ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

A Modified RSA Encryption Technique Based on Multiple public keys

Amare Anagaw Ayele[1] Dr. Vuda Sreenivasarao[2]

M.Sc. (Computer Science), School of Computing and Electrical Engineering, IOT, Bahir Dar University, Ethiopia[1]

Professor, School of Computing and Electrical Engineering, IOT, Bahir Dar University, Ethiopia, India[2]

ABSTRACT: In the today's world, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks.RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & 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. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. In this paper, we have done an efficient implementation of RSA algorithm using two public key pairs and using some mathematical logic rather than sending the e value directly as a public key.Because if an attacker has opportunity of getting the e value they can directly find d value and decrypt the message.

Keywords: Cryptography, RSA, Key, Symmetric Key and Asymmetric Key.

I. INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web . By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. In traditional (symmetric-key) cryptography, the sender and receiver of a message know and use the same secret key.The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. Because all keys in a secret-key (symmetric-key) cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management.To solve the key management problem, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked.

The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integer factorization and discrete logarithm problems).Although 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.

Examples of well-regarded asymmetric key techniques for varied purposes include: Diffie–Hellman key exchange protocol, El Gamal, DSS (Digital Signature Standard), which incorporates the Digital Signature Algorithm, Various elliptic curve techniques, Various password-authenticated key agreement techniques, RSA encryption algorithm, Cramer–Shoup cryptosystem, YAK authenticated key agreement protocol. Among all RSA is most popular one.

The proposed algorithm is similar with RSA with some modification. Proposed algorithm is also a public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors (similar to RSA)

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

.In addition of this we have used two public pair of keys. This modification increases the security of the cryptosystem. So its name is LEE public key algorithm.

II. CRYPTOGRAPHY AND TYPES

Cryptography uses the process of transposition and substitution of the characters to hide and retrieve the data. At the sender side we call it Encryption shown in Figure.1 and at the receiver side we called it decryption shown in Figure.2.We use the various keys to encrypt a decrypt the data. Keys are the special digital functions or methods that convert the plain text into inscribe format and it's vice versa. Every element of the network have two keys namely private or personal key which is known to a particular person and public key which is known by all persons in the network. There are two types of cryptography.

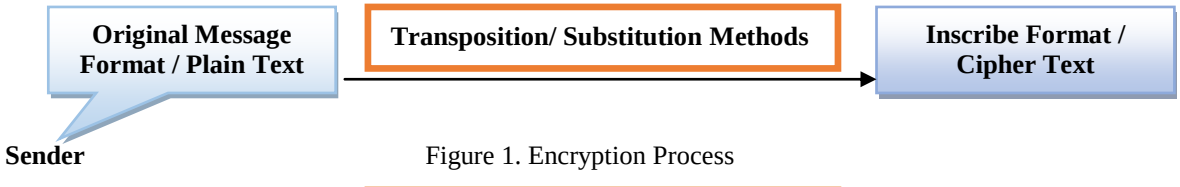

Figure 1. Encryption Process

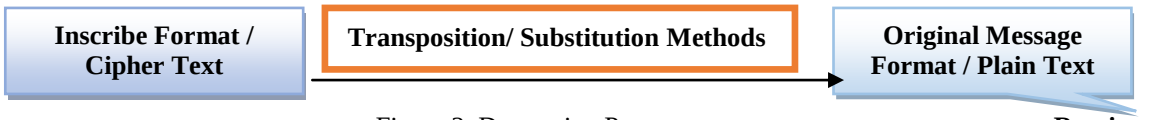

Figure 2. Decryption Process

A. Same key cryptography or Private Key cryptography:

In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recover the plaintext from cipher text and vice versa, so this type of cryptography is also known as symmetric encryption and decryption. Figure.3 is showing the whole process of encryption and decryption which is carried out through receiver's private key. Through this cryptography form, it is obvious that the secret key must be known to both the sender and the receiver that why it is known as private key cryptography. Transmitting the secret key on insecure network can also destroy the security.

