IBBUL Lapai Journal of Applied and Natural Sciences

LAJANS Vol 7(1): 109-115

RESEARCH PAPER

A Comprehensive Evaluation of Hybrid Cryptographic Algorithms: AES, Blowfish, DES and IRSA

***[1]Abdulganiyu, A., [2]Hammawa, M.B., [2]Bisallah, H.I, and [3]Haruna, U.Y.**

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

ABSTRACT

In contemporary global networks, information security has become an important issue in data communication and there have been issues of high security challenges that have made many organizations to have limited interest in putting their data on cloud environment. Encryption algorithms plays an important role in information security system. This paper provides evaluation and in-depth study on hybrid of symmetric (AES, Blowfish, DES) as well as an improved asymmetric (IRSA) cryptographic algorithm by taking different file sizes. Evaluation parameters such as encryption time, decryption time and throughput were used to measure the efficiency of the proposed hybrid algorithm. Experimental results shows that AES is faster in terms g encryption when compared to other symmetric algorithms, So hybrid of IRSA With the AES makes it better and stronger.

Keywords: Symmetric, Asymmetric Keys, IRSA, BLOWFISH, DES, AES

INTRODUCTION

In these age and generation of fraudulent acts perpetrated by hackers of cryptosystem, there is need to review best methods to protect our data in a more centralised database. Cryptosystem helps protect our data from hackers or people that are not authorized to access our vital information. The science of converting our plain text messages to unreadable format is the function of cryptosystem, this will help in protecting our data from data bandits who attack information when it is being sent or by hacking into the database (Alanazi, 2010). Messages that can be read by everyone who come in contact with the plain text means the message is not secure, because it may be confidential which should not be read by unauthorized users, Therefore, we convert the message to an unreadable text which will look meaningless to the hackers. We do the manipulation of information into meaningless text using cryptographs. Cryptography converts plain text messages to cipher text messages applying encryption method and also use decryption method to convert it to readable text messages. It depends on a cryptographic algorithm which is applied during the system conversion. It is shown in figure 1 and figure 2 that there are two ways cryptographs operate.

Depending on the keys used in a cryptographic algorithm as shown in Fig.1 and Fig.2, They are basically sub divided into symmetric and asymmetric key cryptography. The symmetric cryptograph uses one single key to encrypt and decrypt text messages while asymmetric key cryptography uses different keys to encrypt the messages and uses another key for decryption to plain text message (Stergiou *et al*., 2018).

Received 7 July, 2022
Accepted 23 August, 2022
Address Correspondence to:
abdulg2009@yahoo.com;

Fig. 1: Symmetric Key Cryptography (Liu et al., 2017) `

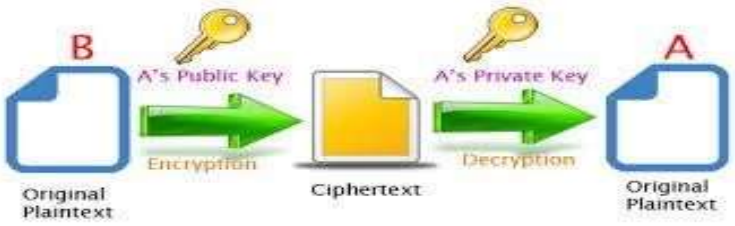

Fig. 2: Asymmetric Key Cryptography (Liu et al., 2017)

PROBLEM DESCRIPTION

The rate at which hackers make attempt to get access to unauthorized information are of great concern. Therefore, protecting and controlling accessibility to information on the internet is paramount, and to maintain their confidentiality. To make sure information confidentiality stand, we must enhance an asymmetric algorithm which will call the IRSA: It will compare and hybrid it with existing symmetric algorithm (Kamardan et al., 2018). The main attacks made on the web is purposely to hack into a client's account. With the help of cryptograph, in which, many data that could have been hacked are safeguarded by using cryptography. Big organizations are able to protect their information, but the bad guys are still working day and night to steal this information by researching on to how cryptograph works. We need to enhance one of the strongest asymmetric algorithms and then compare it with other symmetric algorithms to ensure possible hybrid of these symmetric algorithm that is faster in encryption time.

