IBBUL
Lapai Journal of Applied and Natural Sciences
LAJANS Vol 1(1): 22 - 28

RESEARCH PAPER

Cost and Performance Analysis of Three Cryptographic Algorithms; MXORRSA, RSA and MXOR

Oladipupo E.T., Olayemi D.O., Adeagbo C.O. and Ndubuisi S.A.

Department of Computer Science, The Federal Polytechnic, Bida, Nigeria

ABSTRACT

Internet and networks applications are growing very fast, so the needs to protect such applications are increasing. Cryptography algorithms play a main role in information security systems. However, these algorithms consume a significant amount of computing resources such as CPU time, memory, and power. Other things being equal, a user needs a cryptography algorithm which consumes small amount of computing resources and has a very high performance. However, it is very difficult to get such cryptography algorithm in reality. What is found in real life is a cost performance trade off. In this paper three cryptography algorithms MXOR, RSA and MXORRSA are implemented and analyzed using a laptop having processor of Intel (R) Pentium (R) Dual CPU T2370 @ 1.73GHz, and a RAM of 1GB. A comparison was conducted for these cryptography algorithms at different settings for each algorithm using three pertinent metrics - encryption time, power consumption and encryption throughput. The result of the comparison shows that MXORRSA has the highest encryption throughput, lowest encryption time and consumes lowest amount of energy for large data sizes while for smaller data sizes RSA and MXOR has lower encryption time, higher encryption throughput and consume lower energy than MXORRSA. It is concluded that for applications that need to encrypt files of larger sizes MXORRSA is suitable while for applications that need to encrypt file of smaller sizes MXOR or RSA are suitable.

Keywords: Cryptography algorithm, Encryption throughput, encryption time, cryptography algorithm performance metrics

INTRODUCTION

Various online applications like shopping apps, banking apps, social networking apps provide services round the clock. With these applications, ease of access to shopping, communication, money at any time of the day and anywhere is made possible. The benefits of cloud computing which is a set of IT Services such as network, storage, hardware, software, resources that are provided to a customer over a network cannot be quantified. With cloud computing, it is now easy to have access to your knowledge anyplace, anytime, anyhow, at an affordable cost. Also with this cloud computing we now have availability, cost efficiency, and high reliability of the data. For these benefits each and every organization is transferring its data to the cloud.

All the afore mentioned applications brought about convenience to our day to day activities. But if an attacker gets access to these data it will be catastrophic. For example, if an attacker gets a banking password, money is stolen at the same ease. An attacker may acquire social media login credentials and use it for mischievous activities. Hence, securing information on computer, information sent via network, and information residing in applications is necessary. Cryptography algorithm is one of the mechanisms used in securing information. However, these cryptographic algorithms consume an amount of computing resources.

Since the level of security needed for different application varies from one user to the other, user will have to make choice from among different cryptographic algorithms. For the right choice to be made, the knowledge of strengths, weakness, cost and performance of each algorithm will provide valuable insights.

Received 21 December, 2016
Accepted 15 February, 2017
Address Correspondence to:
taiwotheophilus@gmail.com

In this paper three different cryptographic algorithms namely MXOR, RSA and MXORRSA, were implemented and analyzed to show overall cost and performance analysis.

Cryptography Algorithms

Cryptography algorithms play an important role in information security. They can be divided into Symmetric, Asymmetric and hash function (Rachana & Guruprasad, 2014). In Symmetric key encryption only one key is used to encrypt and decrypt data. The key should be distributed before transmission between two parties. Key plays an important role in encryption and decryption. If a weak key is used in the algorithm, then easily data can be decrypted. The size of the key determines the strength of Symmetric key encryption. Symmetric algorithms are of two types: Block Ciphers and Stream Ciphers (Selin, Sujin, & Saranya, 2016). The block ciphers are operating on data in groups or blocks. Here the size of the block is of fixed size for encryption. Stream ciphers are operating on a single bit at a time. Here continuous stream is passed for encryption and decryption. Asymmetric cryptographic algorithm on the other hand uses two different algorithms for encryption and decryption respectively, a public key for encryption a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of private key. Hash functions are fundamental elementary in the field of cryptography. A hash function H is an efficiently computable algorithm that takes as input an arbitrary length message M and potentially a fixed-length key K (considering a keyed hash function), and makes a fixed-length output D called the message digest (Alam, Biddu, Shafin, & Sharriar, 2016). Mathematically hash function is of the form

$$H(K, M) = D \quad (1)$$

Where D = Message output, K = Fixed key length, M = Input message length.

