A Survey On Some Encryption Algorithms And Verification Of RSA Technique

Abdul Hai Al Hadi

Abstract: Information security becomes much important in data storage and transmission. The term information security refers to the processes and methodologies which are designed and implemented to protect data from unauthorized access, use, misuse, disclosure, modification or disruption. Encryption algorithm play important roles in information security. This paper provides case study of five encryption algorithms: DES, 3DES, Blowfish, CAST, RSA and also provides encryption and decryption data by using the RSA asymmetric encryption algorithm. Simulation has been conducted using C language. Experimental results are given to analyses the implementation of RSA algorithm.

Index Terms: Encryption, Secret key encryption, Public key encryption, DES, 3DES, Blowfish, CAST, RSA encryption.

1 Introduction

Encryption is the process of transforming plain text information using an encryption algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Security is one of the main issues in designing encryption algorithm. Many encryption algorithm are widely available that can be classified into Symmetric (private) and Asymmetric (public) keys encryption. Symmetric encryption techniques are almost 1000 times faster that asymmetric techniques as they require less computational processing power [5].For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form [1].In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).Public key encryption is biased on mathematical function, computationally intensive and is not very efficient for small mobile devices [6, 7].

2 Case Study Of Five Encryption Algorithms

A. DES Encryption Algorithm:

Data Encryption Standard (DES) algorithm: General information
Designers: IBM
First published: 1977 (standardized in January 1979)
Derived from: Lucifer
Successors: Triple DES, G-DES, DES-X, LOKI89, ICE
Key sizes: 56 bits
Block sizes: 64 bits
Structure: Balanced Feistel network
Rounds: 16

- *Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Santosh, Tangail-1902, Bangladesh,*
- *hadi.mbstu@gmail.com*

B. 3DES Encryption Algorithm :

3DES algorithm: General information
First published: 1998 (ANS X9.52)
Derived from: DES
Key sizes: 168, 112 or 56 bits (Keying option 1, 2, 3 respectively)
Block sizes: 64 bits
Structure: Feistel network
Rounds: 48 DES-equivalent rounds

Advantages of DES and 3DES as encryption algorithms:

- Both use symmetric keying, making them much faster at encryption than asymmetric key encryption algorithms.
- Both are easy to implement in both software and hardware when compared to other encryption algorithms.

Disadvantages of DES and 3DES as encryption algorithms:

- Because both use symmetric keying, sharing the symmetric key (or keys) is a problem when the two devices are separated by a public network. Asymmetric key encryption algorithms do not suffer this problem.
- Newer encryption algorithms have been developed that are much faster and more secure than 3DES, such as AES, RC-6, and Blowfish.

C. Blowfish, DES and CAST Encryption Algorithm:

Blowfish is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes. It is significantly faster than DES . Blowfish is unpatented, license-free, and available free for all uses.

D. CAST, DES and 3DES Encryption Algorithm:

CAST is named for its developers, Carlisle Adams and Stafford Tavares. CAST is similar to DES and uses a 128- or 256-bit key structure. It is less secure than 3DES, but is faster.

E. RSA Encryption Algorithm:

RSA are the initials of the three creators: "Ron Rivest, Adi Shamir and Leonard Adleman "in 1977, so RSA stands for Rivest, Shamir, and Adleman. It is most widely used public key algorithm. The two main branches of public key cryptography are Public key encryption and Digital signatures. So it supports

Encryption and Digital signatures. Get its security from integer factorization problem. Relatively easy to understand and implement and Patent free (since 2000). RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, SSH, SILC, and many more.

Advantage and Disadvantage of RSA Cryptography Compared with DES, 3DES, Blowfish, CAST Cryptography:

1. Primary advantage of RSA cryptography is increased security and convenience. Private keys never need to transmitted or revealed to anyone. But DES, 3DES, Blowfish, CAST Cryptography the secret keys must be transmitted. And there may be a chance that an enemy can discover the secret keys during their transmission.
2. Other major advantage of RSA cryptography is that it can provide a method for digital signatures.
3. A disadvantage of using RSA cryptography for encryption is speed. DES, 3DES, Blowfish, CAST Cryptography are significantly faster than RSA cryptography.
4. RSA cryptography may be vulnerable to impersonation, however, even if user's private keys are not available.
5. RSA cryptography is usually not necessary in a single-user environment. In general, it is best suited for an open multi-user environment.

