IBBUL
Lapai Journal of Applied and Natural Sciences
LAJANS Vol 3(1): 183-190

SHORT COMMUNICATIONS

Enrichment Of Information Security By Building New Hybrid Algorithm Using Expanded Rsa, And Des Cryptosystem

Abdulganiyu A.[1*], Hammawa M.B.[2] and Owolabi O.[2]

[1]*Department of Computer Science, Ibrahim Badamasi Babangida University, Lapai, Nigeria*
[2]*Department of Computer Science, University of Abuja, Nigeria*

ABSTRACT

The idea of fuzzing symmetric encryption method, DES (Data Encryption Standard) and asymmetric encryption modification this is to improve the strength of security on a cloud computing. Our article Expanded-RSA algorithm are fuzz to bring about an innovative and enrichment of data security over Internet network . The proposed plan strengthen data by increasing dispersion in ciphertext using DES for data encryption and Expanded-RSA for key encryption. Thus, unauthorized personnel will need more time to decrypt the text and it also find a solution for the brute-force attack, differential attack, and linear attack. The performance analysis of the proposed plan is done and compared with the DES and Expanded-RSA on the foundation of encryption and decryption time. The result shows that the proposed plan takes little time for encryption process and less time for decryption process, hence it upgrades the security of the data.

Keywords: Encryption, ciphertext, decryption time

INTRODUCTION

On a public network, data is exposed to a broad range of attacks. Thus, security is of major importance during data handling, data transfer, and electronic communication. To accomplish the confidentiality in data transfer and to overcome attacks. Numerous cryptography techniques are introduced. Cryptography is used for message randomization, confidentiality, and low modification rate to provide high security to data over network (Chaudhury *et al.*, 2017). Cryptography can be a thought of as a process of transforming the plaintext into a non-readable format and prevents the message from unauthorized access. Thus, in the previously, numerous encryption techniques are introduced to provide a safe transmission of data over network

Cryptography techniques are divided into two main categories such as symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography works in such a way that it uses the same cryptographic key for both encryption and decryption process. It could either be stream cipher or block cipher. In stream cipher, message digits are encrypted one after the other, while in block cipher, some bits are taken and encrypted as a unit. Sometimes, padding in plaintext is needed, so that it could make a multiple of block size. AES is an example of symmetric key cryptography (Akash Kumar Mandal & Tiwari, 2012). In asymmetric key cryptography, different keys are used for the encryption and decryption process. One key is kept public known as public key which is used for encryption process while another key is kept hidden known as private key which is used for decryption process. RSA is an example of asymmetric key cryptography.

There are many drawbacks for symmetric encryption algorithms such as key maintenance is a great problem faced in symmetric encryption methods and less security level is the problem of asymmetric encryption methods even though key maintenance is easy. And there are many drawbacks of asymmetric encryption algorithms such as those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power

Received 24 November, 2018
Accepted 19 December, 2018
Address Correspondence to:
abdulg2009@yahoo.com

(Kamardan et al., 2018).

A proposed protocol architecture by Ren (Dixit et al., 2018), the DES algorithm is used for data transmission due to its efficiency. The RSA algorithm is used for the key encryption of the DES due to the advantages it carries in key cipher. The combination of the session key from RSA encryption and the cipher text from DES encryption are sent out. The decryption algorithm is the reverse direction 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. Therefore, the main target for ensuring security is to develop new hybrid cryptography protocol. This new security protocol using combination of both DES and Expanded encryption RSA cryptographic techniques is proposed by merging both symmetric and asymmetric techniques by a way that avoids the disadvantages of the existing hybrid protocols. This will increase the security of the key plus increasing security using hybrid cryptography. Finally, we will have cipher text cannot be decrypted except the recipient

RSA Algorithm

RSA (Rivest Shamir Adleman) is an asymmetric key cryptography, which uses different keys for encryption and decryption process such as public key and private key, respectively. The practical difficulty of factorization of two large prime numbers defines the security of RSA algorithm (Aules Centeno et al., 2016). The RSA plan is as follows:

Key generation:

1. Select two enormous random prime numbers, *p* and *q* of approximately equal size that their product *n p* **q* is desired bit length.
2. Calculate *n p* **q* and Ø(*n*)(*p* −1)*(*q* −1).
3. Select a positive integer *e*, such that 1<*e* <Ø(*n*), such that GCD (*e*, Ø(*n*))
4. Calculate the value of secret Exponent *d*, 1<*d* <Ø(*n*), such that *e* **d* 1(modØ(*n*)).
5. The pair (*e*, *n*) is a public key and (*d*, *n*) is a private key. The values *d*, *p*, *q*, and Ø(*n*) should be kept as a secret.

where

- *n* is modulus,
- *e* is the public exponent or encryption exponent or simply the exponent, and • *d* is the secret exponent or decryption exponent.