(Selin, Sujin, & Saranya, 2016) selected encryption time, decryption time, throughput of encryption, throughput of decryption, CPU process time, CPU clock cycles, Power consumption and memory utilization as metrics for determining the performance of cryptography algorithms and described how they can be used for performance analysis. (Priyadarshini, Prsshant, Narayan, & Meena, 2015) evaluated blowfish, RSA, DES using performance metrics memory size required for implementation, encryption and decryption time, avalanche effect and entropy. From their experimental results blowfish requires the smallest memory size for implementation whereas RSA requires the largest memory for implementation while DES and AES requires medium memory size. Their experimental result also revealed that blowfish consumes the least time for encryption and decryption. After evaluating the algorithms based on parameter Avalanche effect it was found out that AES scored highest. The result of evaluating the algorithm based on parameter entropy revealed that blowfish has the highest entropy. (Alam, Biddu, Shafin, & Sharriar, 2016) implemented AES, DES, BLOWFISH, 3DES, RC4 and RSA cryptographic algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system. The result of their experiment showed that AES consumes the least encryption time whereas RSA consumed the longest encryption time. The literature survey on comparative study of existing cryptography algorithms carried by (Nithya & Sripriya, 2016) revealed that authors have repeatedly taken DES, 3DES, AES, Blowfish, RC$, RSA and MD5 whereas IDEA, TEA, CAST, RC2, RC5,RC6, Serpent, Twofish, Threefish, Mars, ECC, DHA and SHA are compared and read less.

The three cryptography algorithms considered in this experiment are RSA, MXOR and MXORRSA

RSA, founded in 1977, is a public key cryptosystem. RSA is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir &Adelman. It generates two keys: public key for encryption and private key to decrypt message. RSA algorithm consist of three steps, step one is key generation which is to be used as key to encrypt and decrypt data, step two is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third step is decryption, where encrypted text is converted in to plain text at other side. RSA is based on factoring problem of finding product of two

large prime numbers. Key size is 1024 to 4096 bits

MXOR is an improved technique on traditional XOR encryption method. MXOR is an example of block cipher symmetric algorithm. It was founded in 2014 (Oladipupo, Alade, & Afolabi, 2014).

This algorithm combines XOR and RSA to form an asymmetric cryptographic algorithm. The algorithm uses three keys two generated by using RSA technique and one generated using exclusive OR (XOR) technique. To encrypt the public key of the RSA and the private key of the XOR are used. The decryption is carried out using the private key of RSA and Private key of XOR techniques.

The three algorithms MXORRSA, RSA and MXOR were implemented using Matrix laboratory (MATLAB R2012a). Files of sizes 1.465KB, 2.051KB, 2.930KB,6.446KB, 8.497KB, 9.083KB and 82.040KB consisting of text were used as input for encryption. The encrypted output of each file is saved as a file, which in turn is input for decryption. For sake of comparison the same input files for all algorithms were used throughout the experiment. The same system was used for all implementations and analysis work, so that memory and processor conditions remain same for all algorithms for comparison.

Each of the encryption techniques has its own strong and weak points. The following metrics under which the cryptosystems can be compared were used:

1. Encryption time: The time taken to convert plaintext to ciphertext is encryption time. Encryption time depends upon key size, plaintext block size and mode. In the experiment conducted, encryption time is measured in seconds. If the encryption time is less the system will be fast and responsive. If the encryption time is high the system will be slow and less responsive.

2. Encryption Throughput: The speed of encryption is calculated from throughput of the encryption (Anand & Appathurai, 2014) . Mathematically

$$\text{Throughput of encryption} = \frac{\text{Size of plaintext}}{\text{Encryption time}} \quad (2)$$

(Pratap, 2012).

