FACTORS AFFECTING PERFORMANCE OF RSA CRYPTOSYSTEMS

Sachin Upadhyay[1], Amit Kumar Jain[2]

[1,2]*Department of Mathematical Sciences and Computer Applications,*
Bundelkhand University, Jhansi, (India)

ABSTRACT

Communication is one of the necessities of human being. The effectiveness of computer communication over the network is mainly based on the type of cryptosystem selected for the encryption, decryption & also the proper implementation of the algorithm. The internet made the communication more flexible and resourceful. Security of information now a day is one of the most vital aspects for any organizations. Every now and then agencies try to develop the cryptosystems for the full proof communication of information on any medium. This paper focuses on various factors affecting the performance of RSA Cryptosystem .Also analyses the comparison study for some of the cryptosystems.

Keywords: Cryptanalysis, Decryption, Encryption.

I. INTRODUCTION

A cipher is an algorithm for performing encryption or decryption — a series of well-defined steps that can be followed as a procedure. A cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. Therefore, the term "cryptosystem" is most often used when the key generation algorithm is important. Many ciphers have been developed so far in the field of communication to enhance the security of the information that has been transmitted through the internet In non-technical usage, a "(secret) code" typically means a "cipher". Within technical discussions, however, the words "code" and "cipher" refer to two different concepts. Codes work at the level of meaning — that is, words or phrases are converted into something else and this chunking generally shortens the message. In spite of adopting large block size, wide key length, complex substitution and other key aspects in designing the ciphers an, ,the security of the information and network security is still a challenge. It has been indicated that the security of algorithms and performance of a given algorithm depends on variety of parameters like keys sizes, encryption & decryption techniques used & above all the selection of algorithm plays the most important role for securing our data. This paper shows the analytical results of the cipher which was picked on the basis above parameters.

II. PRINCIPLES OF PUBLIC KEY CRYPTOSYSTEM

Invention of PKC by Whitefield Diffie and Martin Hellman in 1976, solved the past problems key managements and digital signatures of classical cryptosystem. Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key. Under RSA either of the two related keys can be used for encryption, with the other used for decryption.

A public key cryptosystem is a pair of families $\{E_k\}$ and $\{D_k\}$, K ϵ key space K, of algorithms representing invertible transformations

$E_k : P \rightarrow C$ and $D_k : C \rightarrow P$

i. For every K, E_k is the inverse of D_k.

ii. For every K, it is easy to compute E_k and D_k.

iii. For almost every K, each easily computed algorithm equivalent to D_k is computationally infeasible to drive from E_k.

iv. For every K, it is feasible to compute inverse pairs E_k and D_k from K.

III. KEYS USED IN CRYPTOSYSTEM

The keys used in various cryptosystems basically depend on its internal structure like what size of key should be appropriate when secrecy is concerned, Key size is a very important part which affects the security of the cipher. Picking larger keys might create the problems in encryption & decryption etc. is the majors who we need to keep in mind while using any type of cryptosystem. For example, public keys used in the RSA system are the product of two prime numbers. Thus public key systems require longer key lengths than symmetric systems for an equivalent level of security. 3072 bits is the suggested key length for systems based on factoring and integer discrete logarithms which aim to have security equivalent to a 128 bit symmetric cipher. Elliptic curve cryptography may allow smaller-size keys for equivalent security, but these algorithms have only been known for a relatively short time and current estimates of the difficulty of searching for their keys may not survive. Many ciphers employ separate key generation algorithm which works in parallel with the associated encryption and decryption algorithm. Response time & processing time mainly decides the efficiency of the algorithm used.

IV. CONFUSION AND DIFFUSION

In cryptography, confusion and diffusion are two properties of the operation of a secure cipher which were identified by Claude Shannon in 1949. Confusion property makes the cryptanalysis very difficult and thus makes the algorithm stronger. Confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible. This can be achieved by the use of a complex scrambling algorithm that depends on the key and the input. Diffusion means that the output bits should depend on the input bits in a very complex way. In a cipher with good diffusion, if one bit of the plaintext is changed, then the ciphertext should change completely, in an unpredictable manner. An example of diffusion is to encrypt a message $M = m_1, m_2, m_3$, of characters with an averaging operation

$$y_n = \left(\sum_{i=1}^{k} m_{n+i}\right) \bmod 26$$

adding k successive letters to get a ciphertext letter y_n

V. THE STRENGTH OF RSA CRYPTOSYSTEM

There are three approaches to attack the RSA cryptosystem, which are briefly discussed here:

5.1 Brute Force Attack

The success & failure of brute force attack depends upon the length of key space used by the respective cryptosystem. By using a large key space, it is possible to avoid this attack. RSA crypto system uses the key as large as possible for the performance and to avoid brute force attack.

5.2 Factoring Attack

In RSA cryptosystem, in order to decipher the message one needs the private key of the recipient, which being exclusively in the hand of the recipient of the message. To determine the private key of any user, an attacker requires the factor of n. So now the question arises that can it be possible to produce the private key d from the public key e or to calculate the value of ∅ (n) i.e. p & q are the relative prime numbers & ∅ (n) = (p-1) (q-1). Choosing a large size of n is an ultimate solution for the security of RSA cryptosystem.

5.3 Precaution in Choosing the Prime Numbers

While selecting the prime number p & q should be differencing in length by a few digits. They should be closer. The product of (p-1) (q-1) should be small & the gcd of (p-1) (q-1) should be small.

VI. RESULTS

Some of speed results of RSA cryptographic algorithms. All were coded in C++, compiled with Microsoft Visual C++ 2005 SP1 (whole program optimization, optimize for speed), and ran on an Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode.

Operation	Milliseconds/Operation	Megacycles/Operation
RSA 1024 Encryption	0.08	0.14
RSA 1024 Decryption	1.46	2.68
RSA 2048 Encryption	0.16	0.29
RSA 2048 Decryption	6.08	11.12
RSA 1024 Signature	1.48	2.71
RSA 1024 Verification	0.07	0.13
RSA 2048 Signature	6.05	11.06
RSA 2048 Verification	0.16	0.29

Table Shows The Application For Public-Key Cryptosystem

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes

Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

VII. CONCLUSION

Security of information in transit is a very important task in secured communication. Many Ciphers are available which have been developed by using arithmetic and logical operations. The two important desirable properties of the RSA cryptosystems are its speed and security. Speed refers to the time taken by the algorithm to convert a given plaintext to cipher text. The Key plays a very important role in encryption and decryption operations. The Security of the algorithm is based on the key size. The increase in the key size reduces the speed of the algorithm but in turn increases the security. Thus the aim of the designer is to design efficient cryptosystems with acceptable speed and appreciable security strength with large key length. Implementation procedures also play a major role in RSA cryptosystems design.

REFERENCES

[1] Cryptography & Network Security by Kumar Manoj, Krishna's Prakashan Media (P) Ltd.

[2] Cryptography and Network Security, Principles and Practices-William Stallings Third Edition.

[3] Applied Cryptography-Bruce Schneier Second Edition.

[4] Introduction to Modern Cryptography, - jonathan Katz, Yehuda Lindell.

[5] A Performance Analysis of Encryption Algorithms' Text length size on Web Browsers-Syed Zulkarnain Syed Idrus, syed AlweeAljunid, Salina Mohd Asi, Suhizaz sudin and Badlishah Ahmad, school of Computer and ,ommunication Engineering, University Malasia Perlis, Perlis, Malaysia.