



An Efficient RSA Based Technique for the Encryption and Decryption

Sharad Morolia^[1], Professor Manoj Dhawan^[2]

Department Of Information Technology

Shri Vaishnav Institute Of Technology and Science, Indore (M.P.)

Rajiv Gandhi Proudhyogiki Vishwavidyalaya, Bhoapl(M.P.)

INDIA

Abstract: RSA cryptosystem is the most commonly used public key cryptosystem. It is the first public key cryptosystem. The strength of this cryptosystem is based on the larger key size. There are many algorithms and variants of RSA. But, it is steal a burning topic of research. Because the thrust to store data secret is never going to end. In this paper, we have proposed a literature review of some modern variants of the RSA algorithm. All the algorithms have been analyzed. Their merits and demerits are also discussed.

Index Term: Public Key Cryptography, RSA Variant, Data Secrecy.

I. INTRODUCTION

In this age of universal electronic connectivity, the electronic fraud is a matter of concern. There is indeed need to store the information securely. This has led to a heightened awareness to protect data and resources from disclosure, to ensure the authenticity of data and messages, and also to protect systems from network based attacks. Cryptography is the science of encryption. Cryptography plays a central role in mobile phone communications, electronic commerce, sending or receiving private emails, transaction processing, providing security to ATM cards, securing computer from unauthorized access, digital signature and also touches on many aspects of our daily lives. Cryptography consists of all the principles and methods of transforming an intelligible message called plaintext into one that is unintelligible called cipher text and then retransforming that message back to its original form. In modern era, the cryptography is considered to be a branch of both mathematics and computer science. It is also affiliated closely with information & communication theory. Although in the past, the role of cryptography referred only to the encryption and decryption of message using secret keys. But nowadays, the cryptography is used in many areas; it is because of the digitization. It is generally classified into two categories, the symmetric and asymmetric.

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted or scrambled by any encryption algorithm using the key. The user having the access to the same key can decrypt the encrypted data. Such a cryptosystem is known as private key or symmetric key cryptography. There are many standard symmetric key algorithms available. Some popular ones are as:. AES advanced encryption standard, 3DES triple data encryption standard etc. All these standard symmetric algorithms defined are proven to be highly secured and time tested. The main problem related to these algorithms is the key exchange. All the communicating parties require a shared secret key. This key is required to exchange between them to establish a secured communication. Therefore the security of the symmetric key algorithm depends on the security of the secret key. The Key size is typically hundreds of bits in length. The key size also depends on the algorithm used. The key cannot be shared online. Also when a large number of communicating parties are there, then in that case the key exchange is infeasible & very difficult too. All such problems are countered by the public key cryptography. In public key algorithm a shared secret can be established online between communicating parties without any need for exchanging any secret data.

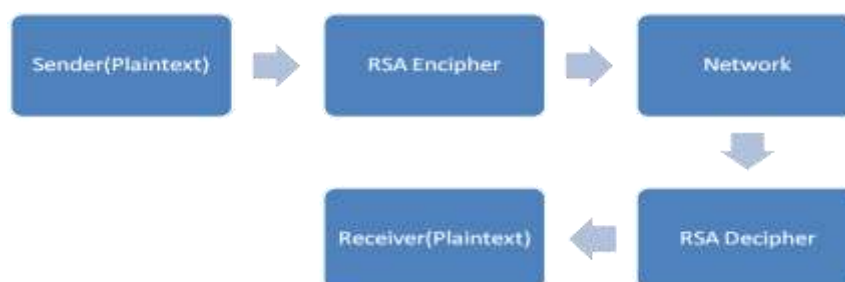


Figure1: RSA Cryptography Process

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted or scrambled by any encryption algorithm using the key. The user having the access to the same key can decrypt the encrypted data. Such a cryptosystem is known as private key or symmetric key cryptography. There are many standard symmetric key algorithms available. Some popular ones are as:. AES advanced encryption standard, 3DES triple data encryption standard etc. All these standard symmetric algorithms defined are proven to be highly secured and time tested. The main problem related to these algorithms is the key exchange. All the communicating parties require a shared secret key. This key is required to exchange between them to establish a secured communication. Therefore the security of the symmetric key algorithm depends on the security of the secret key. The Key size is typically hundreds of bits in length. The key size also depends on the algorithm used. The key cannot be shared online. Also when a large number of communicating parties are there, then in that case the key exchange is infeasible & very difficult too. All such problems are countered by the public key cryptography. In public key algorithm a shared secret can be established online between communicating parties without any need for exchanging any secret data. In the public key or Asymmetric key cryptography sender encrypt the message by using recipient's public key and at the time of decrypt using recipient's private key.