3. Power Consumption: For computation of the energy cost of encryption, the same techniques as described in equation 2 is used. The basic cost of encryption is represented by the product of the total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The basic encryption cost is in unit of ampere-cycle. To calculate the total energy cost, divide the ampere-cycles by the clock frequency in cycles/second of a processor to obtain the energy cost of encryption in ampere-seconds. Then, multiply ampere-seconds by the processor's operating voltage to obtain the energy cost in Joule. That's, by using the cycles, the operating voltage of the CPU, and the average current drawn for each cycle, we can calculate the energy consumption of cryptographic functions. Then, the amount of energy consumed by the MXORRSA algorithm to achieve its goal (encryption or decryption) is given by:

$$E = V_{cc} * I * T \; Joules \quad (3)$$

For a given hardware V_{cc} is fixed. The encryption time, T, is considered the time that an encryption algorithm takes to produce a cipher text from a plain text, and I is the average current consumed per CPU cycle. For this experiment, the performance results were collected using a laptop that consumes approximate average current of 100mA when it is busy, and the CPU voltage is $V_{cc} = 1.25 \; volts$ (both collected from Intel Manual).

Throughput of the encryption algorithm and the power consumption algorithm are inversely proportional to each other. If there is an increase in the throughput of the encryption algorithm, there is a decrease in the power consumption algorithm (Anand & Appathurai, 2014).

Results and Discussions

This section discusses the results obtained based on three (3) evaluation parameters. Table 1 shows the comparative execution time of the algorithms with different packet sizes.

Table 1: Encryption time of MXORRSA, RSA and MXOR at different data sizes

DATA SIZE (bytes)	MXORRSA (s)	RSA (s)	MXOR (s)
1465	14	12.63	11.31
2051	17.54	18.06	15.61
2930	22.72	22.31	21.64
6446	49.09	49.85	49.14
8497	64.74	64.64	62.52
9083	67.94	67.1	66.97
82040	607.68	639.48	644.03

Table 2: Encryption throughput of MXORRSA, RSA and MXOR for various data sizes

Data Size Byte	MXORRSA (Byte/s)	MXOR (Byte/s)	RSA (Byte/s)
1465	104.64	129.53	115.99
2051	116.93	131.39	113.57
2930	128.96	135.40	131.33
6446	131.31	131.18	129.31
8497	131.25	135.91	131.45
9083	133.69	135.63	135.37
82040	135.01	127.39	128.29