The symmetric algorithms that uses Advanced Encryptions Standard (AES), Data Encryptions Standard (DES), Blow Fish are used to enhance RSA algorithm which we call the inproved RSA algorithm (IRSA). In this algorithm, there is comparison of different file sizes which are applied just to find out the fastest encryption time. The comparison has been conducted for these algorithm time base on encryption time. We also simulate these algorithms to see the effectiveness of these algorithms.

COMMON ENCRYPTION ALGORITHMS

A.RSA

The asymmetric algorithm, RSA is a cryptosystem invented by three researchers Rivest, Shamir & Adelman when they were research students in the year 1978. RSA algorithm uses different scope cipher blocks and series of key are been applied. Asymmetric cryptosystem uses public key as a block cipher system based on number theory, RSA algorithm uses advantages of two prime numbers to generate both public keys and secret keys (Chinnasamy & Deepalakshmi, 2018). These keys are used for cipher and decipher of information when storing or sending the text message to a receiver. The originator of the message encrypts the text using receiver encryption public key, when the text message gets to the receiver at the other ends, then the receiver uses decryption key to unveil the message. RSA algorithm has three step processes, the first step is the key generation, this helps in creating encryption and decryption purpose. The second step is the encryption stage where public key is picked while the last stage is the decryption key which is used to convert the cipher text to readable text message (Chinnasamy & Deepalakshmi, 2018).

The IRSA uses four prime numbers instead of two prime numbers. This will advance the strength of our new algorithm.

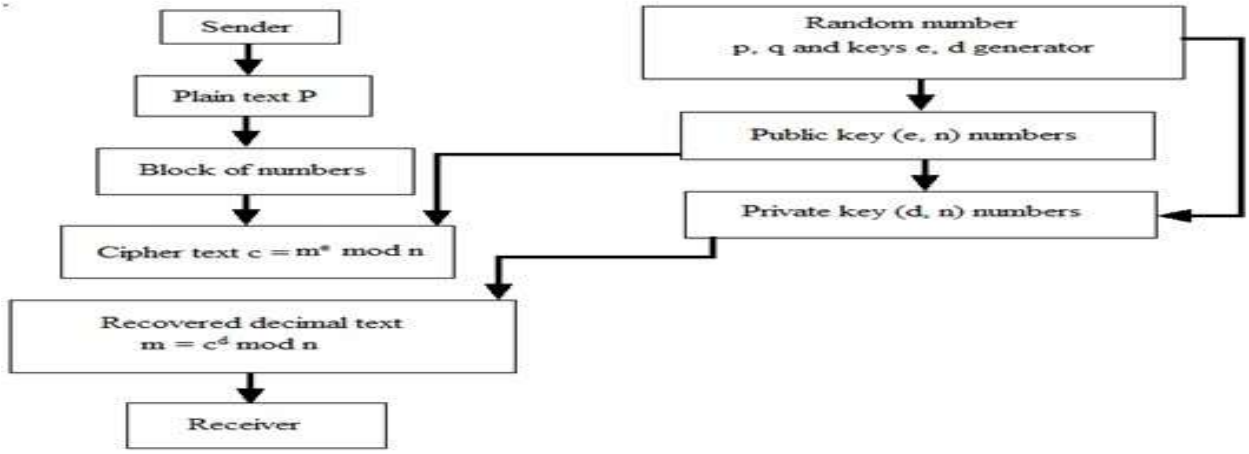

Fig.3: IRSA Algorithm

***Key Generation* of IRSA algorithm**

I. Insert four random selected large prime numbers f, g, h & i,
II. Get the product of these three prime numbers as n= f*g*h*i.
III. Calculate the result of phi, φ= (f - 1) *(g - 1) *(h - 1) *(i - 1), φ is the Euler's Totient Function
IV. We pick exponent of e which $1 < e < \varphi$ and gcd(e, φ) = 1
V. Manipulate d as private exponent $d = e^{-1} \bmod \varphi$
VI. key to be send as public key is (AbdElminaam, 2018), private key that will be use to decipher text is d. The ***Encryption*****:** $c = m^e \pmod n$ while ***Decryption***: $m = c^d \pmod n$.

