IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

THRESHOLD Φ $(n)^{2-}$ Φ(N)-RSA ALGORITHM

S.Venkateswarlu*, **Dr.R.Seshadri**
S.V.University Computer Centre,S.V.University, Tirupati-517502, A.P,
svenkat@svuniv.in, ravalaseshadri@gmail.com

ABSTRACT

Today Computers are used in various data processing applications ranging from ordinary to sensitive. These Applications should ensure security to customers who perform online payments through e-commerce and companies share confidential documents between them. The solution is by Cryptography which provides security to the data such as by 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. In this paper we propose Threshold| φ(n)2 – φ(N)-RSA Algorithm to provide hierarchy implementation of encryption and decryption phases which has better performance than RSA and its variants like Batch-RSA, Multi- Prime RSA, Rebalanced – RSA.

KEYWORDS: *Cryptography, RSA - Totient function- Batch-RSA, Multi- Prime RSA, Rebalanced – RSA – Analysis.*

INTRODUCTION

In the present Smart world Information technology plays a major role in transforming society but at the same time more problems has to be countered among them security plays key role. Security is required to transmit confidential information over the network and in wide range of web applications. Various application on Internet includes upload web pages and other documents from a private development machine to public web hosting servers , transfer of files from one place to another place, like banking, e-transactions, e-shopping, e-business, and tenders etc. need special security mechanism. From mid-1970's cryptographic techniques are used in securing data online and offline. 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.

A cryptosystem is pair of algorithms that take a key and convert plaintext to cipher text and back. It encompass key generation, Encryption and decryption phases. Encryption phase is the standard means of rendering a communication private. The sender enciphers each message before transmitting it to the receiver. The receiver (but no unauthorized person) knows the appropriate deciphering function to apply to the received message to obtain the original message. An eaves dropper who hears the transmitted message hears only garbage" (the cipher text) which makes no sense to him since he does not know how to decrypt it [9].

CRYPTOGRAPHY

Earlier days various security techniques are used which has not given confidence in securing data as cryptography. Cryptography is the science of using mathematics to encrypt and decrypt secret code and is an age-old art. some proficient 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, within 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-repudiation: A mechanism to prove that the sender really sent this message.

Categories of Cryptography

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

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 [9].

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.

Most popularly used Asymmetric cryptosystem is RSA [1] , its difficulty lies in computing eth roots modulo N, where N is the product of two large unknown primes, and believed to be secure for large enough N. The security of RSA is based on the difficulty of factoring problem. So, the prime factors of modulus of RSA algorithm must be strong primes. Currently, it is suggested that the bit length of N should be large [10] at least 1024 for RSA to be considered secure. So implementing RSA signature scheme in a traditional manner can be time consuming in a resource constrained environment. So we propose an efficient Cryptosystem for encryption and decryption with difference totient function.

LITERATURE SURVEY

The developments to the public key cryptography was seen in 1976 when Diffie-Hellman [2] published their well-known paper entitled new direction in cryptography. This paper has suggested a great concept for public key cryptography and to build a scheme without a secure communication, but able to provide a secret communication. However, Diffie-Hellman suggested such technique for distributing the private key to be employed in the classical schemes in insecure communication channel [3]. In 1978 Rivest,Shamir and Adleman (RSA) [4] introduced the first applied scheme which is the most popular public key scheme..In 1985, Elgamal proposed a public key cryptosystem and digital signature scheme based on discrete logarithms. As to our best knowledge, this cryptosystem is still security under discrete logarithm. But if any k is used twice in the signing, then the system of equations is uniquely determined and x can be recovered. So for the system to be secure, any value of k should never be used twice as the note 2 in [5]. based on the above facts we proposed this new threshold $\varphi(n)^2 - \varphi(N)$-RSA algorithm.

COMPARISON ALGORITHMS

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 [8] 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 C_1 is a cipher text obtained by encrypting some M_1 using the public key (N, 3), and C_2 is a Cipher text for some M_2 using (N, 5). To decrypt, we must compute C11/3 and C21/5 mod N. Fiat observed that by setting A = (C15 •C23)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.

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 [7]. Note that we cannot simply speed up RSA decryption by using a small value of d since as soon as d is less than of size 512 bits RSA is insecure [7].

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][11]. 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 d_p = d mod (p − 1), dq = d mod (q − 1) and d_r= d mod (r − 1)
vi. The public key would be (e, N) and the private key would be (d_p, d_q, d_r, p, q, r).

Encryption

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

Decryption

In order to decrypt a cipher-text c:

i. The decipher first computes m1 = $c^p d_p$ mod p, m2 = $c^q d_q$ mod q, and m3 = $c^r d_r$ mod r where c_p = c mod p, c_q= c mod q and c_r= c mod r

ii. Next, using CRT m can be obtained as m = c^d mod 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.

