Multipair Public Key Cryptosystem

[*1] M. Sreedevi, [*2] Prof. M. Padmavathamma

[1] Asst.professor, Dept. Of Computer Science, S.V.University, TIRUPATI, A.P, India.
[2]HOD, Dept. Of Computer Science, S.V.University, TIRUPATI, Andhra Pradesh, India.

***Abstract* — Cryptography mainly deals with security provided to the data access the network. Asymmetric key cryptography, also called as Public Key cryptography, uses two different keys (which forms a key pair),one key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message – not even the original (i.e. the first) key used for encryption. Many cryptosystems has been proposed with modifications to original RSA by improving security, performance of various phases of algorithm. this paper we propose multiple public keys to provide hierarchy implementation of encryption and decryption phases when compare to RSA Batch-RSA, Multi- Prime RSA, Rebalanced – RSA – Analysis.**

***Keywords*— Cryptography, RSA, Batch-RSA, Multi- Prime RSA, Rebalanced – RSA – Analysis**

1. Introduction

Present days, security is required to transmit confidential information over the network. Security is also required in a wide range of applications. Internet is frequently used to upload web pages and other documents from a private development machine to public webhosting servers. Transfer of files from one place to another place, like banking, e-transactions, e-shopping, e-business, and tenders etc. need special authenticated mechanism. As a communications and transmission of files over internet Present days, security is required to transmit confidential information over the network. Security is also required in a wide range of applications. Internet is frequently used to upload web pages and other documents from a private development machine to public webhosting servers. Transfer of files from one place to another place, like banking, e-transactions, e-shopping, e-business, tenders etc 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 file transfer. Most recommended solutions to secure communication is cryptography. Cryptography is an act of writing in code or cipher. Information that can be read and understood without any special measures is called plaintext or clear text. The method of concealing plaintext in such a way as to conceal its substance is called encryption. Encrypting plain text outcomes in unreadable hideous form called cipher text. Cryptography plays a gorgeous role in providing the data security against malicious encroach. It is the art of protecting the information by transforming it into an unreadable format in which a message can be invisible from the casual reader and only the witting recipient will be able to change it into original text. Communication is cryptography. Cryptography is an act of writing in code or cipher. Information that can be read and understood without any special measures is called plaintext or clear text. The method of concealing plaintext in such a way as to conceal its substance is called encryption. Encrypting plain text outcomes in unreadable hideous form called cipher text. Cryptography plays a gorgeous role in providing the data security against malicious encroach. It is the art of protecting the information by transforming it into an unreadable format in which a message can be invisible from the casual reader and only the witting recipient will be able to change it into original text.

1.1. Cryptography

In olden days cryptography called symmetric key cryptography involved only one key used by both sender and receiver for transforming the information. So single key must be maintained in secret was problem unable to solve. Next emerged public key cryptography involving two separate keys, one is public key and other secret linked by mathematical relations.

1.2 The purpose of cryptography

Cryptography is the science of using mathematics to encrypt and decrypt concealed code and is an age-old art. some proficients argue that cryptography come out spontaneously sometime after writing was excogitate, with applications ranging from diplomatic letters to war-time disputation plans. In data and telecommunications, Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient, With in the context of any application-to-application communication, there are some specific security requisite, including:

- *Authentication:* The process of proving one's individuality. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, pair of which are frankly weak.)
- *Concealment/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Absoluteness:* securing the receiver that the received message has not been varied in any way from the original.

- *Non-rejecting:* A mechanism to prove that the sender really sent this message.

Cryptography then, not only protects information from theft or modification, but can also be utilized for user authentication.

1.2 Categories of Cryptography

There are two kinds of cryptographic algorithm to accomplish these goals: symmetric cryptography, asymmetric cryptography.