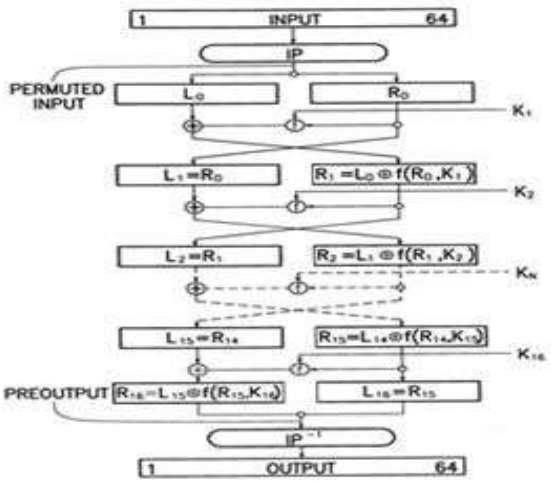

Fig. 4: DES Algorithm

DES

One of the symmetric algorithms is Data Encryption Standard (DES) key block encryption which has length key of 56 bits and it has a block space of 64-bit length. This algorithm was invented by a team of people in IBM company around 1974 and it was generally accepted as national standard for encryption in 1997 (Denis & Madhubala, 2021). One of the reason DES is generally accepted is because it has the capacity to operate in different modes CBC, ECB, CFB and OFB, making it elastic (MB Hammawa, 2019). The chart flow of DES algorithm is revealed in Fig.4.

AES

Advanced Encrypted Standard (AES) is a symmetric cryptograph that uses iteration cipher system. This algorithm was first future in the year 1998 by Vincent Rijmen and Joan Daemen. This algorithm supports variable length of key sizes of multiple of 32 bits, but only block size 128-, 192- and 256-bits keys are detailed as AES standard. (Denis & Madhubala, 2021). The whole 128 bits input block of the encryption system is organized as 4x4 bytes in array and we can call it subject to several rounds as display in Fig.5 where numerous revolutions take place. The length of key is determined by number of rounds; 14 rounds for 256- bit keys while 10 round for 128-bit keys.

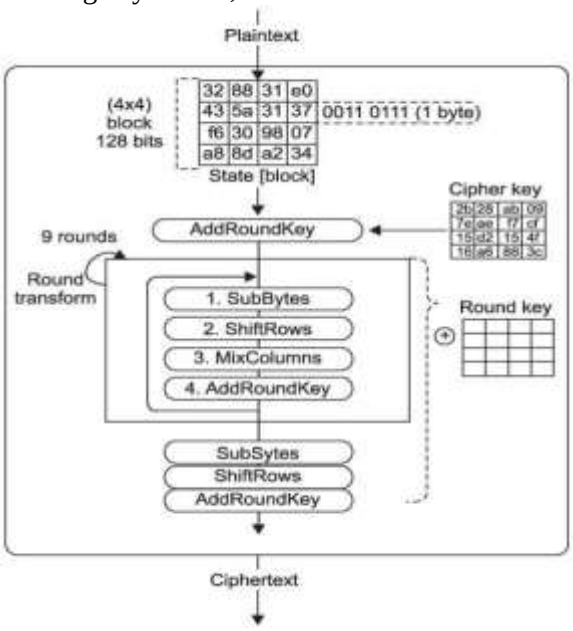

Fig. 5: AES Algorithm

BLOWFISH

Blowfish was introduced in 1993 by Bruce Schneier. This block cipher is a symmetric with a 64-bit length block size, it has a variable length key starting with 32-bits through 448 bits. Sometimes you can have 18 sub-keys which are resultants of single initial key (Islam, Islam, Islam, & Shabnam, 2018). In generating a require subkey we need a total of 521 iterations.