PROPOSED THRESHOLD Φ (N)^2 – Φ(N)-RSA ALGORITHM

Key Generation

1.Choose ‘n’ where ‘n’ is the product of primes such that n=p1 x p2 x p3…….p_n

2. Select any four primes P_i, P_j, P_k, P_l (choose largest multiples of n)

3. Calculate φ(n_1) where n_1=p_i x p_j φ(n_1) = φ(p_i x p_j) = φ(p_i) x φ(p_j) = (p_i – 1)(p_j -1)

4. Calculate φ(n_2) where n_2=p_k x p_l
 φ(n2) = φ(p_k x p_l) = φ(p_k) x φ(p_j)
 = (p_k – 1)(p_l-1)

5. Calculate φ(N)= $\frac{1}{2}$ * n * φ(n_1) * φ(n_2)

(For n>2,n∈Z, the sum of integers co-prime to n in the range [1,n−1] is equal to ½*n*ϕ(n))

6. Choose encrypt key ‘e’ such that gcd(e, φ(N))=1

7. Determine decrypt key ‘d’ such that ed≡1 mod φ(N)

Encryption

1. Obtain authentic public key (n, e).
2. Represent the message as an integer M in the interval [0, n − 1].
3. Compute C = M^e mod n

Decryption

1. Cipher Text ‘C’ is converted into Plain Text ‘M’ by using private key Pv=<d, φ(N)>
2. M ≡ i.e., M= C^{Pv} mod N

EXPERIMENTAL RESULTS OF PROPOSED ALGORITHM

The proposed algorithm is verified with sample input, we have taken input primes of sizes 1024 bit which has generated the following result.

For 1024 Bits:

p=91317715317151789379123789167317891113189712217891119782893287989398739249
3178913287989398739249 31789132879893987392493132879893987392493178913287989739
q=91312712176871762336123753165317890871131897081378801197828932879893987392475
17891328798939873924931789132879893987392493132879893987392493176913287989523
p(bits) = 512 q(bits) = 512
e = 9223372036854775837
d=1052324381004927777590427674208404832530268661720440499644819492606026572
098082380837750406214099899662214426869263863565490993150701352614690879603518383407283086
860274305888188153396900893537084886992416759278948617542911869796280206230316147042870731
511981167760416844887391415497616414063605859238568011489832785564431120818526502293721989
710383172073923309655392394351276147781674320769817761872649091474045783918445895847145366
295554574216736814501880370771705845805090867395560643249260250803228796143250447464106956
171031258907198582853287461327204697809550850793535134437672302937365382678419770304122611
05
n=8338468255404595244513668384405625840972461765772768777349266081359538
893923801218298686530981814311087114637698757809413210117217559925016600020586519372410106
557720488865692889852186885553985812595887918988005703518571398383360224506822408269816935
8945349960370696053406942243742435560523447162233563504497
n(bits) = 1023
Message : SECURITY

For 128 Bits:

p = 9131771531715178981
q = 9131271217687176289
p(bits) = 63 q(bits) = 63
e = 9131521371274666081
d=2289145521735860562672706202898315 280945916038552943124164919050913480211681
n=8338468255404595334436857237413 381509
n(bits) = 126
Message: SECURITY

For 64 Bits:

p = 9131771599
q = 9131271293
p(bits) = 34
q(bits) = 34
e = 9131521459
d=201282762523949525750856287555 1937728031
n=83384683856181407507
n(bits) = 67
Message: SECURITY

GRAPHICAL ANALYSIS

For our proposed threshold φ (n)^2 – φ(N)-RSA we need to consider their efficiency. For each phase of our Crypto System we analysed by taking different p, q values. We have considered 32 to 1024 bit N values and analysed and compared with traditional RSA system**.**

KeyGeneration Phase

Time Cost for Key Generation(in milliseconds)		
N	RSA	Threshold φ (n)2 – φ(N)-RSA
32	22.2	21.5
64	48.8	45.3
128	42.8	40.5
256	29.6	27
512	22.9	18.5
1024	18.1	16.9

