A Modified RSA Cryptosystems and Analysis

Ravi Raj, Yogesh Shriram Solunke

Abstract*— As the growth of the Internet and electronic commerce have brought to the forefront the issue of privacy in electronic communication. Large volumes of personal and sensitive information are electronically transmitted every day. In this paper we present modified RSA algorithm and analysis for secure data transmission. The security of RSA public key cryptosystem is based on the assumption that factoring of a large number (modulus) is difficult. In RSA if one can factor modulus into its prime numbers then the private key is also detected and hence the security of the cryptosystem is broken. Encryption is the standard method for making a communication private with RSA Algorithm. In which one public key and one private have introduced, resulted from two prime number introduced. Here we have introduce n Prime number with evolve method in a modified RSA cryptosystem to provide security over the networks. So, the security of RSA public key cryptosystem is increased due to increase in difficulty of the factoring of a large number (modulus) with increase in prime number and this technique provides more efficiency and reliability over the networks.

Index Terms*—Key, Encryption, Decryption, n prime numbers, RSA Algorithm.

I. INTRODUCTION

In the modern world, everywhere Internet is essential in the communication between millions of people and is being increasingly used as a tool for ecommerce, security becomes a tremendously important issue to deal with upload web pages and other documents from a private development machine to public webhosting servers. Transfer of data need special authenticated mechanism. As a communications and transmission of files over internet has increased exponentially since last few years, there is need of security in such data transfer. One of the solutions to secure communication is cryptography. It is the process of converting plain text into encrypted text and decrypt cipher text to plain text at other end. It is encrypted into cipher text with a cryptographic algorithm, which will in turn be decrypted into usable plaintext. In symmetric key cryptography; key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES). There are challenge in the technique: the key should be transmitted over the secure channel from sender to receiver but if the secure channel exist then there is no need of encryption but there is no practical channel exist, that's the need of encryption.

Manuscript Received on February 2015.

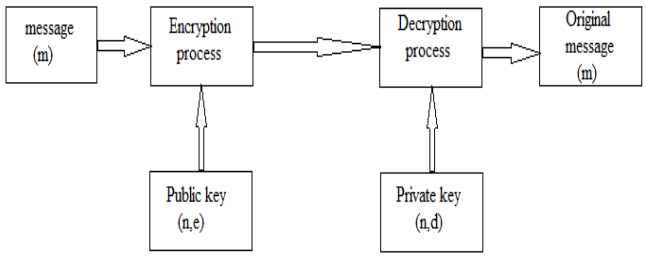
Ravi Raj, Department of Communication Systems, IIITDM Kancheepuram, Chennai, India.

Sriram S. Solunke, Department of Communication Systems, IIITDM Kancheepuram, Chennai, India.

In asymmetric algorithm different keys are used to encrypt and decrypt the data. RSA is widely used in ecommerce protocols. With sufficiently long keys and the use of up-to-date implementations; RSA is believed to be totally secure. RSA is well known cryptography algorithm among different. Which is asymmetric cryptography algorithm developed in 1977.this cryptography uses a pair of related keys, one for encryption and other for decryption. One key, which is called the private key, is kept secret and other one known as public key is disclosed and this eliminate the need for the sender and the receiver to share secret key. In this paper we introduce a modified RSA algorithm. In our algorithm we have consider the n number of prime numbers to increase the security over network And we have also analyzed with evolved method.

II. A BRIEF ANALYSIS OF RSA ALGORITHM

RSA (Rivest, Shamir & Adleman) is asymmetric cryptographic algorithm developed in 1977. It generates two keys: public key for encryption and private key to decrypt message.



RSA algorithm consist of three phases: key generation, encryption and decryption.

A. Key Generation

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

- Choose two very large prime numbers p and q:
  For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length.
- Compute n = pq:
  n is used as the modulus for both the public and private keys.
- Choose an integer e such that $\gcd(e,(p-1)(q-1))=1$ and e is released as the public key exponent.
- Determine d
  As we know that $ax+by=1$ so, we can write,

$$e.x=1+y(p-1)(q-1)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

i.e. $e.d = 1 + k(p-1)(q-1)$

d is kept as the private key exponent. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q must also be kept secret because they can be used to calculate d.

B. Encryption

Ravi transmits her public key (n, e) to yogesh and keeps the private key d secret. Yogesh then wishes to send message m to Ravi. Then he computes the ciphertext c

$$c = m^e \bmod n$$

Yogesh then transmits c to Ravi.

C. Decryption

Ravi can recover m from c by using her private key exponent d via computing

$$m = c^d \bmod n$$

there are more efficient methods of calculating c^d using the precomputed values and final outcome be m.