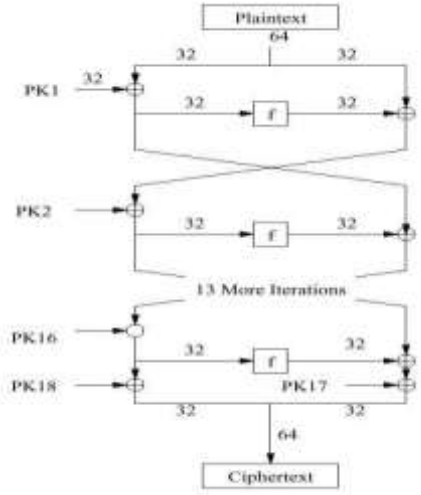

Fig. 6: Blowfish Algorithm

EXPERIMENTAL RESULTS AND ANALYSIS

Our experiment on these symmetric and asymmetric was conducted using three different files size. The matrices performance use: The *Encryption period.* This is the time taken to manipulate our text message to unreadable text message. When the period taken to convert to unreadable time is short that is a good case (Murad & Rahouma, 2022). This is the time in which the unreadable text messages are revert to readable text message which is called decryption time. *Throughput encryption algorithm, we calculate the mean average of the whole text message k bytes by* average encryption period. While throughput decryption algorithm the average of unreadable text message by average decryption period.

Results gotten from each calculation was inserted and graphs were plotted to get a conclusion from the results for inference. Java programing language is used to simulate the experiment. Our computer system uses windows operating system with 64bit and CPU 1.90GHz with a 6 GB of RAM. The information files size was randomly picked as 2MB, 4MB, 8MB and 12MB as the test subjects. The symmetric algorithms used were run in what we called cipher block chaining (CBC) approach with the key size of 64 bits and 128 bits**.** The encryption/decryption for each experiment was repeated about 10 epochs and the time requirement were noted for each experiment. The average period used was taken and computed for the calculation of throughput of each process.

TABLE I. Data table for Encryption runtime of Image Files

FILE	AES (msec)	DES (msec)	IRSA (msec)	BLOWFISH (msec)
2 MB	100.6	176.3	478.5	166.4
4 MB	170.3	242.0	681.5	250.0
8 MB	200.8	350.8	871.7	250.0
10 MB	290.6	477.4	887.1	376.3
12 MB	400.5	660.3	990.0	430.4

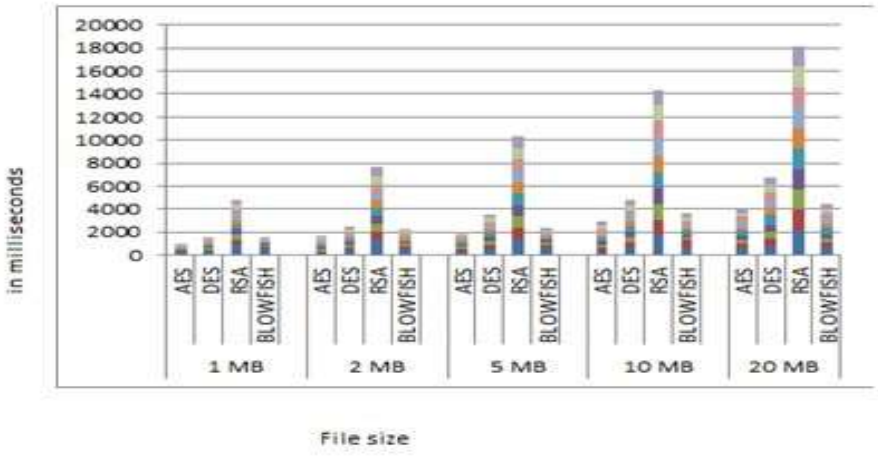

Fig. 7: Graph for Encryption runtime of Image Files

TABLE II. Data table for Decryption runtime of Image Files

FILE	**AES (msec)**	**DES (msec)**	**IRSA (msec)**	**BLOWFISH (msec)**
2 MB	155.8	145.2	4.0	61.5
4 MB	243.1	216.6	4.2	90.7
8 MB	301.0	400.8	4.6	121.8
10 MB	368.6	514.6	4.7	160.9
12 MB	445.4	666.9	4.6	211.5

