International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
Received: 13-09-2019; Accepted: 15-10-2019
www.newengineeringjournal.in
Volume 5; Issue 4; October 2019; Page No. 65-68

Building information security using new expanded RSA cryptosystem

Hammawa MB[1], Owolabi O[2], Abdulganiyu A[3], Mishra Amit[4]
[1, 2] Department of Computer Science, University of Abuja, Nigeria
[3] Department of Computer Science, Ibrahim Badamasi Babangida University Lapai, Nigeria
[4] Baze University, Abuja, Nigeria

Abstract
Our article Expanded-RSA algorithm is to bring about an innovative and enrichment of data security over Internet network (Mathur, Gupta, Goar, & Choudhary, 2018). The proposed plan strengthen data by increasing dispersion in ciphertext using Expanded-RSA to rebrand our information from unauthorized access. Thus, unauthorized personnel determination needs extra period to access the information and we find a resolution to differential attack, linear bout and brute-force attack. Our anticipated research results are done by comparing the existing RSA on the time of encryption and period it takes to decryption text historically. Our outcome shows the manipulated expanded algorithm takes little stretch for encryption period with less stint of decryption. This has upgrades safety of the information.

Keywords: encryption, expanded RSA, information security, cryptography, modification

Introduction
On the net, information's are vulnerable to varieties of attacks. Security of information is the foremost importance during data management, transfer of information, or wireless communication. This has help us to accomplishing confidentiality in data transfer. Numerous cryptography schemes are introduced. Cryptography are apply in messages that are to be sent, this give confidentiality, with low adjustment and offer quality protection to data when transmitting on the internet (Chaudhury et al., 2017) [6]. Cryptography is a method of altering a message into non-readable presentation, this prevents the text from illegal entree to the data, or make look unimportant. Previously, numerous decryption and encryption procedures are acquainted with which provide a safe broadcast of data on the internet.
Cryptography practices are divided into two main categories, the asymmetric cryptosystem and symmetric cryptosystem. Symmetric cryptosystem it functions in a means that the same key is used for public and private key process. This cryptosystem might be stream cryptograph text or block cryptograph text. In stream cipher, information or data are manipulated one by one, while in block cipher text, nearly all bits are manipulated in units. Occasionally, lining in plaintext are required, this could make manifold of block size. Blowfish is a good representation of symmetric cryptosystem (Akash Kumar Mandal & Tiwari, 2012) [1]. while asymmetric cryptosystem defers as two keys are apply to manipulate and decryption. The manipulation key is called public key and is known to both person and is for encryption while the other key is hidden as private key, it's used for decryption; RSA algorithm is a good illustration of asymmetric cryptosystem.
Here are several weaknesses for secret encryption key maintenance is one of the challenges in secret encryption systems and weak security strength, in asymmetric encryption methods key maintenance is easy. There are drawbacks of asymmetric encryption algorithms but is better than symmetric in computing resources such as processing time, power consumption and memory usage, (Kamardan et al., 2018) [10].
A proposed protocol architecture by Ren (Dixit, Gupta, Trivedi, & Yadav, 2018) [9], the DES procedure are apply in data communication because of its effectiveness. The RSA algorithm is good in place of key encryption due to merits it has on key cipher. The fuzz key RSA encryption and the encryption message from DES encryption are sent out. The decryption algorithm is the inverse of encryption algorithm. The limitation of this research is using traditional RSA algorithm which most hackers has been working had to bypass. We need to upgrade the RSA algorithm to strengthen security surrounding data.
Hence, the focal goal is to ensuring security by developing new expanded cryptography protocol. This new security protocol using Expanded encryption RSA cryptographic techniques is proposed systems help us to eliminate the disadvantages on the existing protocols. This will increase the security of the key plus increasing security using cryptography. Finally, we will have cipher text cannot be decrypted except the recipient

