International Journal of Engineering & Technology, 7 (4.36) (2018) 293-295

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paperv

Lightweight Rsa Algorithm Using Three Prime Numbers

Mustafa M. Abd Zaid[1], Dr. Soukaena Hassan[1]

[1]Computer Sciences Department/ University of Technology, Baghdad, Iraq
**Corresponding author E-mail:mustafamajeed2014@gmail.com*

Abstract

The computing devices utilized as a part of an extensive class of remote correspondence systems, for example, cell phones, remote sensor systems (WSNs), vehicular ad hoc networks (VANETs), mobile ad hoc networks (MANETs), Internet of Things (IoT), body area networks (BANs) and so on, are little and asset compelled. In the current developments of the resource constraint environments, the trend is shifted towards lightweight cryptographic algorithm. Many lightweight cryptographic algorithms have been developed and also existed algorithms are modified in terms of resource constraint environments. One of such new procedures is utilizing three prime numbers for RSA cryptosystem, which is not easily breakable. Our approach using three prime number rather than two prime-dependent systems to get (n) with same length of standard RSA but less bits for prime numbers. The suggested algorithm has speed enhancement on standard RSA key generation side and decryption side by utilizing three primes and the Chinese Reminder Theorem (CRT). The results indicate that the average of speed improvement is ~80% in key generation process, ~96% in decryption process, and only 4% in the encryption process.

Keywords: *Decryption, encryption, key generation, three prime-RSA algorithm*

1.Introduction

The encryption system using asymmetric key includes the utilization of two unmistakable related keys, the private key and the public key (1). The original message is changed over to cipher text utilizing the public key. This one procedure is called “encryption” which is completed by the sender. Then again, decoding of the cipher text is performed by the receiver via utilization of the private key, and this is called “decryption”. The private key is known by the receiver only with a specific end-goal to keep the private keys confidentially. In the opposite, the public key is uncovered to users in general. To guarantee that the message is originated by the intended side and with confidentiality, the public key is used. The cipher text created by the sender can be deciphered by the recipient’s private key only. Since information of the public key isn't adequate to decrypt the cipher-text, messages exchange can be done in a protected way. As a result of the above preferred standpoint, in our suggested algorithm we followed the asymmetric key cryptography method (1).

The RSA cryptosystem was uncovered for the first time in August, 1977 (2). For giving protection and guaranteeing authenticity of digital information, RSA is used. Interestingly, RSA is utilized by numerous business frameworks. It is utilized to anchor web activity, to guarantee protection and authenticity of Emails (3), and to anchor remote login sessions (4), and it is at the core of electronic charge card installment frameworks (5). B.Persis (6), for giving the security over the systems, they utilized many prime numbers to ease the cryptography use for better quality. In RSA cryptosystem, the ‘n’ prime numbers play (act) a very essential part to build up the RSA-based algorithm utilizing 4 prime numbers.

Somani and Mangal (7) described the RSA cryptosystem and its variations. Speed enhancement on the decryption side of RSA algorithm was introduced by utilizing the idea of Chinese remainder theorem. The suggested strategy likewise enhances the security of RSA algorithm by keeping it away from few attacks that are available on RSA algorithm like chosen cipher-text attack, common modulus attack, known plaintext attack, and timing attack.

Padmaja et al (8) used an RSA algorithm utilizing three primes (Mersenne) as against the standard RSA algorithm of two normal primes. The choice of the public key and generation of the private key is vital part of RSA cryptography. Public key can be produced haphazardly. The expectation that the encryption work is the security of RSA that depends on, thus it is computationally infeasible for an intruder to decode a cipher text. Mersenne primes are utilized to improve the security. The primes (p, q, and r) are the three components that the strength of a huge prime number is relied on. It is regarded to be hard to break the vast number into three.

Sahu et al (1) presented a RSA-algorithm-based system with an increase in the potential of security. The standard RSA-algorithm-based end of “n” and insertion of a new number f in the place of n is the security highlight proposed. This replacement is used in both private and public keys. Mathematical factorization attacks are prone to the RSA algorithm, and eliminating n with f makes the process very hard to factorize it and get the original numbers i.e. p and q. Despite of a slight increase of time complexity, this modification makes the algorithm more secure.

2.RSA methodology

It is hard to discover the factors of large integers, the supposition that the asymmetric key encryption system (RSA) depends on. In RSA, the private key is kept mysterious; however, the public key is sent to everybody in the framework. Key generation, message encryption, and message decryption, are the three steps used in the RSA algorithm (1). The steps are shown below:

2.1. Key generation

➢ Select arbitrary huge prime integers p_n and q_n of generally a similar size.
➢ Find $N = p_n$ x q_n.
➢ Find φ(N) = (p_n -1) × (q_n-1).
➢ Choose integer e_x, such that gcd (e_x, φ (N)) = 1; 1 < e_x < φ (N).
➢ Find the decryption exponent d, $e_x \times d \equiv 1$ mod φ(N).
➢ Now, e_x and N (e_x, N) are the Public Key, d and N (d, N) are the Private Key.