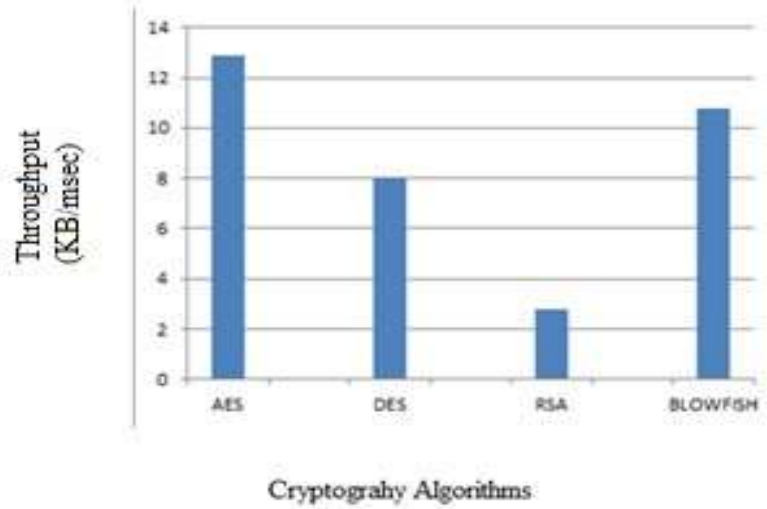

Fig.8: Graph for Decryption runtime of Image Files

TABLE III. Data table for Throughput of Image Files

FILE	AES (msec)	DES (msec)	IRSA (msec)	BLOWFISH (msec)
2 MB	100.6	101.3	451.5	456.4
4 MB	168.3	205.0	621.5	220.0
8 MB	216.8	316.8	701.7	240.0
10 MB	274.6	460.4	837.1	306.3
12 MB	400.5	609.3	881.6	400.4
AverageTime	1,160.8	1,692.8	3,493.4	1,623.1
Throughput (KB/ms)	232.16	338.56	698.68	324.62

The results in Table I and II determined that the AES algorithm takes less time to convert text messages to unreadable text files while IRSA takes less time to convert unreadable text files. This is shown in Fig.9. Throughput of AES is faster in case files encryption compare to other three algorithms.

CONCLUSION

From our evaluation performance of these symmetric algorithm, we have seen from our simulation that AES algorithm is faster in terms of encryption time, so it will be good for us to hybrid it with our IRSA algorithm which is fast in decryption time. This will enhance security and confidentiality of information to be sent through the appropriate channel and medium.

References

AbdElminaam, D. S. (2018). Improving the security of cloud computing by building new hybrid cryptography algorithms. International Journal of Electronics and Information Engineering, 8(1), 40-48.

Chinnasamy, P., & Deepalakshmi, P. (2018). Improved Key Generation Scheme of RSA (IKGSR) Algorithm Based on Offline Storage for Cloud Advances in Big Data and Cloud Computing (pp. 341-350): Springer.

Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 80(14), 21165-21202.

Hamdan.O.Alanazi, B. B. Z., A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani. (2010). New Comparative Study Between DES, 3DES and AES within Nine Factors. Journal of Computing and Applied Informatics, 2(3), 152-157.

Islam, M. A., Islam, M. A., Islam, N., & Shabnam, B. (2018). A Modified and Secured RSA Public Key Cryptosystem Based on “n” Prime Numbers. Journal of Computer and Communications, 6(03), 78.

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, J., Fan, C., Tian, X., & Ding, Q. (2017). Optimization of AES and RSA Algorithm and Its Mixed Encryption System. Paper presented at the International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

Hammawa, MB (2019). Strengthen Agriculture with ICT. Daily Trust, 35.

Murad, S. H., & Rahouma, K. H. (2022). Hybrid Cryptography for Cloud Security: Methodologies and Designs Digital Transformation Technology (pp. 129-140): Springer.

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.