Table-1 Key generation Phase for input of Size N bits

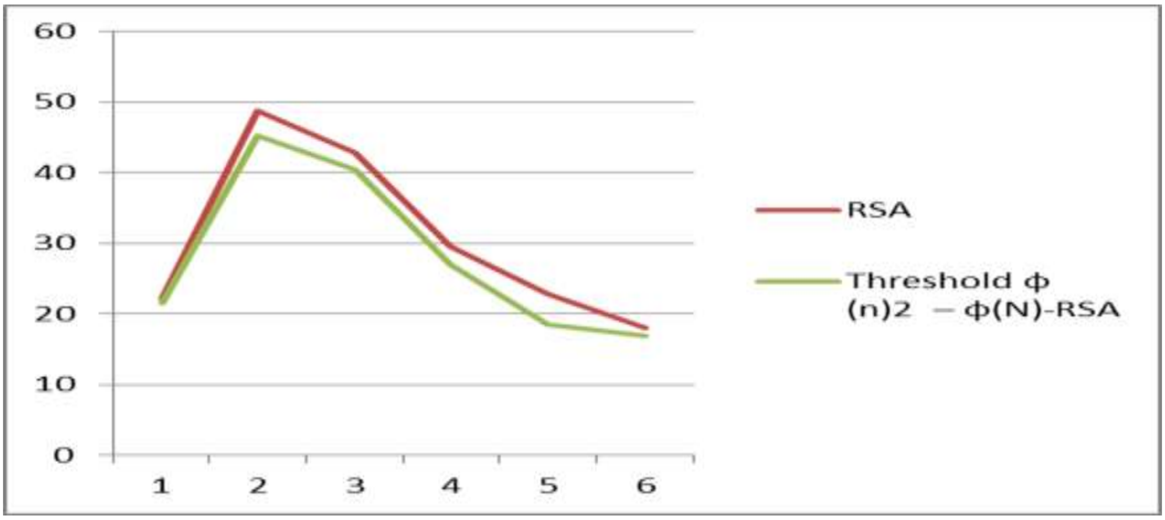

Fig-1 Graph showing comparison between RSA and Threshold φ (n)2 – φ(N)-RSA (on X-Axis 1-32 bits,2-64 bit ,…..)

Encryption Phase

The proposed algorithm is executed with different sizes of N and analyzed with RSA which has given better results shown below for encryption phase.

Time Cost for Encryption(in milliseconds)		
N	RSA	Threshold φ $(n)^2$ – φ(N)-RSA
32	0.157	0.126
64	0.081	0.065
128	0.145	0.096
256	0.151	0.112
512	0.485	0.245
1024	1.45	1.25

Table-2 Encryption Phase for input of Size N bits

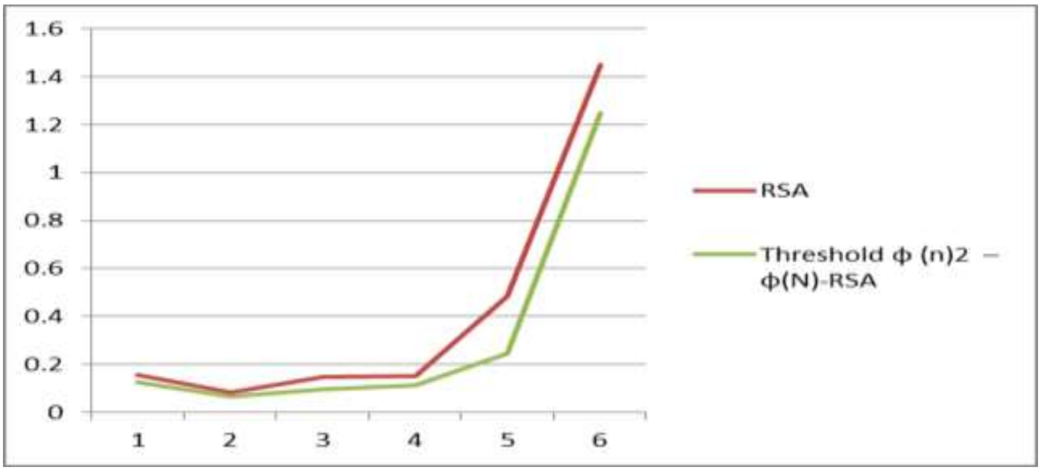

Fig-2 Graph showing comparison between RSA and Threshold φ (n)^2 – φ(N)-RSA (on X-Axis 1-32 bits,2-64 bit ,…..)

Decryption Phase

The proposed algorithm is executed with different sizes of N and analyzed with RSA which has given better results shown below for decryption phase.