2.2. Encryption of RSA

To encrypt the message “Me”, the sender utilizes the following step:
• Cipher text Cm = Me^{e_x} Mod N :
where “Cm” is the cipher text created after encryption.
In the RSA encryption step, the message “Me” is encrypted by the user B by utilizing the public key of the sender.

2.3. Decryption of RSA

The reception should do the following step to get the message “Me” or plaintext from “Cm”, utilizing the private key “d” to recover:
Me = Cm^d mod N.

2.4. Proposed RSA

The proposed scheme includes providing an improvement to the RSA technique by proposing a technique that has speed enhancement on the RSA key generation/decryption sides.
A new component "s_n" was added to increase the complexity of the RSA algorithm. So the time of key generation must be decreased, and the analysis difficulty of the variable “N” must be increment because of the presence of three prime numbers rather than two.

2.5. The proposed RSA-based key generation

Three-prime-dependent generation of the key requires user “A” to perform the following steps:
➢ Three large prime numbers p_n, q_n and s_n are generated.
➢ Calculate N=p_n×q_n×s_n.
➢ Calculate φ(N) = (p_n -1)(q_n -1)(s_n-1).
➢ Chooses e, 1 < e_x < φ (N) like that gcd (e_x, φ (N)) = 1
➢ Finds d such that e_x×d = 1 mod φ (N).
➢ Finds d_p such that e_x×d_p = 1 mod (p_n -1) , d_q such that e_x×d_q = 1 mod (q_n -1).
➢ Finds Q_{in} such that
o q_n ×Q_{in} = 1 mod p_n. if p_n > q_n
o p_n ×Q_{in} = 1 mod q_n. if q_n > p_n
➢ Public Key Ku=(e_x, N) and Private key Kr=(Q_{in}, d_p, d_q, p_n, q_n).

2.6. The proposed RSA-based encryption

User “B” encrypts the massage “Me” performing the following steps:
• User “B” should get the public key of user “A” (e_x, N)
• Cipher text Cm = Me^{e_x} Mod N

2.7. Decryption for the proposed RSA

To recover the message from cipher-text Cm, we use the concept of RSA with CRT on the decryption process. The receiver must do as per the following:
➢ M_a = C^{dp} mod p_n
➢ M_b = C^{dq} mod q_n
➢ h= (Q_{in}×(M_a-M_b)) mod p_n
➢ Me=M_b+(h×q_n) =plaintext
Figure1 given below shows the flowchart of the proposed RSA algorithm, which is suggested here in this paper.

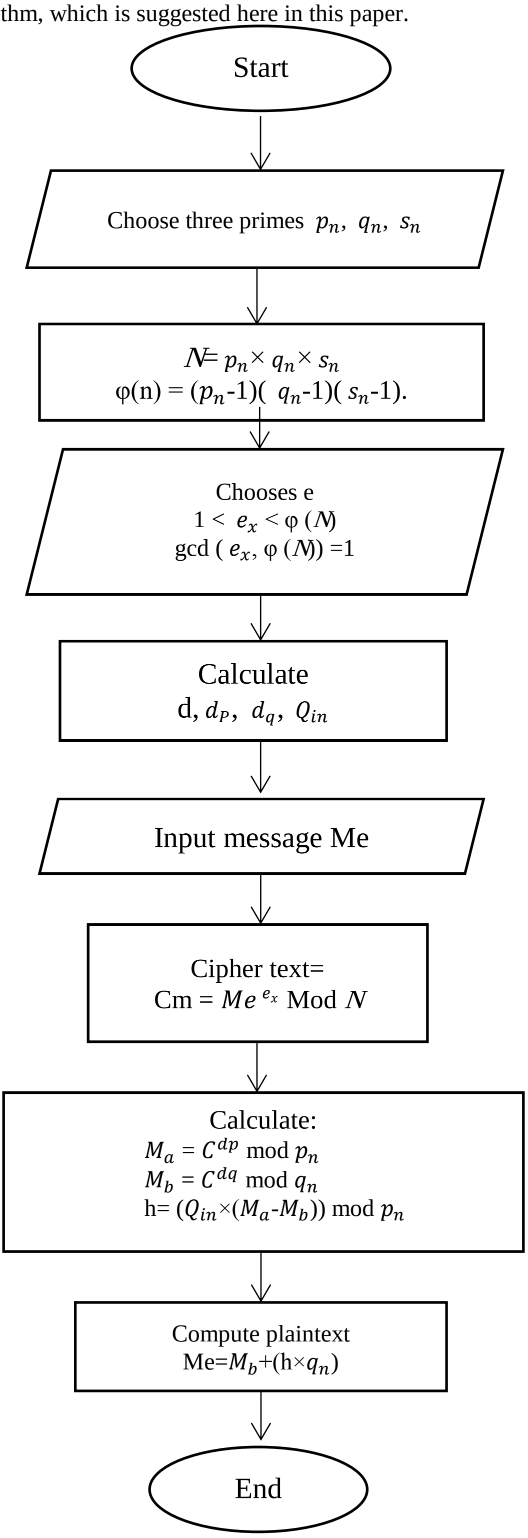
Start
Choose three primes p_n, q_n, s_n
N= p_n× q_n× s_n
φ(n) = (p_n-1)(q_n-1)(s_n-1).
Chooses e
1 < e_x < φ (N)
gcd (e_x, φ (N)) =1
Calculate
d, d_P, d_q, Q_{in}
Input message Me
Cipher text=
Cm = Me^{e_x} Mod N
Calculate:
M_a = C^{dp} mod p_n
M_b = C^{dq} mod q_n
h= (Q_{in}×(M_a-M_b)) mod p_n
Compute plaintext
Me=M_b+(h×q_n)
End