II. CRYPTOGRAPHIC GOALS

“Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack”.

These three concepts form what is often referred to as the CIA triad. The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

A. Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

B. Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

C. Availability

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

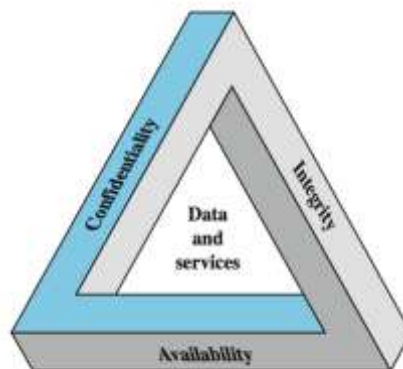


Figure2: Security Goals

D. Algorithms and Keys

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. (Generally, there are two related functions: one for encryption and the other for decryption).

If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a restricted algorithm. Restricted algorithms have historical interest, but are woefully inadequate by today's standards. A large or changing group of users cannot use them, because every time a user leaves the group everyone else must switch to a different algorithm. If someone accidentally reveals the secret, everyone must change their algorithm.

Even more damning, restricted algorithms allow no quality control or standardization. Every group of users must have their own unique algorithm. Such a group can't use off-the-shelf hardware or software products; an eavesdropper can buy the same product and learn the algorithm. They have to write their own algorithms and implementations. If no one in the group is a good cryptographer, then they won't know if they have a secure algorithm. Despite these major drawbacks, restricted algorithms are enormously popular for low-security applications. Users either don't realize or don't care about the security problems inherent in their system.

Modern cryptography solves this problem with a key, denoted by K . This key might be any one of a large number of values. The range of possible values of the key is called the key space. Both the encryption and

decryption operations use this key (i.e., they are dependent on the key and this fact is denoted by the K subscript), so the functions now become:

$$Ek(M) = C$$

$$Dk(C) = M$$

Those functions have the property that:

$$Dk(Ak(M)) = M$$

Some algorithms use a different encryption key and decryption key. That is, the encryption key, K_1 , is different from the corresponding decryption key, K_2 . In this case:

$$Ek_1(M) = C$$

$$Dk_2(C) = M$$

$$Dk_2(Ek_1(M)) = M$$

All of the security in these algorithms is based in the key (or keys); none is based in the details of the algorithm. This means that the algorithm can be published and analyzed. Products using the algorithm can be mass-produced. It doesn't matter if an eavesdropper knows your algorithm; if she doesn't know your particular key, she can't read your messages.

D.1 Symmetric Algorithms

There are two general types of key-based algorithms: symmetric and public-key. Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret.

Encryption and decryption with a symmetric algorithm are denoted by:

$$Ek(M) = C$$

$$Dk(C) = M$$

Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called stream algorithms or stream ciphers. Others operate on the plaintext in groups of bits. The groups of bits are called blocks, and the algorithms are called block algorithms or block ciphers. For modern computer algorithms, a typical block size is 64 bits large enough to preclude analysis and small enough to be workable. (Before computers, algorithms generally operated on plaintext one character at a time. You can think of this as a stream algorithm operating on a stream of characters.)

D.2 Public-Key Algorithms

Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key. The algorithms are called "public-key" because the encryption key can be made public: A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key. The private key is sometimes also called the secret key, but to avoid confusion with symmetric algorithms, that tag won't be used here.

Encryption using public key K is denoted by:

$$Ek(M) = C$$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$$Dk(C) = M$$

Sometimes, messages will be encrypted with the private key and decrypted with the public key; this is used in digital signatures. Despite the possible confusion, these operations are denoted by, respectively:

$$Ek(M) = C$$

$$Dk(C) = M$$

III. LITERATURE SURVEY

Fault-based attacks are the attacks which are capable of recovering secret keys by. The fault based attacks introducing one or more faults in and then analyzes the output. It is a very powerful method to crack the key. The work done by Kun Ma et al in [1] contains a novel Concurrent Error Detection scheme to overcome the problem due to fault-based attack against RSA. This proposed method is based on the concept of the multiplicative homomorphic property. The time overhead of this technique is more.