1.2.1 Symmetric Key Cryptography

In symmetric cryptography only one key is used for encryption and decryption. In symmetric-key (traditional) cryptography, both of the sender and receiver of a substance know and utilize the same secret key. The main challenge is attainment the sender and receiver to agree on the secret key without anybody else finding out. If they are in another physical positions, they must hope a courier, a phone system, or some other transmission medium to check the disclosure of the secret key. Anyone who hears or tap the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. hence all keys in a secret-key (symmetric-key) cryptosystem compulsory stay secure, secret-key cryptography frequently has trouble providing secure key management. Some of the currently used cryptographic technologies in symmetric key cryptography are DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, RC5 (Rivest Cipher 5), AES (Advanced Encryption Standard) etc.

1.2.2 Asymmetric Key Cryptography

To work out the key management problem, Whitfield Diffie and Martin Hellman bring in the concept of public-key cryptography (asymmetric). In asymmetric algorithm distinct keys are used to encrypt and decrypt the data. Cryptographic system needs two separate keys, one of which is secret and one of which is public. While varied, the two parts of the key pair are mathematically linked. (the ones being the integer factorization and discrete logarithm problems).while it is easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one (or more) secret keys between the sender and receiver. In practice, only a hash of the message is typically encrypted for Signature verification purposes. Public-key cryptography is a fundamental, important, and widely used technology. It is an approach used by many cryptographic algorithms and cryptosystems.

2. Literature survey

The threats to data security, from malicious attacks, viruses, spyware, and phishing to bullying, scams, and identity theft, create a feeling of vulnerability. Some of these threats are aimed directly at individuals, whereas many more target organizations with which those individuals do business. To encounter these threats and provide greater confidence, there should be a sound security technique which is resilient to above mentioned attacks which we are discussed in sections below.

The basic RSA cryptosystem has two public quantities referred to as n (modulus) and e (public key), as well as private quantities d (private key) and $\emptyset(n)$. $\emptyset(n)$ is defined as the Least Common Multiple (LCM) of all the prime factors of n. The secret exponent d is chosen as an integer smaller than $\emptyset(n)$ and relatively prime to $\emptyset(n)$. The public key e is the "multiplicative inverse" of d and can be calculated as $d = e^{-1} \bmod \lambda(n)$ .There are two processes in the RSA cryptosystem, one is encryption/decryption and the other is signing/signature-verification process. Before the message is encrypted or signed, it is split into several blocks m_1 , $m_2, \cdots m_j$ ($m_k < n$ for $k \in [1, j]$) with the same word length in the case it has larger word length than the modulus n. However, in this thesis, the message m is assumed to have smaller word length than the modulus n. During the encryption/decryption process, the public key e is used to encrypt the message $m$as $c = m^e \bmod n$, and the secret key d is used to recover the message m from the encrypted information c as $m = c^d \bmod n$. In the signing/signature-verification process, the secret key d is used to obtain the signature s from the message m by using public key document is verified.

3. Comparison Algorithms

3.1 Batch RSA

Batch RSA is one of the first variant of RSA, which increases the speed of decryption process and also guarantees the security of the Batch RSA Cryptosystem. Fiat [14] observed that, when using small public exponents e1 and e2, it is possible to decrypt two cipher text for approximately the price of one. Suppose C1 is a cipher text obtained by encrypting some M1 using the public key (N, 3), and C2 is a Cipher text for some M2 using (N, 5). To decrypt, we must compute $C1^{1/3}$ and $C2^{1/5}$ mod N. Fiat observed that by setting A = $(C1^5 \cdot C2^3)^{1/15}$. At the cost of computing a single 15th root and some additional arithmetic, we are able to decrypt both C1

and C2. Computing a 15th root takes the same time as a single RSA decryption. This batching technique is only advisable when the public exponents e1 and e2 are small(e.g., 3 and 5). Otherwise, the extra arithmetic required is too expensive. Also, one can only batch-decrypt cipher-texts encrypted using the same modulus and distinct public exponents. The algorithm for Bach RSA has three phases: Key generation, Encryption, Decryption[18].

3.2 Rebalanced RSA

In standard RSA, encryption and signature verification are much less processor-intensive than decryption and signature generation. In some applications, one would like to have the reverse behavior. For example, when a cell phone needs to generate an RSA signature that will be later verified on a server one would like signing to be easier than verifying. Similarly, for SSL, web browsers (doing encryption) typically have idled cycles to burn whereas web servers (doing decryption) are overloaded. In this section we describe a variant of RSA that enables us to rebalance the difficulty of encryption and decryption. It is based on a proposal by Wiener [12]. Note that we cannot simply speed up RSA decryption by using a small value of d since as soon as d is less than N0.292 RSA is insecure [12] The key generation, encryption, and decryption.