Encryption:
Suppose user *A* wants to send message "*m*" to user *B.*

1. Procure the public key (*e*, *n*) of user *B.*
2. Represent the plaintext as positive integer *m*.
3. Calculate the ciphertext*c* m^e mod *n*, using user *B*'s public key.
4. Send the ciphertext*c* to user *B.*

***Decryption*:**
User *B* will retrieve the original message from cipher text.

1. Use private key (*d*, *n*) to compute *m* c^d mod *n*.
2. Extract the plaintext *m* from *c*.

DES (Data Encryption Standard) *Algorithm*
A symmetric key block cipher DES (Data Encryption Standard) based on Feistel Cipher. Works on 16 round Fiestel Structure and with a block size of 64 bit. It has a effective key length of 56 bits. As 8 of the 64 bits of the key are not used by the algorithm (8 of those bits are used for parity checks). It can run in four various modes by encrypting blocks one by one or by making cipher block dependent from former blocks. But it is very easy to crack the key with the unreasonable force which involves trying every possible key until you find the right one and maximum it would take 2^56. So company came with the successor to DES which is 3DES IN which we execute three iterations of the DES algorithm to raise key length from 56 bit to 168 bits but it's comparatively slower than DES (Usman, Jan, & He, 2017).

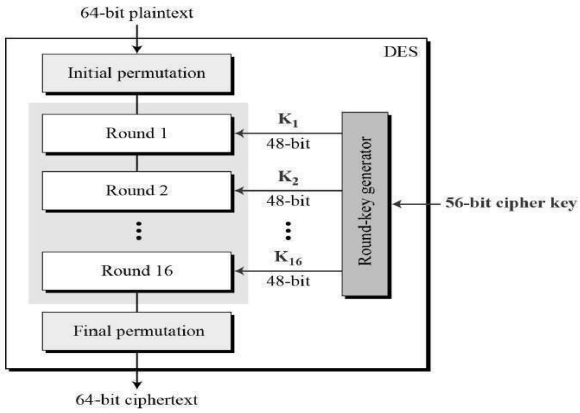

Figure 3. workflow of DES

Literature survey:

There are many solutions which are available for solving data security in data centers but putting into practice strong security for which big data (size > 1Terra Byte) being approached to the data center is one of the interesting topics. According to (Chaudhary et al., 2018), big data based on digital information has been doubling every 2 years since 2011. Based on the recent research, estimate also suggested that 2.5 zettabytes (2.5×10^{21} bytes) of data were handled in 2012. Keeping privacy is another major issue in data center which handles the data using proper management techniques.

(Chandravathi & Lakshmi, 2017) Their research aims to bring security of data in the Cloud using Multiplicative Homomorphic Approach. This encryption process is done with RSA algorithm, Shor's algorithm is used for generating Public Key Component, which improves the security Shor's algorithm plays as essencial role in producing public key. Plain Text Message is encrypted with Public Key to produce Cipher Text and for decryption Chinese Remainder Theorem (CRT) is used to speed up the calculations. By doing so, it shows how the CRT representation of numbers in Zn can be used to execute modular exponentiation about much more efficiently using three extra values pre-calculated from the prime factors of n. Hence, security is improve in the cloud provider. This researcher tries to add a fair performance of the most used RSA (Rivest-Shamir-Adleman) algorithm in the data encryption.

However, this approach poses privacy concerns. Mostly with popular cloud services, the control over the privacy of the sensitive data is lost. Even when the keys are not shared, the encrypted material is shared with a third party that does not necessarily need to access the content. Moreover, untrusted servers, providers, and cloud operators can keep identifying elements of users long after users end the relationship with the services. Indeed,

(Aules Centeno et al., 2016) research aims to perfect the RSA encryption algorithm and thus increase the security, integrity and availability of information. The results show the efficiency and functionality of the RSA algorithm in terms of information security. Also, we can see that time, memory, processor and network performance when performing encryption and decryption are lower than other RSA solutions, because computations are performed on the client and server. The main restriction was that when the size of implementation increases then the number of rounds unrolled or pipelined was increased and this increase was partially offset by the packing of the round keys within the round structure.