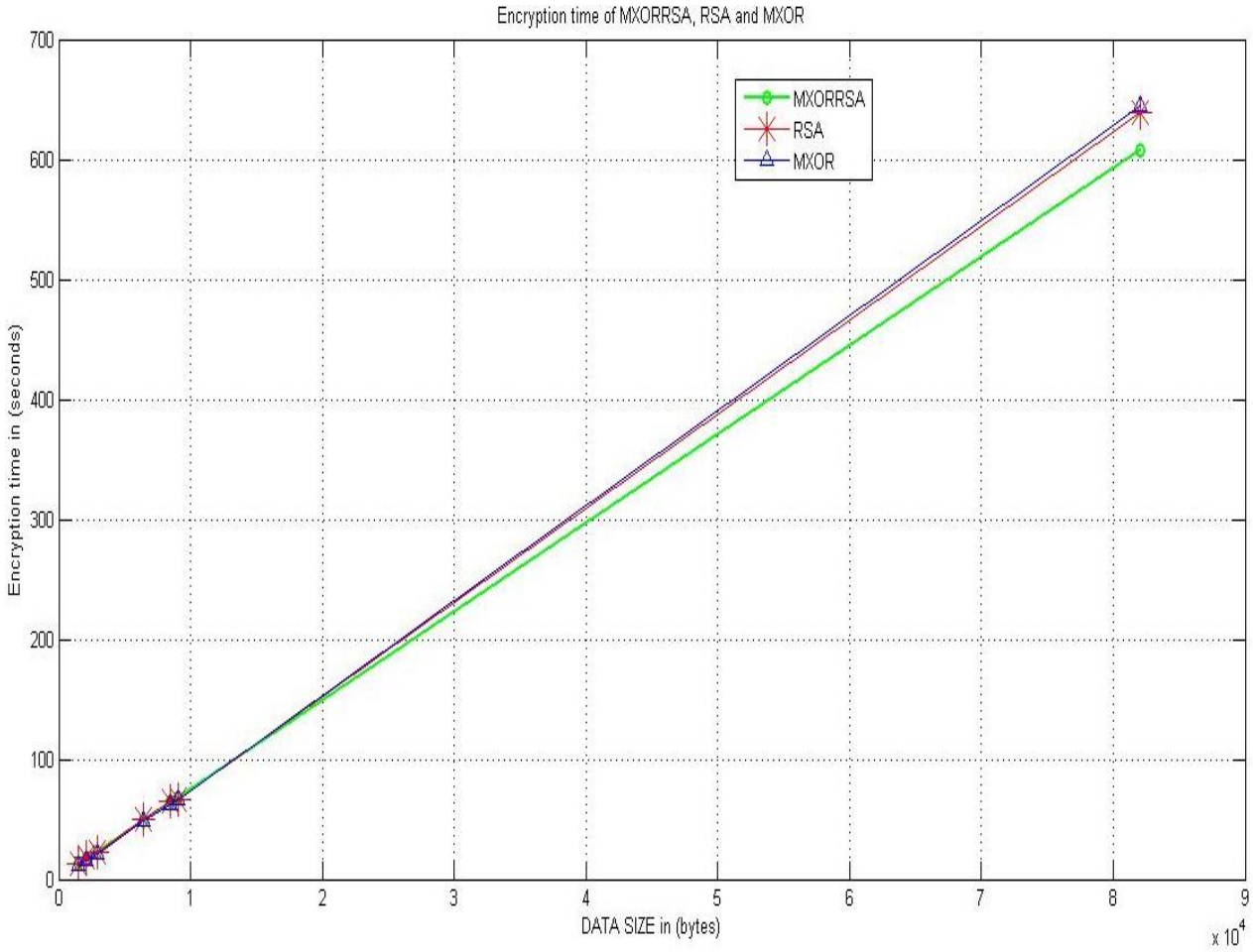

Figure 1: Graph of Data Size Vs Encryption time of MXORRSA, RSA and MXOR

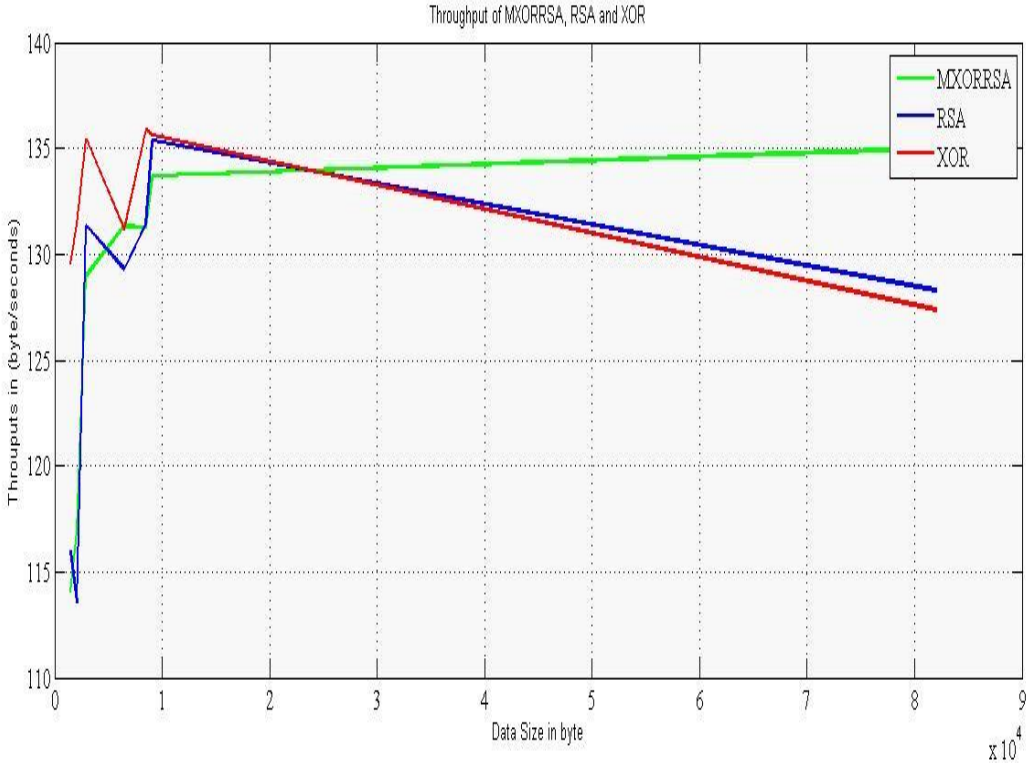