RSA Algorithm
RSA (Rivest Shamir Adleman) is one of the commonly use public key cryptosystem, that uses two keys, one for encryption and the other one for decryption procedure such as public key and private key, respectively. The real-world exertion of factorization of two or more large prime numbers gives strength and defines the security of RSA algorithm (Aules Centeno et al., 2016) [2]. RSA Key generation and implementation goes as follows:

RSA key generation Pseudocode
1. Randomly Select dual number prime, f and g which their product f *g is n

2. Calculate n= f g and
3. Ø(n)=(f −1)*(g −1).
4. Choice a number e, such that 1<e <Ø(n), such that GCD (e, Ø(n))
5. Calculate the secret key d, 1<d <Ø(n), such that e *d 1(mod Ø(n)).
6. (e, n) as the encryption key while (d, n) represent the private key.

where
• n is modulus,
• e is the public exponent and d is the secret exponent or decryption.

Encryption pseudocode
Assume a user A sending message "m" to user B.
1. Obtain a public key (e, n) of user B.
2. Present plaintext as positive integer m.
3. Calculate the cipher text c me mod n, using user B's public key.
4. Send the ciphertext c to user B.

Decryption psuedocode
User B will retrieve the original message from cipher text.
1. Use private key (d, n) to compute m cd mod n.
2. Extract the plaintext m from c.

Literature survey
Numerous ways out for solving information security in centralize information in a server nonetheless putting into application, strong security for which large data (size > 1Terra Byte). According to (Chaudhary et al., 2018) [5], giant data built on electronic information has been increasing annually since 2011. Based on the current investigation, it suggested that about 3.5 zettabytes (3.5 x 1021 bytes) of data were held in 2012. Privacy is a main challenge in information center which hold information in a proper management technique.
(Chandravathi & Lakshmi, 2017) [4] Their research objectives is to bring safety of information in applying Multiplicative Homomorphic Method. This encryption procedure is implemented using RSA algorithm adding Shor's algorithm was used to generating encryption Key Module, Shor's algorithm has a crucial part in computing encryption key. main Text is manipulated with encryption Key to produce Secret Text and for decryption a Chinese Remainder Theorem is integrated to fasten calculations. This CRT is applied to implement modular exponentiation which is more efficiently applying three additional values pre-calculated from the prime factors of n. This makes security improve over cloud provider. This researcher tries to add a fair performance of the most used RSA (Rivest-Shamir-Adleman) algorithm in the data encryption.
This Method postures privacy concerns with popular cloud services provider, to bar unauthorize hacker from sensitive information are lost. The keys are hacked by impostor, the encrypted material is shared with impostor that suppose not to have access the content. Besides, untrusted servers and cloud workers can hold back essentials data of users long after users end the bond with the services provided,
(Aules Centeno et al., 2016) [2] research target is to perfect the RSA encryption system by increasing the security and integrity of information. The output shows an efficiency and strength of the RSA algorithm in terms of information security. It is also shown that time, memory used, and performing encryption and decryption are period take little time than other RSA algorithm, because computations are performed on the client and server. The main setback was that when the size of prime numbers increases then the number of rounds unrolled and this rise was initially counterpoise by packing the round keys within round structure.
(Cordova, Maata, Halibas, & Al-Azawi, 2017; Davis, 2017) [7, 8] Their examination goals is to offer safekeeping of information within the cloud utilizing, increasing Homomorphic method. This coding procedure is completed with RSA algorithmic rule, Shor's algorithmic rule is employed to creating Public Key part, that improves the safety Shor's algorithmic plays imperative in creating public key. Chinese Remainder Theorem is employed to accelerate de encryption. Thus, it demonstrates however the CRT portrayal of numbers in metal is used to perform isolated operation regarding fruitfully utilizing 3 extra esteems pre-processed from the prime variables of n. Thus, security is improved within the cloud provider. These individual tries to expand an affordable execution of the foremost usually utilised RSA (Rivest-Shamir-Adleman) algorithmic rule within the encoding. The key limitation of those schemes was that they supply security to a specific parameter at the value of different.
(Barnes, 2016) [3] Proposed using RSA algorithm applying three primes numbers as against the two prime number RSA. The significant part of RSA cryptosystem is the picking of public key and generation of private key. Public key can be randomly generated. The strength of RSA is based on the fact the encryption role is one way and so it is computationally difficult for an unauthorize hackers to decipher text messages. Mersenne primes technique are apply to improve the security. The strength of this research is using large prime number as dependent on three factors, f, g, and h. This make it hard to break the large figure into three. The limitation of their research is the use of Mersenne primes numbers, which means only selected prime numbers can be used. In the result algorithm generated using minor numbers, and proposed algorithm were never verify using any mathematical tools like MATLAB.
Another approach was proposed for combining symmetric and public key methods in (Cordova et al., 2017) [8] research on application using multi-level encryption with Data Encryption Standard (DES) with modified RSA Algorithm, the multi-prime RSA. In Her research multi-level RSA and DES overcome the disadvantage of using DES encrypting key. The cryptography tools used are RSA, DES and Random Number Generator. This technique is more profound on small amount of data like passwords.