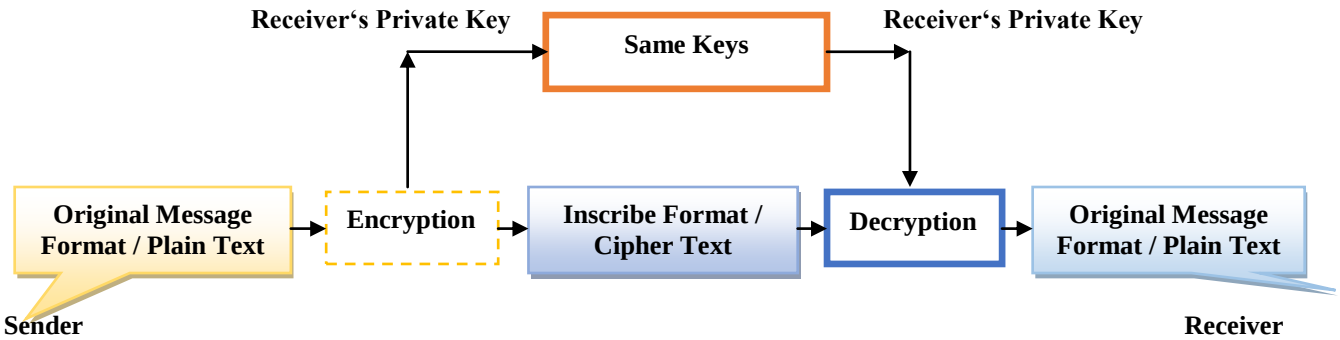

Figure3.Same key cryptography

B. Different key cryptography or public key cryptography:

In this type of cryptography, the receiver and sender apply the Different keys to encrypt and decrypt the message or recover the plaintext from cipher text and it's vice versa. This type of cryptography is also known as asymmetric encryption and decryption.Figure.4 is showing the whole process where receiver's public key is used for encryption and receiver's private key is used for decryption. In public key cryptography, each user or the workstation take part in the communication have a pair of keys, a public key and a private key and a set of operations associated with the keys to do the cryptographic operations. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