Fig1: Proposed RSA flowchart

2.8. Simple Example

Me= 4228

➢ **Keys generation**

- Select three prime numbers.

p_n = 367, q_n = 331, s_n = 197

- N =p_n *q_n*s_n = 23930969
- φ(N) = (p_n -1)(q_n -1)(s_n -1) =23672880
- Chooses e_x < e_x < φ (N) like that gcd (e_x, φ (N)) = 1, e_x= 9855803
- If e_x=9855803 then d=7163267, d_p= 281, d_q= 287, Q_{in}= 316
- Public Key= {9855803, 23930969}, private key= {316,281,287,367,331}

➢ **Encryption step**

- Cm = Me^{e_x} Mod N = 6751754

➢ **Decryption step**

- M_a = C^{dp} mod p_n=6751754^{281} mod 367= 191
- M_b = C^{dq} mod q_n =6751754^{287} mod 331= 256
- h= (Q_{in}×(M_a-M_b)) mod p_n=12
- Me=M_b+(h×q_n) =**4228**

2.9. Experiment results

The performance of the modified RSA algorithm was done by taking different key sizes for comparing the speed of key generation step, the encryption process, and the decryption process between the standard RSA algorithm and the modified RSA.
Table1 shows time comparison between standard RSA algorithm and the proposed RSA.

Table 1: Time comparison between the standard and the modified RSA algorithms

Key size	Massage size	Standard RSA time			Modified RSA time		
		K-generation	Encryption	Decryption	K-generation	Encryption	Decryption
68 bit	3 bit	0.01111	0.00015	0.000151	0.00791	0.000137	0.00005
340 bit	20 bit	0.228	0.0157	0.0144	0.107	0.01005	0.00096
664 bit	94 bit	5.34	0.219	0.202	0.989	0.213	0.00643

The results show that the modified RSA algorithm was faster than the standard RSA especially when taking in considerations key generation and decryption steps.

3.Conclusion

In this paper, we have introduced RSA algorithm utilizing three primes as compared to the standard RSA algorithm which uses two primes. The determination of the public key and generation of the private key is the essential part of RSA cryptography system. Public key can be generated randomly.
The suggested algorithm has speed enhancement on the key generation and decryption sides of RSA algorithm. On the key generation side by using three primes number rather than two primes, The process provides N with same length of the standard RSA but with less bits for prime numbers. In the other side, the speed of decryption face has improvement by utilizing the idea of CTR (Chinese remainder theorem), and this technique avoids some attacks that are conceivable on the RSA algorithm which leads to enhancing the security of RSA algorithm. The large prime number strength is reliant on three variables p_n, q_n, and s_n. So it is esteemed to be hard to break the huge number into three.

References

[1] J.Sahu, V.Singh VS and AC. An Enhanced Version of RSA to Increase the Security. J Netw Commun Emerg Technol. 2017;7(4):2395–5317.

[2] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM [Internet]. 1978;21(2):120–6. Available from: http://portal.acm.org/citation.cfm?doid=359340.359342

[3] Kelly G, McKenzie B. Security, privacy, and confidentiality issues on the Internet. J Med Internet Res [Internet]. 2002 [cited 2018 Sep 27];4(2):E12. Available from: http://www.ncbi.nlm.nih.gov/pubmed/12554559

[4] Amin R, Biswas GP. An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS. J Med Syst [Internet]. 2015 Aug 28 [cited 2018 Sep 27];39(8):79. Available from: http://www.ncbi.nlm.nih.gov/pubmed/26123833

[5] Alhothaily A, Alrawais A, Song T, Lin B, Cheng X. QuickCash: Secure Transfer Payment Systems. Sensors (Basel) [Internet]. 2017 Jun 13 [cited 2018 Sep 27];17(6). Available from: http://www.ncbi.nlm.nih.gov/pubmed/28608846

[6] B.Persis Urbana Ivy PMMK. A modified RSA cryptosystem based on 'n' prime numbers. Int J Eng Comput Sci. 2012;1(2):63–6.

[7] Somani N, Mangal D. An Improved RSA Cryptographic System [Internet]. Vol. 105, International Journal of Computer Applications. 2014 [cited 2018 Sep 27]. Available from: https://research.ijcaonline.org/volume105/number16/pxc3899820.pdf

[8] Padmaja CJL, Bhagavan VS, Srinivas B. RSA ENCRYPTION USING THREE MERSENNE PRIMES [Internet]. Vol. 14, Int. J. Chem. Sci. 2016 [cited 2018 Sep 27]. Available from: www.sadgurupublications.com