The original algorithm of RSA encryption algorithm:

1. Generate two primes, p and q, of approximately equal size such that product n = pq is of the required bit length.
2. Compute n = pq and (phi) f = (p-1)(q-1).
3. Choose an integer e, 1<e<phi, such that GCD (e, phi) = 1
4. Compute the secret exponent d,1<d<phi, such that ed=1(mod phi).
5. The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q, and phi secret.[sometimes to write the private key as (n, d) because need the value of n when using d.]
   - n is known as the modulus.
   - e is known as the public exponent or encryption exponent.
   - d is known as the secret exponent or decryption exponent.

3 Experimental Design

Encryption and decryption data by using the RSA asymmetric encryption algorithm. Simulation has been conducted using C language.

4 Experimental Results And Analysis

A. Summary of RSA:

1. n = pq, where p and q are distinct primes.(A prime is a number divisible only by that number and 1)
2. phi, f = (p-1)(q-1)
3. e<n such that GCD(e, phi)=1
4. $d = e^{-1}$ mod phi.
5. $c = m^e$ mod n.
6. $m = c^d$ mod n.

B. Key Generation:

(1) Generate two prime numbers p and q.
p=7
q=17
(2) Let n=pq
n=7*17
=119
(3) Let phi=(p-1)(q-1)
=(7-1)(17-1)
=6*16
=96
(4) Choose a number, e co prime to phi Euclid's algorithm is used to find the GCD of two numbers
e=2 =>GCD(2, 96)=2(NO)
e=3 =>GCD(3, 96)=3(NO)
e=4 =>GCD(4, 96)=4(NO)
e=5 =>GCD(5, 96)=1(YES)
(5)Determine $d=e^{-1}$ mod phi
=1/e mod phi
Using the Extended Euclid's algorithm
d=77
(6) Public key=(n, e)=(119, 5)
Private key=(n, d)=(119, 77)

According to the above key, now encrypt the data (Plaintext): Student Of MBSTU

Cipher text for this data is:
104 114 87 53 33 94 114 95 51 42 19 104 84 85

If Cipher text is:
104 114 87 53 33 94 114 95 51 42 19 104 84 85

Plaintext: Student Of MBSTU

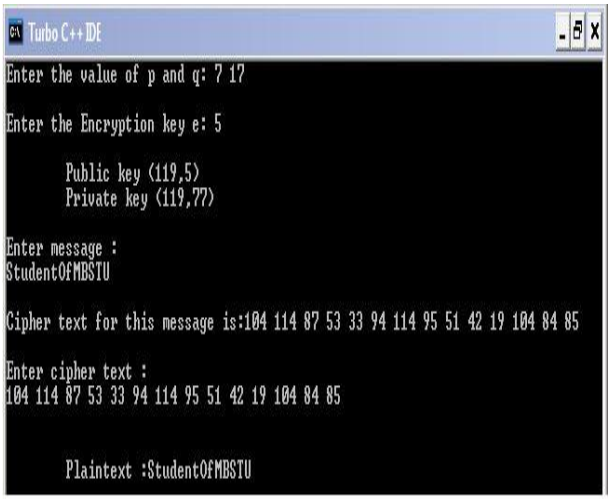

Fig.: The Implementation of RSA using C language

5 Conclusion

With the rapid growing of internet and networks applications, data security becomes more important. Encryption algorithms play a crucial role in information security systems. In the future work we will investigate the encryption algorithms and implement several algorithms with different parameters.

REFERENCES

[1]. Shashi Mertra Seth, Rajan Mishra, “Comparative Analysis” of Encryption Algorithoms For Comunication”, IJCST VOL.2, Issue 2, June 2011.

[2]. Erik Olson, Woojin Yu, “Eneryption for Mobil;e Compoting”

[3]. Dr.S.A.M Rizvi, Dr.Syed Zeeshan Hussain and Neeta Wadhwa, “A Comparative Study of Two Symentirc Encryption Algorithoms Across Different Platfroms”

[4]. Abdel-Karim AI Tamimi, “Perpormance Analysis of Data Encryption Algorithom”

[5]. M A Matin, Md. Monir Hossain2, Md Foizul Islam2, Muhammad Nazrul Islam2, M Mofazzal Hossain3 “Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN”

[6]. P.Ruangchaijatupon, P.Krishnamurthy, “Encryption and power consumption in wireless LANs-n,” The Third IEEE workshop on wireless LANS, pp. 148-152, Newton, Massachusetts, sep. 27-28,2001.

[7]. Marshall D.Abrams, Harold J.podell on Cryptograohy.

[8]. Anoop Ms, “public key cryptography Applications Algorithms and Mathematical Explanations”

[9]. http:// en.wikipedia.org/wiki/information security

[10]. http:// en.wikipedia.org/wiki/Encryption

[11]. “Information security principles and practice”, mark stamp.