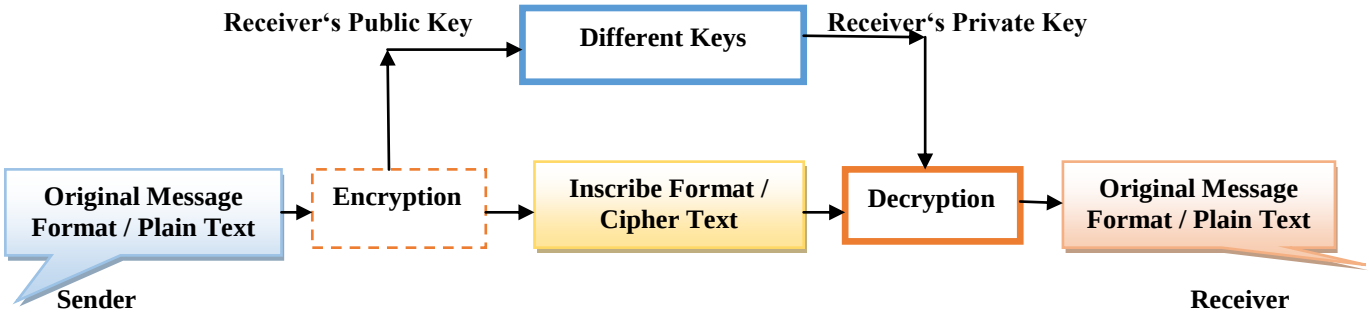

Figure4. Different key cryptography

C VIII. THE RSA ALGORITHM AND ITS MATHEMATICAL FOUNDATION

A. The Mathematical Foundation for RSA Algorithm:
The RSA digital signature has precise mathematical foundations, which are as follows [1]:
Theorem 1: (fundamental theorem of mathematics) any positive integer *a* can be denoted as ai=P1.....Pn, which $P1 > P2 > P3 \ldots > PT$ are all prime numbers, $a_i > 0$.
Theorem 2: (Euclid theorem) Any two integers a and b has a greatest common factor d, in which d can be expressed as the linear combination of a and b with integer coefficient, namely $s, t \in Z$, which satisfies $d = sa + tb$.
Theorem 3: (Fermat theorem) If *p* is a prime number, then for any positive integer a that prime to *p*, $a^{(p-1)} \equiv 1 \pmod p$.
Definition 1 (Euler function (*n*)) When $n = 1$, $\phi(1) = 1$, when $n > 1$, the value of $\phi(n)$ is the amount of positive integer that less than *n* and prime to *n*.
Theorem 4: If *p* and *q* are all prime numbers and $p \neq q$, then $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.
Theorem 5: (Euler theorem) If integer *a* is co prime to integer n, then $a^{\phi(n)} \equiv \pmod m$.
Above theorem have the following 3 deductions:
(1) If p is prime number and $n = p$, then $a^{(p-1)} \equiv 1 \pmod p$, namely the Fermat theorem.
(2) $a^{\phi(n+1)} \equiv a \pmod p$.
(3) If $n = pq$, *p* and *q* are prime numbers and $p \neq q$, for $0<m<n$, if $(m, n) = 1$, then $m^{\phi(n)+1} \equiv m \pmod n$, namely $m^{(p-1)(q-1)+1} \equiv \pmod n$.
Above five theorems will be used in the feasibility proof of RSA digital signature algorithm in the following section.
Theorem 6: If *p* and *q* are prime numbers and $p \neq q$, $rm \equiv 1 \pmod{(p-1)(q-1)}$, *a* is any positive integer, $b \equiv am \bmod pq$, $c \equiv br \bmod pq$, then $c \equiv a \bmod pq$.
B. RSA Key Generation Algorithm:
1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1)(q-1) [Theorem 4].
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1. [Theorem 2].
4. Compute the secret exponent *d*, 1 < d < phi, such that $ed \equiv 1 \pmod{phi}$. [Theorem 6].
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

C. Encryption Algorithm:
Sender A does the following:-
1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer *m*
3. Computes the cipher text c = me mod n.
4. Sends the cipher text *c* to B.

D. Decryption Algorithm:
Recipient B does the following:-
1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative *m*.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. The RSA scheme has become the most widely accepted and implemented approach to public-key encryption. RSA is named after its inventors Rivest, Shamir, and Adleman.RSA is a block cipher in which the plaintext and cipher text are integers between 0 and *n*- 1 for some *n*.Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the values of *n* and *e*, and only the receiver knows the value of *d*. This is a public-key encryption algorithm with a public key of *KU = {e,n}* and a private key of *KR = {d,n}*.For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of *e, d, n* such that $M^{ed} = M \bmod n$ for all M<*n*.
2. It is relatively easy to calculate M^e and C^d for all values of M <*n*.

Steps:

- Begin by selecting two prime numbers, *p* and *q*, and calculating their product *n*, which is the modulus for encryption and decryption.
- Next, we need the quantity *φ(n) re*ferred to as the Euler totient of *n*, which is the number of positive integers less than *n* and relatively prime to *n*.
- Then select an integer *e* that is relatively prime to *φ(n) (i*.e., the greatest common divisor of *e* and *φ(n)* is 1].
- Finally, calculate *d* as the multiplicative inverse of *e*, modulo *φ(n).*
- Itcan be shown that *d* and *e* have the desired properties.
- Suppose that user A has published its public key and that user B wishes to send the message *M* to A.
- Then B calculates $C = M^e \pmod n$ and transmits C.
- On receipt of this cipher text, user A decrypts by calculating $M = C^d \pmod n$.

IV. PROPOSED RSA ALGORITHM

RSA is a block cipher in which the plaintext and cipher text are integers between 0 and *n*- 1 for some *n*.Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$C = M^{b/a} \bmod n$

$M = C^d \bmod n = (M^{b/a})^d \bmod n = M^{b/ad} \bmod n$

Both sender and receiver must know the values of *n, b and a* only the receiver knows the value of *d*. This is a public-key encryption algorithm with a public key of *KU = {b,n},{a}*and a private key of *KR = {d,n}*.For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of *b, a, d, n* such that $M^{b/ad} = M \bmod n$ for all M<*n*.
2. It is relatively easy to calculate $M^{b/a}$ and C^d for all values of M <*n*.
3. b is a multiple of a and e (which the public key in the normal RSA algorithm)

Steps:

