key \((p, a, d)\) and the private key \(x\)

B. Generator Number

How to test \( a \) generator or not:
1) \( a \) must be between 1 and \( p - 1 \)
2) Find \( \varnothing = p - 1 \)
3) Find all factors of \( \varnothing \) \( \{f_1, f_2, \ldots, f_n\} \) \(-\{1\}\)
4) \( a \) is a generator number if and only if
\[
wi = a^{\varnothing/qi} \mod p \neq 1 \text{, for all qi}
\]
C. Encryption

Sender B must do the following:
1) Obtain the public key \((p, a, d)\) from the receiver A.
2) Choose an integer \(k\) such that:
   \[1 < k < p-2\]
3) Represent the plaintext as an integer \(m\) where \(0 < m < p-1\)
4) Compute \((y)\) as follows:
   \[y = a^k \mod p\]
5) Compute \((z)\) as follows:
   \[z = (d^k \cdot m) \mod p\]
6) Find the cipher text \((C)\) as follows:
   \[C = (y, z)\]
7) The sender B sends C to the receiver A.

D. Decryption

Receiver A must do the following:
1) Obtain the cipher text \((C)\) from B.
2) Compute \((r)\) as follows:
   \[r = y^{p-1-x} \mod p\]
3) Recover the plaintext as follows:
   \[m = (r \cdot z) \mod p\]

I) Limitations Of Existing System
- The main disadvantage of ElGamal is the need for randomness, and its slower speed.
- Not secure against common modulus attack
- Not secure against known plaintext attack

IV. PROPOSED METHOD

- There are many cryptographic methods for encryption and decryption purpose.
- AES and DES are algorithms which provide greater security for this purpose.
- In our proposed work, we use a Chinese Remainder Theorem to provide better security and designing Encryption and Decryption algorithm.

A. Proposed Algorithm

INPUT is:
1) Keys \(P, Q\).
2) \(M\) (message to be encrypted)
and
OUTPUT is:
- Secured sending of message from A to B.

B. Key Generation

Generate Key()
{
Choose \(P\) and \(Q\) two large prime numbers of the form
\(4K + 3\) and \(P \neq Q\)
Calculate \(N = P \cdot Q\)
Public key = \(N\)
Private key = \((P, Q)\)
}
1) Generate key(B)
2) Transmit public key to A
3) Select the message \(M\) to be transferred by A to B.
4) N is the product of two prime numbers in the form that if they are divided by four, the reminder remains 3.
5) Now A sends a message to B by using the following encryption equation
   \[ C = P^2 \mod N \]
6) At the receiver side B, the decryption is performed. It creates four equally probable plaintexts.
7) Now B uses P and Q again while generating keys. P & Q are private keys for B
   \[ X_1 = C^{\frac{P+1}{4}} \mod P \]
   \[ X_2 = P - C^{\frac{P+1}{4}} \mod P \]
   \[ Y_1 = C^{\frac{Q+1}{4}} \mod Q \]
   \[ Y_2 = Q - C^{\frac{Q+1}{4}} \mod Q \]
8) Now Chinese remainder theorem is called for generating four equiprobable Plaintexts
   \[ P_1 = \text{CRT} (X_1,Y_1,P,Q) \]
   \[ P_2 = \text{CRT} (X_1,Y_2,P,Q) \]
   \[ P_3 = \text{CRT} (X_2,Y_1,P,Q) \]
   \[ P_4 = \text{CRT} (X_2,Y_2,P,Q) \]
Now B choose one of the P1, P2, P3, P4 as the final answer.

C. Advantages Of Proposed Method Are As Follows:
1) Encryption complexity is less in comparison to present system
2) Decryption complexity is also less
3) Key generation complexity is constant
4) There is no need of randomness
5) More secure against common modulus attack
6) Size of the message remains same during the encryption.

V. IMPLEMENTATION

A. About R

R is the leading tool for statistics, data analysis, and machine learning. It is more than a statistical package; it’s a programming language, so you can create your own objects, functions, and packages. Speaking of packages, there are over 2,000 cutting-edge, user-contributed packages available on CRAN[10]. Like all programs, R programs explicitly document the steps of your analysis and make it easy to reproduce and/or update analysis, which means you can quickly try many ideas and/or correct issues.

You can easily use it anywhere. It's platform-independent, so you can use it on any operating system. And it's free, so you can use it at any employer without having to persuade your boss to purchase a license. Not only is R free, but it's also open-source. That means anyone can examine the source code to see exactly what it’s doing. This also means that you, or anyone, can fix bugs and/or add features, rather than waiting for the vendor to find/fix the bug and/or add the feature--at their discretion--in a future release.

R allows you to integrate with other languages (C/C++, Java, Python) and enables you to interact with many data sources: ODBC -compliant databases (Excel, Access) and other statistical packages. Explicit parallelism is straightforward in R. several packages allow you to take advantage of multiple cores, either on a single machine or across a network. R has a large, active, and growing community of users.
B. How to Use R?

This is the first console page of the R software. Here we need to open the script of our R file. The security file we open here is named as Security.R.

When we open the file it will display like this:
This is the main script of our algorithm. When we want to execute this script first we need to select all the script and then we can execute it.

The execution will be like this:
C. Output File

This is the output file for our script.

VI. EVALUATION PARAMETER

A. Complexity Analysis of the Proposed Method:

- Encryption Complexity: \(O(M^2)\) Where M is the length of the vector
- Decryption: \(O(M)\)
- Key generation: \(O(1)\)

B. Complexity Analysis of Elgamal Method:

Elgamal is a hard problem. It takes a lot of time for encryption and decryption. It depends on diffie- Hellman. Whose complexity is \(O(M^3)\).

C. Comparison

<table>
<thead>
<tr>
<th>Method</th>
<th>Encryption Complexity</th>
<th>Decryption Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Method</td>
<td>(O(M^2))</td>
<td>(O(M))</td>
</tr>
<tr>
<td>Elgamal method</td>
<td>(O(M^4)).</td>
<td>(O(M^3)).</td>
</tr>
</tbody>
</table>

D. Computation Table

<table>
<thead>
<tr>
<th>No.</th>
<th>User Key</th>
<th>Public Key</th>
<th>Private Key</th>
<th>Four Intermediate Calculations</th>
<th>Four Equi- Probable Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>52</td>
<td>77</td>
<td>7,11</td>
<td>4,3,3,6</td>
<td>25,74,3,52</td>
</tr>
<tr>
<td>2</td>
<td>123</td>
<td>437</td>
<td>19,23</td>
<td>9,10,8,15</td>
<td>123,199,238,314</td>
</tr>
</tbody>
</table>
VII. CONCLUSION & FUTURE ENHANCEMENT

In our system we overcome the problem that arises in the previous system and it has also less time complexity and it is more powerful than the existing system. In our system we enforce Chinese Remainder Theorem and other function which provide better security against various vulnerabilities. Due to the enhanced securities, an attacker cannot easily misguide the user or reveal the main information. Hence our main purpose which needs to provide greater security to our system is served. In Future, our system can also be upgraded for digital signaling..

REFERENCES