3.3 Multi-prime RSA

Generally, the software implementations of RSA algorithm are based on 2-prime RSA. Mprime RSA was introduced by Collins et al. [3], who modified the RSA modulus so that it consists of k primes (N = p1*p2*…pk) instead of the traditional two primes p and q. the multi-prime RSA speed up the RSA implementations. Both 2-prime and multi-prime implementations require squaring reduction and multiplication reduction of multi-precision integers [3]. Multi-prime RSA decrypts the data four times faster than the classic RSA. But multi secrete keys algorithms are may be possible to break able keys. The multi-prime RSA-CRT fundamentally employs RSA algorithm with more than two prime numbers. The algorithm is described below:

Key Generation

The steps included in the key generation operation of multi-prime RSA are illustrated as: i. Select three large prime p, q and r at random, each of which is n/3-bit in length. ii. Set N = p x q x r and φ (N) = (p−1) x (q−1) x (r−1) iii. Randomly pick an odd integer e such that gcd (e, φ (N)) = 1, example, e = 216+1 = 65537 iv. After that compute d = e−1 mod φ (N) v. Finally, calculate dp = d mod (p − 1), dq = d mod (q − 1) and dr= d mod (r − 1) vi. The public key would be (e, N) and the private key would be (dp, dq, dr, p, q, r).

Encryption

For a given plain text m which belongs to ZN the encryption algorithm is the same as that of the original RSA:
$c = m^e \bmod N$.

Decryption

In order to decrypt a cipher-text c: i. The decipher first computes $m1 = cp^{dp} \bmod p$, $m2 = cq^{dq} \bmod q$, and $m3 = cr^{dr} \bmod r$ where $cp = c \bmod p$, $cq = c \bmod q$ and $cr = c \bmod r$ ii. Next, using CRT m can be obtained as $m = cd \bmod N$ (q x r) -1 mod p, (p x r) -1 mod q and (p x q) -1 mod r can be pre-calculated in order to increase its efficiency.

4. Proposed Algorithm

Multiple Public-Keys-Algorithm

In this algorithm instead of generating a single public key we have generated pairs of public keys and a single private key. The working of algorithm like key generation phase, decryption phase and encryption phase is given below.

4.1 Key Generation Process:

i. Select p,q, r *and* s where $p \neq q \neq r \neq s$ and

both p, q, r, s are prime numbers.

ii. Determine $n = p$ x q x r x s

iii. Compute $\varphi(n) = (p\text{-}1)$ x (q-1) x (r-1) x (s-1)

iv. Choose an integer e such that

gcd ($\varphi(n)$, e) = 1 and $1 < e < \varphi(n)$

v. Evaluate d as $d \equiv e^{-1} \pmod{\varphi(n)}$

Vi. Calculate the ed = e x d and Eued = ed

Repeat the steps 1,2,3,4 until find the e1,e2,e3,e4

1. Eued = Eu.add(Eued);
2. g = Eued.mod(Eu);
3. if (g.intValue() == 1) {

eval=Eued.mod(d);

4. if(eval.intValue()==0)

{

E[j]=Eued.divide(d);// Alternatives for e, that is e1,e2,e3,e4

}

End loop

Step 1: Compute M1=Cr^1 mod p & M2 =Cr^2 mod q.

Step 2: Using the CRT compute an M €Z_N such that M = M1 mod p and M = M2 mod q.

Note that M = C^d mod N. Hence, the resulting M is a proper decryption of C.