III. A Modified RSA Algorithm analysis

As we discussed the RSA algorithm in account of two large prime numbers through which little easy to find out the private key. So, In this paper we are introducing an algorithm that is modification to the existing RSA Algorithm. In modified RSA Algorithm, we have consider Four large prime numbers to overcome the problem on existing and It should be become very difficult to find out the private key because It should be very difficult to factor the modulus in four large prime numbers. Similar to existing one here also have one public key and one private key. There is also have three phase: key generation, encryption and decryption.

A. Key Generation

A Modified RSA also involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key and decrypted by the private key. The keys for the RSA algorithm are generated the following way:

- Choose four very large prime numbers p, q, r and s:
  For security purposes, the integer's p, q, r and s should be chosen at random, and should be of similar bit-length.
- Compute n = pqrs:
  n is used as the modulus for both the public and private keys.
- Choose an integer e such that
  $$\gcd(e,(p-1)(q-1)(r-1)(s-1)) = 1$$
  and e is released as the public key exponent.
- Determine d
  As we know that $ax + by = 1$ so, we can write,
  $$e.x = 1 + y(p-1)(q-1)(r-1(s-1)$$
  i.e. $e.d = 1 + k(p-1)(q-1)(r-1)(s-1)$

here d is also kept as the private key exponent. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q. r, s must also be kept secret because they can be used to calculate d.

B. Encryption

Ravi transmits her public key (n, e) to yogesh and keeps the private key d secret. Yogesh then wishes to send message m to Ravi. Then he computes the ciphertext c

$$c = m^e \bmod n$$

Yogesh then transmits c to Ravi.

C. Decryption

Ravi can recover m from c by using her private key exponent d via computing

$$m = c^d \bmod n$$

Which can be written as

$$m = m^{e.d} \bmod n$$

$$m = m^{1+k(p-1)(q-1)(r-1)(s-1)} \bmod n$$

Now, message can decrypt when

$$m^{k(p-1)(q-1)(r-1)(s-1)} = 1 \bmod n$$

and this can be proved as we know that

$$(1+a)^p = p_{c_0} a^p + p_{c_1} a^{p-1} + p_{c_2} a^{p-2} + \ldots\ldots\ldots p_{c_p} a^0$$

$$(1+a)^p = (a^p + 1) \bmod p$$

Now, apply Fermat's little theorem. This theorem states that if p is prime and p does not divide an integer a.

So, $a^p = a \bmod p$

Similarly, $a^q = a \bmod q$

$a^r = a \bmod r$

$a^s = a \bmod s$

Now, apply Chinese remainder Theorem.

so, we can write $m^{k(p-1)(q-1)(r-1)(s-1)} = 1 \bmod n$

hence message have decrypted, which results m=m.

IV. Conclusion

The study of various algorithms used for the secured communication in network has been done. From the related work it has been observed that the strength of security of encrypted data has been increased. Because it depends on upon the key management, type of cryptography and no of prime number. For the task the optimal selection of prime number makes the model optimized and from discussed process it have cleared the n number of prime number can satisfied the RSA algorithm. The more prime number having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data.

References

[1] Ajay Kakkar, M. L. Singh and P. K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012

[2] Behrouz A Forouzan, "Data Communications and Networking", McGraw-Hill, 4th Edition.

[3] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE The 6th International Forum on Strategic Technology, 2011, Volume 2, page 22-24.

[4] Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9, ISSN 0148-9615.

[5] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, June 2011, Vol. 2, Issue 2, pp. 292-294.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

[6] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), February 2013, Volume-1, Issue-4, ISSN: 2319–6378.
[7] S. Sharma, P. Sharma, R. Shankar Dhakar, "RSA Algorithm Using Modified Subset Sum Cryptosystem", Computer and Communication Technology (ICCCT), 2011 2nd International Conference, Sept. 2011, pp. 457 - 461
[8] Yunfei Li, Qing Liu, Tong Li, "Design and implementation of an improved RSA algorithm" E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference (Volume:1), April 2010, pp. 390 – 393.

Ravi Raj, pursuing Master of Design in Communication System from Indian Institute of Information Technology: Design & Manufacturing Kancheepuram, Chennai, India. His current research interest areas are Communication, RF & Microwave and Cryptography. He has awarded 2nd position in international conference (student paper contest) for best paper.

Yogesh Shriram Solunke, pursuing Master of Design in Communication System from Indian Institute of Information Technology: Design & Manufacturing Kancheepuram, Chennai, India. His current research interest areas are Communication & Cryptography.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.