Figure 2: Graph of Data Size Vs Encryption Throughput of MXORRSA, RSA and MXOR

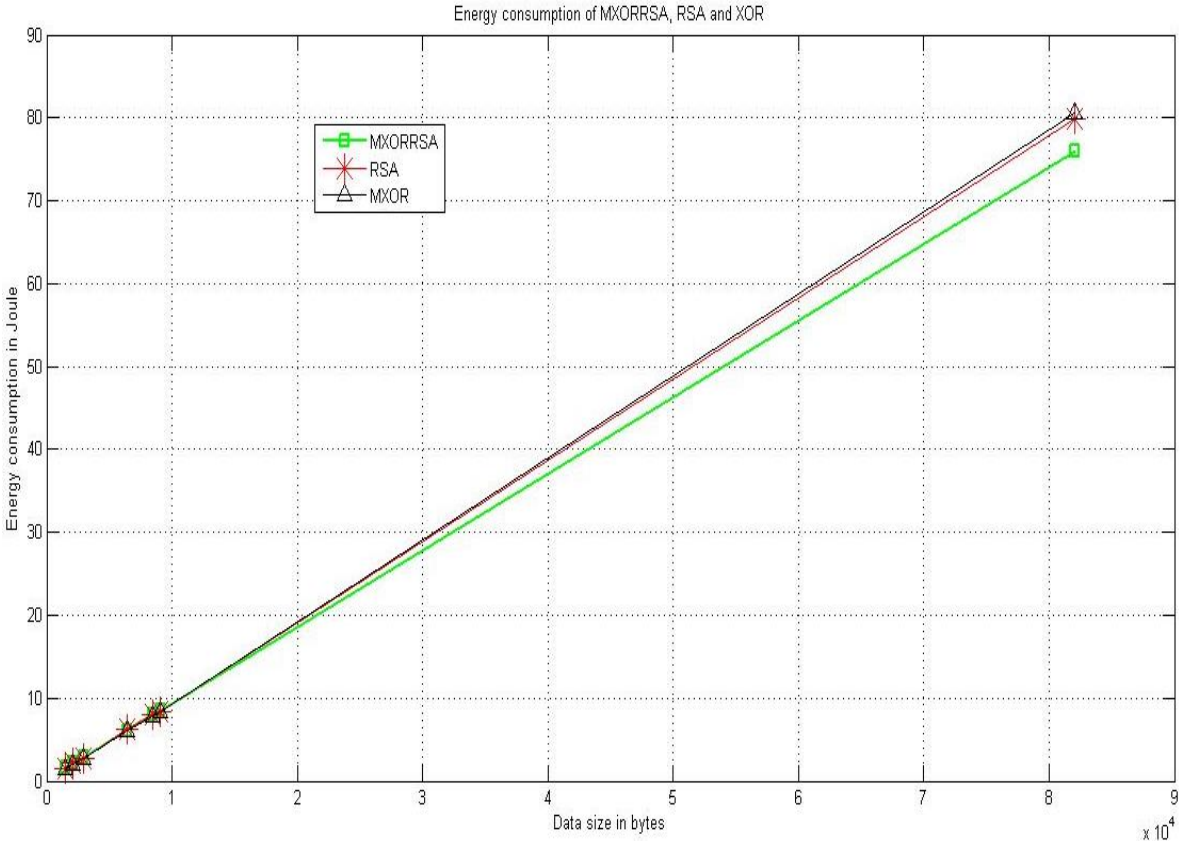

Figure 3: Graph of Data size vs energy consumption by Encryption process.