(Cordova, Maata, Halibas, & Al-Azawi, 2017; Davis, 2017)Their examination aims to offer security of information within the Cloud utilizing, increasing Homomorphic Approach. This coding procedure is completed with RSA algorithmic rule, Shor's algorithmic rule is employed for generating Public Key part, that improves the safety Shor's algorithmic rule plays as imperative half in generating public key. Plain Text Message is encrypted with Public Key to supply Cipher Text and for decoding Chinese Remainder Theorem (CRT) is employed to accelerate the calculations. 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. This 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) Proposed RSA algorithm using three Mersenne primes as against the traditional RSA algorithm of two normal primes. The important aspect of RSA cryptography is the selection of public key and

generation of private key. Public key can be generated randomly. The security of RSA is based on the hope that the encryption function is one way and so it is computationally infeasible for an intruder to decrypt a cipher text. Mersenne primes are used to enhance the security. The strength of large prime number is dependent on three factors, p, q, and r. It is deemed to be difficult to break the large number into three. The limitation of their research is the use of Mersenne primes numbers, which means only selected prime numbers can be used. In their result the algorithm is generated using only small 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) research on implementation of multi-level encryption using the Data Encryption Standard (DES) and a modified version of the 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 companies store business and individual information over the Internet or cloud computing. Much of the information stored is highly confidential and not for knowing publicly. Data encryption is most traditional technique that secure highly confidential information by using some conventional algorithm, which already exist or prewritten. Most powerful part of encryption technique is key generation, which has two parts, one is symmetric key generation and another is asymmetric key generation. Nowadays hackers are easily capable to break the key with the help of modern high computing machines. Current need is strongly modifying encrypted data which cannot be decrypt through cryptanalysis.

We have concluded after literature study that the best method to provide security to data is to use symmetric DES and Expand asymmetric RSA algorithms on the data at same time. We used DES to encrypt our data, then the private key is being encrypted by using our expanded RSA algorithm for more data security. The reason behind using DES symmetric algorithm is that it takes less amount of time in cryptographic operations compared to asymmetric algorithm. 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 $r \geq 2$, 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 $j=ke^2$.

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: Suppose the sender wish to send some text message to someone whose public key is (n, e). The sender then represents (n, e) with (n, j), (n, k)

Stage 2 Represent the plaintext message as a positive message as a positive integer.

Stage 3: Calculates the cipher text: $C=M^e \bmod (n)$

Stage 4: Send the cipher text to the receiver.

$C= M^{(j/k)1/2} \bmod n$

Stage 5 Send the cipher text to the receiver.

Decryption for Proposed Scheme:
Recipient does the following:

Stage 1 Use the private key (n, d) to compute calculate plaintext:

$M=C^d \bmod (n)$

Stage 2: Extract the plaintext from the message representative M.

WORKING EXAMPLE
Here small prime numbers are used for convenience; Let the plaintext: 2530

Key Generation:
Generate three large 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) Gcd(e,phi(n))=1 public key e= 140
(4) Choose two integers j and k such that {sqr(j/k)=e}a.
(5) The public key pairs are: {j, n}: {1176000, 121, 330, 189}
{k, n}: {60, 121, 330, 189}
(6) private key d= 47762873

Encryption:
(1) Selecting the random integer 'a' such as:
GCD(a, 1337243153) = 1 a=202
(2) Cipher texts: [C1= 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