Problem description
Most establishments and private information that are kept over the Internet or cloud computing. This information deposited are extremely confidential and which unauthorized people should not have access to it. Manipulating of data is most traditional practice which highly secure our information, applying few unadventurous algorithms, which is in existence or modify. The most commonly encryption method is generation of key in symmetric and asymmetric key. Currently hackers are proficient to disruption secret keys with the help of

contemporary high processing power of technologies. Currently we need a strongly modifying or expanded encrypted data which was difficult to decrypt using cryptanalysis.
From our conclusion after literature study, the best method to offer safety to data is to use a new Expand asymmetric RSA algorithms on the data. We used new RSA to encrypt our data, then the private key will be manipulated using our expanded RSA algorithm for more data security. Our research target on how to expand the prime number of RSA algorithm so to make it difficult in predicting the prime factor. We also changed the public key of RSA before sending the modification to the receiver.

Proposed method
Extended-prime RSA is a variation of RSA in which the modulus is the result of in excess of two particular primes. The upside of Extended-prime RSA over standard RSA lies with the expansion of numbers of prime, this will strengthen the security process (Liu, Tang, Liu, Zhang, & Ma, 2018). The encryption procedure is also modified to strengthen the standard of RSA.
We start by showing a streamlined variant Extended-prime RSA. For any whole number r≥2, r - prime RSA comprises of the accompanying seven algorithms:

Method of generating Key in Proposed Scheme
Phase 1: Let F,G,H,I represents a large prime number
Phase 2: The product n=F*G*H*I and phi (n) = (f-1) (g-1) (h-1) (i-1).
Stage 3: Select e with a definitive target that (e, phi(n)) are overall co-prime.
Stage 4: Pick out two whole figure j and k to such an extent, to the point j=ke2.
Stage 5 Solve e= sqr(j/k)
Stage 6: Find d by utilizing the recipe e*d = 1 mod (phi(n)).

Encryption for Proposed Scheme
To scamper the substance M step are as per the going with:
Stage 1: Assume Mr A. which is the sender wish to send information to someone whose public key is (n, e). The sender will represent (n, e) with (n, j), (n, k)
Stage 2 We present the message.
Stage 3: Compute cipher text as:

C=Me mod (n)

Stage 4: we convey cipher text to the receiver using manipulated public key as:

C= M(j/k)1/2 mod n

Stage 5 Transmit encrypted text to the receiver.

Decryption for proposed scheme
Receiver take the following action:
Stage 1 Apply remote key (n, d) to compute plaintext:
M=Cd mod (n)
Stage 2Tthe plaintext from the message representative M.