Alexandra Boldyreva, Hideki Imai proposed another variant of RSA[2]. It is known as RSA-OAEP. It is based on OAEP. OAEP is one of the most popular and well formatted public-key encryption scheme. It was originally designed by Bellare and Rogaway. The OAEP is based on a trapdoor permutation. But the guaranteed level of security is not very high for a practical parameter choice. The authors [2] proposed a very simple modification of the OAEP encryption in which the trapdoor permutation instance is only applied to a part of the OAEP transform. The security is tight in this updated version. OAEP can also be used to encrypt long messages without using hybrid encryption.

The work done in [3] focuses on the problem of how to prevent the fast RSA signature and decryption computation with residue number system speedup from a hardware fault cryptanalysis in a highly reliable and efficient approach. It is a well known fact that the CRT- based speedup for RSA signature has been widely used. But it is a possibility that a hardware fault cryptanalysis can totally break the RSA system by factoring the public modulus. Many solutions exist to counter this problem. But we have observed that very few of these existing solutions are both sound and efficient. Experimental results have shown that the expanded modulus approach proposed by Shamir is superior to the approach of using a simple verification function when other physical cryptanalysis. The proposed work is based on the concepts of fault infective CRT computation and fault infective CRT recombination.

RSA is the asymmetric or public key cryptography system. The security of RSA public key cryptosystem is based on the larger value of modulus. One of the main problems associated to RSA cryptosystem is factorization. The authors [4] proposed a new special purpose algorithm to perform factorization. This algorithm is compared with trial division algorithm TDM. The experimental results prove that the proposed algorithms runtime depends on the difference of factors and is independent of size of the modulus. So it is more effective whenever factors are close to each other & in that particular case it outperforms the TDM.

The authors of [5] proposed an enhance algorithm for the RSA cryptosystem. This new proposed cryptosystem uses a third prime number in calculating the value of n . This additional third prime number increases the factor complexity of n . It will provide more security to the RSA.

The public key cryptosystem RSA is the first and most popular cryptosystem for performing encryption and decryption of data, to keep data secret, to transfer data from one location to another. Also it is known that the security of RSA depends on large factorization. If the factorization is possible then the whole algorithm can become breakable. Authors [6] proposed a new methodology to change the original modulus with the fake modulus. Therefore if the hacker factorizes this new modulus value then he will not be able to locate the original decryption key.

Giraud [7] proposed a new countermeasure scheme based on the concept of Montgomery Ladder Exponentiation. The proposed algorithm performs two modular multiplications for each bit of exponent. Whereas the square and multiply algorithm which performs on average 1.5 modular multiplications per bit of the exponent. Therefore the proposed method is faster.

IV. COMMON PROBLEMS IN EXISTING RSA

- [1] The main disadvantage of RSA decryption its slow speed.
- [2] Not secure against the Weiner's attack.
- [3] Problem arise to common modulus attack.
- [4] known plaintext attack are possible.
- [5] Another attack are Low decryption exponent attack.

V. CONCLUSION

In this paper, the introduction & the application of cryptography is given. The problems related to private keys are discussed. The public key cryptography & its utility in so many areas of the life are discussed. The modern variants of the RSA cryptosystem are discussed with their merits and demerits. With this analysis find out the possible type of attack are possible in RSA Cryptography system.

REFERENCES

- [1] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE, "Homomorphic Property-Based Concurrent Error Detection of RSA:A Countermeasure to Fault Attack", IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 7, JULY 2012.
- [2] Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE, and Kazukuni Kobara, "How to Strengthen the Security of RSA-OAEP", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 11, NOVEMBER 2010.
- [3] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon, "RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis" IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 4, APRIL 2003.
- [4] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", Second International Conference on Advance Computing and Communication Technologies, IEEE 2012.
- [5] Prof. Dr. Alaa Hussein Al-Hamami, Ibrahim Abdallah Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm" International conference on Advance Computing & Communication Technologies, IEEE 2012.
- [6] "Enhancing Security Features in RSA Cryptosystem", 2012 IEEE SYMPOSIUM ON COMPUTERS & INFORMATICS, PP.214-217, 2012.
- [7] Giraud, " An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis", IEEE Trans. Computer, VOL. 55, NO. 9, PP. 1116-1120, SEPTEMBER. 2006.