- Begin by selecting two prime numbers, *p* and *q*, and calculating their product *n*, which is the modulus for encryption and decryption.
- Next, we need the quantity *φ(n) re*ferred to as the Euler totient of *n*, which is the number of positive integers less than *n* and relatively prime to *n*.
- Then select an integer *e* that is relatively prime to *φ(n) (i*.e., the greatest common divisor of *e* and *φ(n)* is 1).
- Select two numbers a and b such that b=ae
- Using this numbers formulate two public key {b,n},{a}
- Finally, calculate *d* as the multiplicative inverse of *e(which is public key in normal RSA),* modulo *φ(n). but to calculate it let the receiver choose any positive natural number and multiply it with a then add b, divide the result by a and finally subtract the chosen value then the receiver has e. then calculate d as usual.*
- Itcan be shown that *d* and *e* have the desired properties.
- Suppose that user A has published its public key and that user B wishes to send the message *M* to A.
- Then B calculates $C = M^{b/a} \pmod n$ and transmits C.
- On receipt of this cipher text, user A decrypts by calculating $M = C^d \pmod n$.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

Key generation	
Select p, q	p and q both prime, p! =q
Calculate n=p*q	
Calculate phi= (p-1) (q-1)	
Encryption	
Plaintext:	M<n
Decryption	
Cipher text	C
Plaintext	$M = C^d \bmod n = (M^{b/a})^d \bmod n$

RSA	Modified RSA
Use only one public key	Use two public key
Less communication overload	High communication overload
More vulnerable to brute force attack	Less vulnerable to brute force attack
Less secure	More secure
The Public key is sent once	The Public key is sent separately twice

VI. CONCLUSION

In this paper an algorithm is proposed for RSA a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation.This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security. but with less speed.

REFERENCES

[1] Maheswari Losetti, Kanaka Raju Gariga "An Enhanced Rsa Algorithm for Low Computational Devices" International Journal of Advanced Research and Innovations Vol.1, Issue .2, pp 114-118.
[2] Kuldeep Singh, Rajesh Verma, Ritika Chehal "Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012, pp 204-206.
[3] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, pp 134-138.
[4] MJ Wiener. (1990), "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, Vol 36, No 3, pp 553-558.
[5] R Gennaro. (2000), "RSA-Based Undeniable Signatures", Journal of Cryptology, Vol 13, No. 4, pp 397-416.
[6] R Cramer, V Shoup. (2008), "Signature schemes based on the strong RSA assumption", ACM Transactions on Information and System Security, Vol 3, No 3, pp 161-185.
[7] Gennaro. (2008), "Robust and Efficient Sharing of RSA Functions", Journal of Cryptology, Vol 13, No 2, pp 273-300.
[8] D Boneh, M Franklin. (2001), "Efficient generation of shared RSA keys", Journal of the ACM, Vol 48, No. 4, pp 702-722.
[9] Rivest, R.; A. Shamir; L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 (2): 120–126, doi: 10.1145/359340.359342, 1977.
[10] B. Schneier, Applied cryptography, second edition, NY: John Wiley & Sons, Inc., 1996.
[11] William Stallings, Cryptography and Network Security, Pearson Education, Fourth Edition.
[12] Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publishing Company Limited.
[13] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.
[14] Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar "Reverse Encryption Algorithm: A Technique for Encryption & Decryption" International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013,pp 90-95.
[15] Gagandeep shahi, Charanjit singh "Cryptography and its two Implementation Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013,PP 668-672.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2013

BIOGRAPHY

Amare Anagaw Ayele received his B.Sc. Degree in Computer Science from Gondar University in 2008.Currently perusing M.Sc. in Computer Science, School of Computing and Electrical Engineering, IOT, Bahir DarUniversity, Ethiopia. His main research interest is Network Security, Data Mining and Algorithms. He is a member of professional society like SDIWC.

Dr. Vuda Sreenivasarao received his M.Tech degree in computer science and engineering from Sathyabama University from 2007.He received PhD degree in computer science and engineering from Singhania University, Rajasthan, India from 2010. Currently working as Professor in School of Computing and Electrical Engineering, IOT, Bahir Dar University, Ethiopia. His main research interests are Data mining, Fuzzy logic, Mobile communication and Network Security. He has got 13 years of teaching experience. He has published 27 research papers in various international journals and one Springer international conference paper. He hasEditorial Board / Reviewers memberships in various international journals. He is a life member of various professional societies like IEEE, ACM, MAIRCC, MCSI, SMIACSIT, MIAENG, MCSTA, MAPSMS, MSDIWC, SMSCIEI and MISTE.