© International Scientific Conference on Engineering, Technologies and Systems
TECHSYS 2018, Technical University – Sofia, Plovdiv branch
17 – 19 May 2018, Plovdiv, Bulgaria

RSA ENCRYPTION ALGORITHMAND CRYPTANALYSIS OF RSA

TARIK YERLİKAYA, CANAN ASLANYÜREK

Abstract: *With the development of technology the amount of information roaming through network is increasing in a daily basis, and this brings about the issues of information security. In this study, encryption algorithms that are used for the transmission of secure data were classified and RSA cryptosystem that one of the public key cryptography algorithms used of information security and digital signature was investigated. First, it announced the features of asymmetric and symmetric encryption algorithms. The structure and features of RSA cryptosystem algorithm was announced. Focused on cryptanalysis and performance of RSA cryptosystem.*

Key words: *RSA, Encryption Algorithms, Cryptanalysis*

1. Introduction

The privacy of information of great importance has been known since ancient times. For this reason, there are many methods developed for the confidentiality of information. For this reason, there are many methods developed for the confidentiality of information. Previously these methods the displacement of the characters of the text, and of the deterioration of the shape of the text was performed. By the developing technology, with computers has evolved into methods.

Cryptology, cryptography (encryption) and cryptanalysis (decoding) is divided into two. Cryptography, works to protect the security of communication [1]. Cryptanalysis is a set of methods involving analysis of cryptosystems.

Cryptography, symmetric and asymmetric cryptography are divided into two groups. 20. Century, widely used in symmetric cryptography is used a single key called a secret key for encryption and decryption operations [2]. Those who use this method should make a secure channel to share the key.

Public-key cryptosystem, asymmetric cryptography, called public and private key, two different keys is used. While in the encryption process public key and the private key is used in the decryption process. The person who learns the public key cannot open the encrypted text. Because it is difficult to obtain the private key from the public key. The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT. In cryptography, RSA is an algorithm for public key cryptography [1,2,4,10].

This study will examine encryption algorithms. It will focus on the widely used RSA encryption algorithm. Performance and cryptanalysis of RSA cryptosystem will be examined

2. Encryption Algorithms

Encryption techniques are generally classified in two groups [4,5]:

- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithms

Symmetric encryption algorithms are algorithms for cryptography that use the same secret key for both encryptions of plaintext and decryption of cipher text. This key is known by the sender and receiver. Symmetric

ISSN Online: 2535-0048

encryption algorithm runs faster than asymmetric encryption algorithms. However, symmetric encryption algorithms are powerless against attacks than asymmetric encryption algorithms. The sender encrypts plaintext and sends it to the recipient. The receiver converts the text that is encrypted with a secret key to plaintext. For this reason, key is shared between the sender and receiver. This is one disadvantage of symmetrical encryption algorithms. Because, if the encryption key is known the obtaining of information is very simple. Examples of common symmetric algorithms include AES, DES, 3DES, Blowfish, IDEA and RC4[4,6].
There is no problem of secret key asymmetric encryption algorithms. Asymmetric encryption systems are used different keys for encryption and decryption operations. These keys are called a public key and private key. These keys are generated together. The person with any of these keys cannot produce the other key this is impossible. Therefore, asymmetric encryption is more secure than symmetric encryption. Performance of asymmetric algorithms is significantly lower than symmetric algorithms. In asymmetric algorithms both sender and recipient has pair of keys. The private key of person belongs to him. The private key mustn't be known by anyone else. The public key of person is used by anyone who wants to send a message to this person. The sender encrypts the message with the public key of the recipient. The recipient opens the message with private key of own.

3. RSA Encryption

RSA encryption system is best known of asymmetric encryption algorithms [7]. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977[3,8]. This encryption has been developed on the basis of a simple mathematical account. Then it is developed compatible with asymmetric encryption algorithms. Both message encryption and digital signature process is used safely [9,11]. RSA encryption algorithm used public and private keys are generated by the receiver. The public key is open to everyone. The sender encrypts the message with this public key and sends it. The receiver opens the message with the secret key and obtains the original message. The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. The following key generation, encryption and decryption processes are given.

4. Key generation algorithm

1. Generate a pair of large, random primes p and q.
2. Compute the modulus N as N = p.q and $\varnothing(N) = (p-1).(q-1)$
3. Choose an integer e, $1 < e < \varnothing(N)$, such that $\gcd(e, \varnothing(N)) = 1$.
4. Compute the secret exponent d, $1 < d < \varnothing(N)$, such that $ed \equiv 1 \pmod{\varnothing(N)}$
5. Output (N, e) as the public key and (N, d) as the private key.