Time Cost for Decryption(in milliseconds)		
N	RSA	Threshold φ (n)^2 – φ(N)-RSA
32	0.23	0.18
64	0.107	0.94
128	0.226	0.196
256	0.396	0.235
512	3.43	1.536
1024	18.7	13.25

Table: 3 Encryption Phase for input of Size N bits

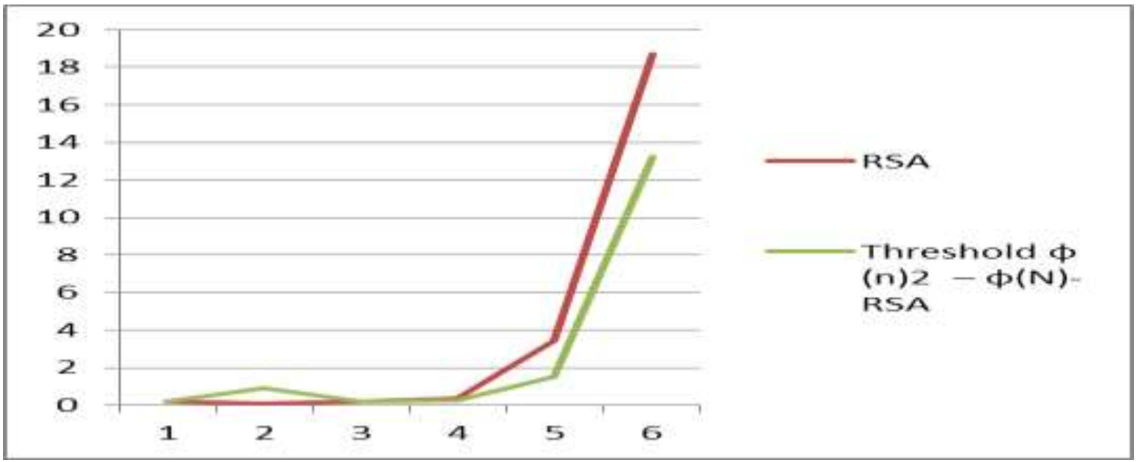

Fig-3 Graph showing comparison between RSA and Threshold φ (n)^2 – φ(N)-RSA (on X-Axis 1-32 bits,2-64 bit ,…..)

SECURITY ANALYSIS

1. Unlike RSA algorithm, we have chosen four primes which are the multiples of ‘n’ and these primes are secret keys. It is very difficult to find these secret keys as none of them are not equal to half of n (n/2) which is an attack on RSA algorithm [6].
2. In this algorithm, ‘d’ is a secret key whose size in bits is always double than that of ‘n’ bits size. ‘d’ is generated with double the bit size of ‘n’, so that no attack will affect to find ‘d’ since the size if unbreakable.

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. So in this paper we have developed a threshold cryptosystem Threshold φ (n)^2 – φ(N)-RSA which uses different totient function to improve security and performance. we considered different data values and analyzed our method with RSA and given complete analysis. Therefore by taking from above investigations we developed a robust cryptosystem which is resistant to attacks than RSA .

REFERENCES

[1] R. Rivest, A. Shamir, and L. Aldeman, “, A method for obtaining digital signatures and public-key cryptosystems,” Communications. ACM, vol. 21, no.2, pp. 120–126, 1978

[2] Diffie W and Hellman M, “New Direction in Cryptography”, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[3] Bruce S, "Applied Cryptography", 2nd John Wiley and Sons, Inc. 1996

[4] Rivest R, Shamir A and Adelman L, “*A Method for Obtaining Digital Signature and Public Key Cryptosystems*”, Communications of the ACM, 21, pp. 120-126, 1978

[5] T. Elgamal, ”A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm,” IEEE Trans. on Inf. Theory, IT-31, No.4, pp.469-472, 1985

[6] *Dan Boneh. “*Twenty Years of Attacks on the RSA Cryptosystem”

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

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

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

[10] R. Rivest and R. Silverman, Are “Strong Prime” Needed for RSA? Cryptology ePrint Archive Report 2001/007, 2001 [Online]. Available: http://eprint.iacr.org/2001/007

[11]. Suresh.K, Venkataramana.K , “*Study of nalysis on RSA and its Variants*”, International Journal of Computer Science Research & Technology (IJCSRT), , ISSN: 2321-8827 ,Vol. 1 Issue 4, September – 2013

AUTHOR BIBLIOGRAPHY

Dr.R.Seshadri working as Professor & Director, University Computer Centre, Sri Venkateswara University, Tirupati. He was completed his PhD in S.V.University in 1998 in the field of “ Simulation Modeling & Compression of E.C.G. Data Signals (Data compression Techniques) Electronics & Communication Egg.”. He has richest of knowledge in Research field, he is guiding 10 PhD in Fulltime as well as Part time. He has vast experience in teaching of 26 years. He published 10 national and international conferences and 8 papers published different Journals.

S. Venkateswarlu Research Scholar in SV University, Tirupati and Working as Programmer in the Computer Centre, S.V.University, Tirupati. He has 16 years of Computer programming experience.