A Working example
Let the plaintext: 2530

Key Generation
Predict any four prime numbers: f = 101, g = 103, h = 107, i = 109
1. Calculation of parameters: N = f x g x h x i = 101 x 103 x 107 x 109 = 121, 330, 189
2. phi(n), Ø (N) = (f – 1) (g – 1) (h – 1) (i – 1 100 x 102 x 106 x 108 = 116, 769, 600
3. (3) Gcd (e,phi(n)) = 1 public key e= 140
4. Pick integers j and k such that {sqr(j/k)=e}a.
5. (5) The manipulated e will be: {j, n}: {1176000, 121, 330, 189} {k, n}: {60, 121, 330, 189}
6. (6) private key d= 47762873

Encryption
1. Selecting the random integer ‘a’ such as: GCD (a, 134243153) = 1 a=202
2. Cipher texts: [C= 106310778] [C2= 707324781]

Decryption for Proposed Scheme
140d (mod 116, 769, 600) = 1
834, 068.5714
0.5714284 ≈ 1
66, 725, 477.37
≈ 66, 725, 477

Results and discussion
While using the above stated methodology, we came across various advantages of using New Expanded RSA cryptosystem which is an advancement over simple RSA. The plaintext is encrypted with new Expanded RSA cryptosystem, this help data securely stored on cloud system. Proposed system is highly efficient against malicious data it provides high security with good execution time. Encryption New Expanded RSA has ensured competence and trustworthiness in store servers. During messages are sent in the cloud computing it improve security of cipher text message send during communication, it also reduced time consumption and storage size. The new expansion algorithm which is an improvement on traditional RSA algorithm. We conclude that our New algorithm has serve better than the existing RSA algorithm, as it can withstand Brute Force attack, Timing Attack as well as Mathematical attacks.

References

1. Akash Kumar Mandal CPAM, Tiwari A. Performance Evaluation of Cryptographic Algorithms: DES and AES. IEEE Students’ Conference on Electrical, Electronics and Computer Science, 2012, 1-5.
2. Aules Centeno HM, Meneses F, Fuertes W, Sancho J, Salvador S, Flores D, Nuela D. RSA encryption algorithm optimization to improve performance and security level of network messages, 2016.
3. Barnes J. Nice numbers: Springer, 2016.
4. Chandravathi D, Lakshmi P. Advanced Homomorphic Encryption for Cloud Data Security. JOIV: International Journal on Informatics Visualization. 2017; 1(1):1-4.
5. Chaudhary R, Jindal A, Aujla GS, Kumar N, Ds AK, Saxena N. LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. IEEE Communications Magazine, 2018, 25.

6. Chaudhury P, Dhang S, Roy M, Deb S, Saha J, Mallik A, Kumar S. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. Paper presented at the Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual.
7. Cordova RS, Maata RLR, Halibas AS, Al-Azawi R. Comparative analysis on the performance of selected security algorithms in cloud computing. Paper presented at the Electrical and Computing Technologies and Applications (ICECTA), 2017 International Conference on, 2017.
8. Davis VA. Internet security for mobile computing, 2017.
9. Dixit P, Gupta AK, Trivedi MC, Yadav VK. Traditional and Hybrid Encryption Techniques: A Survey Networking Communication and Data Knowledge Engineering Springer, 2018, 239-248.
10. Kamardan MG, Aminudin N, Che-Him N, Sufahani S, Khalid K, Roslan R. Modified Multi Prime RSA Cryptosystem. Paper presented at the Journal of Physics: Conference Series, 2018.
11. Liu Y, Tang S, Liu R, Zhang L, Ma Z. Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications. 2018; 97:95-105.
12. Mathur S, Gupta D, Goar V, Choudhary S. Implementation of Modified RSA Approach for Encrypting and Decrypting Text Using Multi-power and K-Nearest Neighbor Algorithm Networking Communication and Data Knowledge Engineering, 2018, 229-237): Springer.