An Advanced Cryptography Scheme

Ritesh Bagalkoti¹, Prof. Mr. Shamshekhar S Patil²

¹²Ambedkar Institute of Technology, Bengaluru

Abstract

Data Transfer in the digital world, due to the advent of Internet is inevitable. Sensitive or Non-Sensitive, Data of any kind has to be securely transferred in order to prevent it from all types of active and passive attacks. Sensitive data in the hands of a masquerader could be a curse. Cryptography can be defined as an art or science of protecting data. Availability of all cryptography and encryption algorithms still cannot ensure a safe and a passive-attack free environment.

Purpose of this project is to build a standard to be used for data transfer, which uses the features of both cryptography and encryption algorithms. Thus, enabling the two communication entities a secure communication environment.

Keywords: Cryptography, Encryption, Safe and Secure Data Transfer.

1. INTRODUCTION

A combination of the DES and the Public key cryptography algorithms is used to create the advanced cryptography scheme. Introduction of the above algorithms will be given.

1.1 DES Data Encryption Standard

A diagrammatic representation of the working of the DES algorithm is shown here.

The DES is an acronym for Data Encryption Standard, is an algorithm used for encryption of data. DES is an block cipher algorithm, so it uses fixed length of plain-text and converts it to same fixed length of cipher-text. DES uses a series of operations to achieve encryption.

Sequence of steps for the operation of a single round of DES Algorithm is as follows:

1. Outputs from the previous stage as the left block : L i-1 and right block : R i-1of 32 bits each.
2. The block R i-1 goes through an expansion stage after which, the size is increased to 48 bits.
3. Key parts, C i-1 and D i-1 of 28 bits each.
4. Each of these segments undergoes a left shift, which will be used as a final key, of size 48 K I.
5. An Exclusive-OR operation is performed taking input, block R i-1 and key K I.
6. Substitution-box is the core of the algorithm that performs substitution. Size of the output 32 bits.
7. Permutation is performed on the output of substitution stage.

Figure 2.4 Single Round of DES Algorithm
(8) A final Exclusive-OR is performed between block L i-1 and the Permutation output.
(9) Final blocks, L i and R i are obtained that form input for the next round.

Decryption is performed as an mirror opposite of actions in the Encryption to obtain the plain text back.

1.2 Public Key Cryptography.
A diagrammatic representation of the working of Public Key Cryptography is shown here:

Public Key Cryptography is a cryptography method that uses an asymmetric key pair, a public key and a private key. These keys are used for encryption and decryption. The public key is made widely available and distributed freely. The private key is kept secret.

The factor that differentiates Public Key Cryptography from Symmetric key cryptography is that, in Public Key Cryptography introduces a concept involving two distinct key pairs, one for encrypting and the other for decrypting.

The sequence of operations in the working:

(1) Assume Bob wants to send data to Alice.
(2) Bob will encrypt the data with Alice's public key.
(3) Alice gets the data and is able to unlock it with its own public key.
(4) Any other person other than Alice will not be able to read the data due to the absence of private key.

2. PROPOSED SYSTEM
The proposed system as already stated is an combination of both the explained algorithms. An attempt to make a communication environment that exercises the features of both by following these steps.

Step (1) Plain text: Plain text is collected from the user through console of any length.

Step (2) Appending Key: Sender will encrypt the data with Receiver's public key.

Step (3) Mix: The Mix stage splits the field, combined with the Plain text and Key.

Step (4) Generate a 2 digit prime number: A random 2 digit prime number is generated.

Step (5) Split & encrypt: In this stage, the generated 2 digit prime number is split and after the first digit's place a random field of the second digit is added.

For example, for the number 13, the first digit is 1 and the second digit is 3. So the final output for the string “HELLO” is HrrrELLO.

Step (6) The final pattern is sent to the destination.

3. Implementation and Results

1.1 Plain-text: The plain text is simply collected through the console using a scanner class. The string entered here is “something”.

Example of this stage is,

```
<terminated> client [Java Application] /usr/lib/jvm/java-7-openjdk-amd64/bin/java
in client
Enter String.
something
$string entered is,something
in client
```

1.2 Appending key: The Sender will encrypt the string with the receiver's Public key.

Example of this stage is,

```
in encrypt
19
Pattern is somethingabcdef123A
in mix
pattern value from mix is somethingabcdef123A
```

The string is appended with the receiver's public key, which is a field of characters containing both alphabets and numbers, like “abcdef123A”. The last alphabet denotes the receiver's ID.

1.3 Mix stage:

In this stage, the pattern is split in half and the lengths are calculated.

Example of this stage is,

```
pattern value from mix is somethingabcdef123A
a is something
b is abcdef123A
29
```

The string pattern, “somethingabcdef123A” is split in halves in a and b as “something” and “abcdef123A”.

1.4 Generate prime no.: In this stage, a random two digit prime number is generated using BigInteger Probable Prime method and its digits are split.

```
from big int13
in split
digit 1 is 1
digit 2 is 3
in split
```

The value from big integer is, 13 and using remainder method, the number is split in two digits as digit 1 and digit 2.

1.5 Split and Encrypt: In this stage, according to the two digits, a string is inserted. After the first digit, a string of the length of the second string is inserted.

Example of this stage is,
At the destination side, at the same series of events is performed in opposite way to obtain the original text.

4. CONCLUSION AND FUTURE WORK
Goal of our proposed work was to combine the features of two algorithms, of encryption and cryptography. An advanced cryptography scheme that works on the basis of these and pertains more features was presented.

REFERENCES
[1] A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms TAHER ELGAMAL, MEMBER, IEEE