Table 3: Energy consumption of MXORRSA, RSA and MXOR for various data sizes

Data Size (KB)	MXORRSA E(J)	MXOR E(J)	RSA E(J)
1465	1.75	1.41	1.58
2051	2.19	1.95	2.26
2930	2.84	2.71	2.79
6446	6.14	6.14	6.23
8497	8.09	7.82	8.08
9083	8.49	8.37	8.39
82040	75.96	80.50	79.94

Figure 1 shows that the encryption time of the three algorithm increases as data size increases. It also shows that for large data sizes MXORRSA requires shorter time for encryption than RSA and MXOR.. Figure 2: Graph of Data Size Vs Encryption Throughput of MXORRSA, RSA and MXOR. Figure 2 is the graph of data in Table 2. It shows that for small size data the encryption throughput increases as data size increases for all the three algorithms until it reaches a pick where further increment in data size leads to decrease in encryption throughput. It can also be seen from the graph that for larger size data the encryption throughput of MXORRSA is higher than that of both MXOR and RSA. Figure 3 is the graph of table 3. It shows that the energy consumption increases as the data size increases. For larger data size the energy consumption of MXORRSA is lower than that of both RSA and MXOR.

Figure 3 is the graph of table 3. It shows that the energy consumption increases as the data size increases. For larger data size the energy consumption of MXORRSA is lower than that of both RSA and MXOR.

Conclusion

Each of the cryptography algorithm has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. From the experiment results, it is evident that MXORRSA algorithm has highest encryption throughput, lowest encryption time and consumes lowest amount of energy for large data sizes. On the other hand, RSA and MXOR algorithms have higher encryption throughput, lower encryption time and consume lower amount of energy than MXORRSA for smaller data sizes. Therefore, if the demand of an application is to encrypt data of smaller size, MXOR or RSA will be the right choice. If, however the demand of an application is to encrypt data of larger size, MXORRSA will be an appropriate choice.

Recommendation

Base on the results from the experiment carried out in this study, MXORRSA is recommended for users who need to encrypt files of larger sizes while either MXOR or RSA cryptographic algorithms are recommended for users need to encrypt files of smaller sizes.

REFERENCES

Alam, H., Biddu, H., Shafin, U., & Sharriar, I. (2016). Performance Analysis of Different Cryptography Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, 659-665.

Anand, K. M., & Appathurai, K. (2014). Performance analysis of Blowfish, IDEA and AES Encryption Algorithm. *Journal of Computer Science (JCS), 9*(1).

Nithya, B., & Sripriya, P. (2016). A Review of Cryptographic Algorithms in Network Security. *International Journal of Engineering and Technology (IJET), 8*(1), 324-331.

Oladipupo, E. T., Alade, O. A., & Afolabi, A. O. (2014). An Approach to Data Security Using Modified XOR Encryption Algorithm. *International Journal of Core Research in Communication Engineering, 1*(2), 1-9.

Pratap, C. M. (2012). Evaluation of Performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. *Journal of Global Research in Computer Science, 3*(8), 67-78.

Priyadarshini, P., Prsshant, N., Narayan, D., & Meena, S. (2015). A Comprehensive Evaluation of Cryptographic Algorithms:DES, 3DES, AES, RSA and Blowfish. *International Conference on*

Information Security and Privacy (ICISP2015) (pp. 617-624). Nagpur, India: Elsevier B.V.

Rachana, S. C., & Guruprasad, H. S. (2014). Emerging Security Issues and Challenges in Cloud Computing. *International Journal of Engineering Science and Innovative Technology (IJESIT), 3*(2).

Selin, C. C., Sujin, L. S., & Saranya, A. (2016). Evolution of cryptographic Algorithms and Performance Parameters. *Integrated Intelligent Research Journal of Scientific Research, 1*(1), 18-23.