Vii. Public Key (PU) = {*e1, e2, e3, e4, n*}

Viii. Private Key (PR) = {*d, n*}

4.2 Encryption Phase

The steps for encryption of message in order to get the cipher-text are explained below :

i. Obtain a plain text M such that M <*n*.

ii. Compute the cipher text as C = M^e mod *n* *//where e is any one of the public keys (e1, e2, e3, e4)*

4.3 Decryption Phase

The steps for decryption of cipher-text in order to get the original message are explained below:

i. Get the cipher text C.

ii. Calculate the plain text as M = C^dmod *n*

5. Experimental results for Proposed Algorithm

Key Generation Phase starts….

n:..210
Eu:..48

e:7

d:7

Key pairs

(e1,e2,d):55,103,7

(e3,e4,d):151,199,7

enter your text:

sri venkateswara university

Encryption Phase starts...

Enter Your public Key...

103

Encrypted Text:
1151141051582021011102313116101115119131141315833 1

10105202101114115105116121

Decryption Phase starts...

Enter Your private Key... 7

Decrypted string:

sri venkateswara university

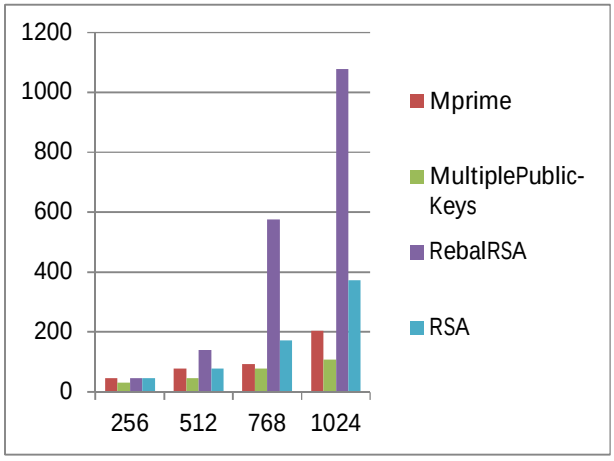
6. Analysis of Proposed Algorithm

In this section we have given analysis of public key pair algorithm and the other variants of RSA by taking various sizes of ‘n’ value.

6.1 Analysis of Key generation Phase

TABLE I

Key Generation Time				
Bits(n)	Mprime	Multiple Public-Keys	RebalRSA	RSA
256	47	31	47	47
512	78	47	140	78
768	94	78	577	172
1024	203	109	1077	374

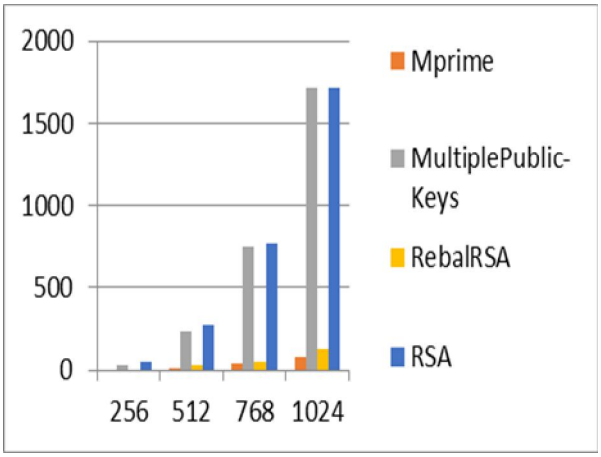


Key Generation Phase

6.2 Analysis of Encryption Phase

TABLE 2

Encryption Time				
Bits (n)	**Mprime**	**Multiple Public-Keys**	**RebalRSA**	**RSA**
256	15	62	46	0
512	15	265	250	15
768	16	765	749	31
1024	32	1716	1716	31