N is known as the modulus
e is known as the public exponent
d is known as the secret exponent

5. Encryption

1. The sender generates the public key of recipient. (N,e)
2. Represents the plaintext message as a positive integer m, $1 < M < N$
3. Computes the cipher text $C \equiv M^e$ mod N
4. Sends the cipher text c to recipient.

6. Decryption

Recipient does the following:

- $M^{\varnothing(N)} \equiv 1 \bmod N$
- $e.d \equiv 1 \bmod \varnothing(N)$
- $e.d \equiv k.\varnothing(N) + 1$
- $C^d \equiv M^{e.d} \equiv M^{k.\varnothing(N)+1} \equiv (M^{\varnothing(N)})^k . M$

  $\equiv M \bmod N$

Cryptanalysis of RSA Encryption Algorithm cryptanalysis is related to the breaking of the password. Cryptanalysis is a process of finding weaknesses in cryptographic algorithms and using these weaknesses to decipher the cipher text without knowing the secret key. Cryptanalysis is an important tool in assessing the reliability of encryption algorithms. The RSA algorithm encryption method widely used because it is attacked a lot. Cryptanalytic attacks on RSA algorithm either aim at exploiting the mathematical vulnerabilities of RSA. RSA encryption algorithm uses a very large prime numbers. So it is difficult to solve. These are Factorization Attack, Timing & Brute-Force Attacks, Implementation Attacks, Mathematical Brute-Force Attack. This algorithm breaks can be explained in several different ways. But the most damaging attack is a cryptanalyst find the secret key from the public key. The one who carried out these attacks, all encrypted messages can be read. There is an easy way to do it in the RSA encryption algorithm. This way, the primes factorization of N separation or calculating p and q. D can be calculated using p,q and e. This decryption process is in the most difficult thing in the primes factorization of N separation. To make more secure of the RSA algorithm is used a very large number N.

7. Conclusion

With the development of technology the amount of information roaming through network is increasing in a daily basis, and this brings about the issues of information security. The transmission of information to the desired address must be performed safely. Encryption / decryption (encryption-decryption) is used to ensure the security of data in computer networks. In information security, digital signature widely is used RSA one of the public key encryption. RSA crypto system used in large numbers to provide the security. If the number N is large, the factorization process takes longer. This also reduces the operating speed of the algorithm.

In this study, RSA encryption algorithm is one of the most important asymmetric encryption algorithms was announced. The cryptanalysis of RSA algorithm are examined. Consequently, there is one important RSA encryption algorithms used today. Importance is increasing day by day. Large prime numbers are used to make this algorithm more secure. Reduces the efficiency of this algorithm. In order to increase the efficiency of this algorithm, scientists continue to work.

REFERENCES

[1] Yıldırım H. M ., 2014. Bilgi Güvenliği ve Kriptoloji. Uluslararası Adli Bilişim Sempozyum, http://hmurat.bilkent.edu.tr/kripto-01062014.pdf.

[2] Okumuş, İ., 2012. RSA Kritosisteminin Hızını Etkileyen Faktörler, Doktora Tezi, Atatürk Üniversitesi.

[3] Schneider B. ”Applied Cryptography Second Edition”, John Wiley & Sons, Inc., New York, 1996.

[4] Stallings W., “Cryptography and Network Security: Principles and Practice”, ISBN 0-13-869017-0, Prentice Hall, 1998.

[5] Schneier, B., “Applied Cryptology, Second Edition: Protocols, Algorithms, and Source Code in C”, Wiley Publishing, (1996)

[6] Salomaa, A., “Public-Key Cryptography”, Springer Verlag, New York, (1990).

[7] Bellare, M., and Rogaway, P ., “Optimal Asymmetric Encryption-How to encrypt with RSA”. Advances in Cryptology-CRYPTO’94.

[8] Yıldırım, K. , 2006. Veri Şifrelenmesinde Simetrik Ve Asimetrik Anahtarlama Algoritmalarının Uygulanması. Y. Lisans Tezi, Kocaeli Üniversitesi.

[9] Koltuksuz A., “Elektronik Ticarette Güvenlik, Özgürlük Denetimi, Doğruluk- Bütünlük ve Sayısal İmza“, 4.Türkiye İnternet Konferansı, 1998, İstanbul, Türkiye.

[10] Yerlikaya, T. , 2006. Yeni Şifreleme Algoritmalarının Analizi, Doktora Tezi, Trakya Üniversitesi.

[11] Yerlikaya, T., Buluş, E., Ve Buluş, H. N. 2007. RSA Şifreleme Algoritmasının Pollard Rho Yöntemi İle Kriptanalizi.

Organization:
Tarık YERLİKAYA
Trakya University

Canan ASLANYÜREK
Kırklareli University