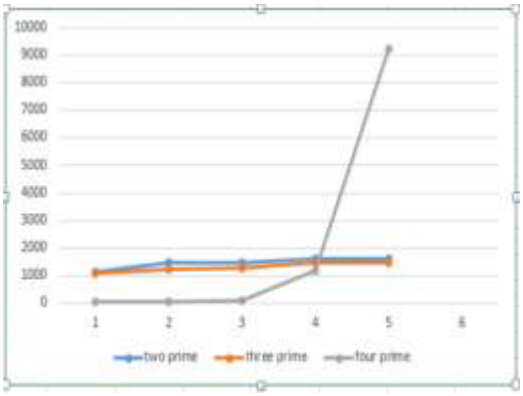

Fig. 1. Comparison of Encryption Time

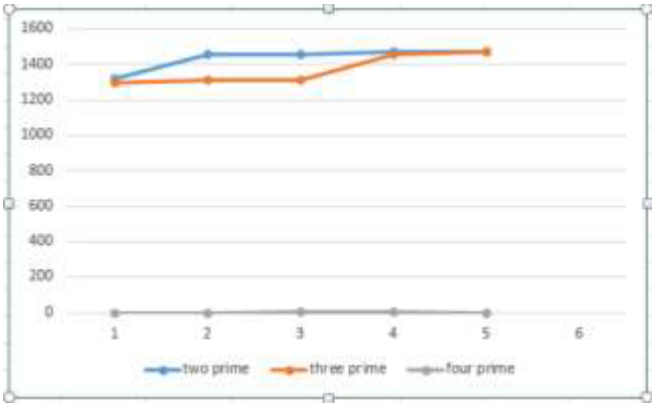

Fig. 2. Comparison of Decryption Time

TABLE 1: Encryption and Decryption Using Four Prime Numbers

PRIME 1	**PRIME 2**	**PRIME 3**	**PRIME 4**	**N**	**Phi (N)**	**Public Key e**	**Public Key d**	**Eneryption Time (ms)**	**Deeryption Time (ms)**
53	59	51	67	12780049	11943360	49	2437421	1534	1882
101	103	107	109	121330189	116769600	140	66725477	1711	1231
151	157	163	167	645328247	629272800	178	282819109	1177	2112
199	211	223	227	2125525169	2086151760	563	1111918888	1172	69743
263	269	271	277	5310765049	5232496320	850	123115406	9238	114248

RESULTS AND DISCUSSION

While using the above stated methodology, we came across various advantages of using the Expanded RSA along with DES cryptosystem which is an advancement over simple RSA. The data is encrypted using Expanded RSA, and DES cryptosystem, so data is successfully and securely stored on cloud. Proposed system is highly efficient against malicious data it provide high security and higher execution time. Hybrid encryption RSA along with Advanced Encryption Standard or DES has ensured efficiency, consistency and trustworthiness in cloud servers. During communication along with its application in cloud computing and to improve the security of cipher text or encrypted data in cloud servers along with reducing the consumption of time, cost and memory size during encryption and decryption. Hybrid encryption algorithm along with DES which is an improvement over simple RSA we can conclude that as the exponent size increases beyond 1024 bits, there is a significant difference between Original RSA and the proposed algorithm. However, it is efficient in terms of Brute Force attack, Timing Attack as well as Mathematical attacks.

REFERENCES

Akash Kumar Mandal, C. P. a. M., & Tiwari, A. (2012). Performance Evaluation of Cryptographic Algorithms: DES and AES. *IEEE Students' Conference on Electrical, Electronics and Computer Science*, 1-5.

Aules Centeno, H. M., Meneses, F., Fuertes, W., Sancho, J., Salvador, S., Flores, D., . . . Nuela, D. (2016). RSA encryption algorithm optimization to improve performance and security level of network messages.

Barnes, J. (2016). *Nice numbers*: Springer.

Chandravathi, D., & Lakshmi, P. (2017). Advanced Homomorphic Encryption for Cloud Data Security. *JOIV: International Journal on Informatics Visualization, 1*(1), 1-4.

Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., Das, A. K., & Saxena, N. (2018). LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. *IEEE Communications Magazine*, 25.

Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., . . . Kumar, S. (2017). *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.

Cordova, R. S., Maata, R. L. R., Halibas, A. S., & Al-Azawi, R. (2017). *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.

Davis, V. A. (2017). *Internet security for mobile computing.*

Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and Hybrid Encryption Techniques: A Survey *Networking Communication and Data Knowledge Engineering* (pp. 239-248): Springer.

Kamardan, M. G., Aminudin, N., Che-Him, N., Sufahani, S., Khalid, K., & Roslan, R. (2018). *Modified Multi Prime RSA Cryptosystem.* Paper presented at the Journal of Physics: Conference Series.

Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications, 97*, 95-105.

Mathur, S., Gupta, D., Goar, V., & Choudhary, S. (2018). Implementation of Modified RSA Approach for Encrypting and Decrypting Text Using Multi-power and K-Nearest Neighbor Algorithm *Networking Communication and Data Knowledge Engineering* (pp. 229-237): Springer.

Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences, 387*, 90-102