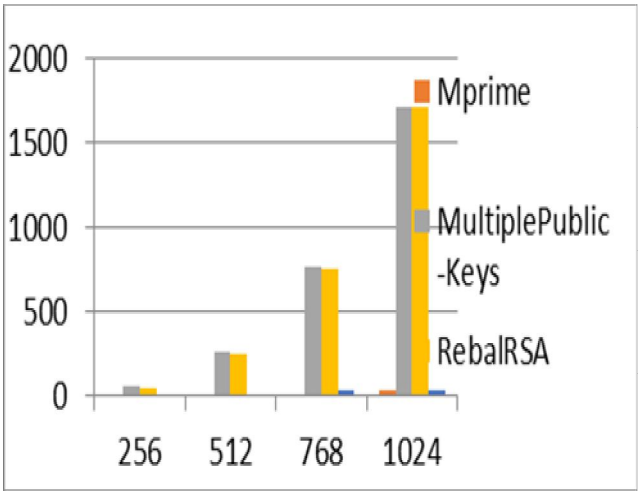


Encryption Phase

6.3 Analysis of Decryption phase

TABLE 3

Decryption Process Time				
Bits (n)	**Mprime**	**MultiplePublic-Keys**	**RebalRSA**	**RSA**
256	0	32	0	47
512	16	234	31	265
768	38	749	47	764
1024	80	1711	124	1716



Decryption Phase

7. Conclusion:

In this paper we have studied about RSA and its variants designed to speed up RSA encryption, decryption and various deficiencies of standard RSA and reduce the storage space for keys. Batch RSA is fully backwards-compatible, but requires the decrypter to obtain and manage multiple public keys and certificates. The multi-prime RSA techniques are promising in that speedup the RSA decryption process along with hierarchy advantage. The rebalanced RSA method gives a large speedup in decryption process and takes less memory than the standard RSA and multi-prime RSA, but it encryption process takes more time than the other two algorithms. After above analysis and study we have proposed a new Multi-Pair public key cryptosystem which produces multiple pairs of Public keys and single Private key for better security from data threats. All these techniques are orthogonal to work in improving the performance of the fundamental number-theoretic algorithms (e.g., modular multiplication and exponentiation) on which RSA is built. Finally in this paper we have given results and analysis of Multi-Pair public key cryptosystem along with RSA and its variants.

References

[1] *Dan Boneh.* "Fast variants of RSA"

[2] Behrouz A. Forouzan,―Data Communications and Networking‖, Tata McGraw Hill Education Private Limited, 4th Edition.

[3] Cesar Alison MonteiroPaix~ao?. ―An efficient variant of the RSA cryptosystem

[4]Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek. ‖ Dual RSA and Its Security Analysis‖

[5] *Dan Boneh.* "Twenty Years of Attacks on the RSA Cryptosystem

[6] Satyendra NathMandal ,Kumarjit Banerjee Modified Trail division for Implementation of RSA Algorithm with Large Integers‖.

[7] D. Chaum, ―Untraceable electronic mail, return address and digital pseudonyms,‖ *Commun. ACM*, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[8] Sun H.-M. and C.-T. Yang, ―RSA with balanced short exponents and its application to entity authentication in Public Key Cryptology‖, Springer, NewYork, 2005, pp. 199–215.

[9] Sun H.-M. and Wu M.-E., ―An approach towards Rebalanced RSA-CRT with short public exponent Cryptology‖.

[10] Anand Krishnamutrhy and et.al ―an efficient implementation of multi-prime rsa on dsp processor‖

[11] Enterprise Solutions ―Cryptography using Compaq MultiPrime technology in parallel processing environment‖.

[12] M. Wiener. ―Cryptanalysis of Short RSA Secret Exponents.‖ IEEE Trans. Information Theory 36(3):553–558. May 1990.

[13] Stallings William, ―Cryptography and Network Security - Principles and Practices‖ India : Pearson Prentice Hall, 4th Edition.

[14] A. Fiat. ―Batch RSA.‖ In G. Brassard, ed., Proceedings of Crypto 1989, vol. 435 of LNCS, pp. 175–185. Springer-Verlag, Aug. 1989.

[15] Dictionary of terms, Help Desk for Digital Ids, Soltrus Inc., Available:

www.soltrus.com/english/digitalidhelpcentre/digitalid_about_dictionary.html.

[16]wordiQ.com, "History of cryptography," Available: http://www.wordiq.com/definition/History _of_cryptography.

[17]A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of applied cryptography, *CRC press*, 1996.

[18] Suresh K,Venkataramana.K, "*Study of Analysis on RSA and its Variants*",International Journal of Computer Science Research & Technology (IJCSR),Vol. 1 Issue 4, September - 2013