A Comparative Analysis of Different Encryption Techniques of Cryptography

Md Imran Alam

Department of Computer Engineering & Networks, Jazan University, Jazan
Saudi Arabia
imran.amu2008@gmail.com

***Abstract*— Nowadays sharing the data or information over unsecured channel like internet is a very big challenge to computer users such as business, professionals and home users from the intruders. Any misuse or theft of data or information can be a huge loss for an individual person or for an organization. Hence we need some Encryption techniques to protect the shared data in an unsecured channel. Encryption is a technique which transforms the original data or message to some non readable format. This non readable data or message is called Cipher text. When this Cipher text reaches to the receiver side it again revert back to its original form, so receiver can read the message. For security of data we use so many Encryption techniques or Algorithms. This paper performs comparative Analysis of some of the Encryption Algorithms like DES, 3DES, AES, BLOWFISH and RSA. Algorithms has been compared on the following factors: input size of data, encryption time, decryption time , CPU time in the form of Throughput and battery consumption. If throughput value of an algorithm is increased then power consumption and battery consumption value of that algorithm is decreased and vice versa.**

***Keywords*— Encryption, Decryption, Algorithm, techniques, Cipher text, DES, 3DES, AES, BLOWFISH, RSA, Security, Throughput**.

I. INTRODUCTION

Cryptography plays a very important role in security of data. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the intended recipient. It basically hides the information.

Concepts used in Cryptography [10]

A. **Plain Text:** The original message that the person want to Communicate is defined as plain text

B. **Cipher Text:** The message which cannot be understood by anyone is defined as cipher text.

C. **Encryption:** Converting plain text to cipher text is referred as encryption. It requires two processes. Encryption algorithm and a key.

D. **Decryption:** Reverting cipher text to plain text is referred as decryption .This may also need two requirements Decryption algorithm and key. Figure 1 shows the simple flow of commonly used encryption algorithms.

E. **Key:** Combination of numeric or alpha numeric text or special symbol is referred as key. It may use at time of encryption or decryption .key plays a vital role in cryptography because encryption algorithm directly depends on it.[10]

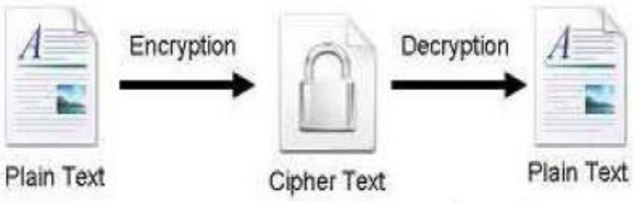


Figure-1: Encryption-Decryption Flow

Keys play a very important role in cryptography. If we use small keys then encryption algorithm will be weak. Anyone can break it easily. To make Algorithm strong we use large and complex keys.

Based on the keys we divide Cryptography in two parts. One is Symmetric key cryptography and other one is public key cryptography.

In symmetric key cryptography we use same key for encryption and decryption.

In Asymmetric key cryptography we use two keys: Private and public key. Public key is used for encryption and private key is used for decryption.

RSA is the name of Algorithm which is based on public key cryptography.

Symmetric key cryptography is further divided into two parts one is block Cipher and the second one is Stream Cipher.

- A block cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data at once as a group. Example of block ciphers are DES (Data Encryption Standard), AES (Advanced encryption standard) and Blowfish.
- Stream ciphers convert plaintext to cipher text one bit at a time. Example of stream cipher is RC4.

© 2013 IJAIR. ALL RIGHTS RESERVED

An overview of field of cryptography is as follows:[8]

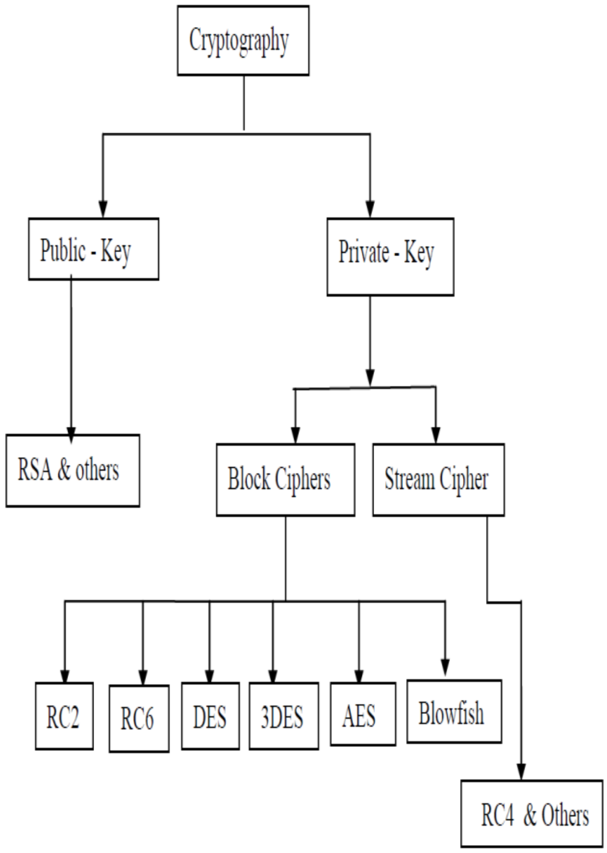


Figure 1 : Overview of the field of Cryptography

This paper is organized as follows: In section I Introduction part of cryptography is discussed. Section II covers the literature reviews. In section III the different types of Encryption algorithms are discussed. In section IV the various performance factors for the algorithms are given. In section V the results and the discussions are presented. With the section VI the final conclusion of paper is provided.

II. LITERATURE REVIEW

In this section various performance factors and Encryption techniques used by different papers are discussed.

Paper[3] presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. In the case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption.

In Paper[5] it is discussed that in symmetric key encryption techniques the AES algorithm is specified as the better solution then follows the blowfish algorithm. In the Asymmetric encryption technique the RSA algorithm is more secure key generation. since it uses the factoring of high prime number hence, the RSA algorithm is found as the better solution in this method.

In paper[6] it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Our future work will include experiments on image and audio data and focus will be to improve encryption time and less memory.

Paper[10] surveyed the existing encryption techniques like AES, DES and RSA algorithms along with LSB substitution technique. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm, but RSA consume more encryption time and buffer usage is also very high . We also observed that decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm

III.CLASSIFICATION OF ENCRYPTION ALGORITHMS

A. **DES (Data Encryption Standard)** is the most popular computer encryption algorithm. DES is a U.S. and international standard. It is a symmetric algorithm; the same key is used for encryption and decryption. “Reference[5] shows” Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses using a 56-bit. DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

B. **3DES:** In cryptography, Triple DES is the common name for the Triple Data Encryption algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple

© 2013 IJAIR. ALL RIGHTS RESERVED

method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. 3DES is slower than other block cipher methods. [8]

C. **AES:** The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001.”Reference [9] shows” that it is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemenand Vincent Rijmen, who submitted a proposal which was evaluated by the NIST during the AES selection process.

AES has been adopted by the U.S. government and is now used worldwide.

It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure-3.It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. Reference [10] shows” The following steps processed in AES algorithm.”Following steps used to encrypt a 128-bit block:

[i].Derive the set of round keys from the cipher key.
[ii].Initialize the state array with the block data (plaintext).
[iii].Add the initial round key to the starting state array.
[iv] Perform nine rounds of state manipulation.
[v].Perform the tenth and final round of state manipulation.
[vi].Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations . They are:
a. Sub Bytes : This operation is a simple substitution that converts every bite into a different value.
b. ShiftRows : Each row is rotated to the right by a certain number of bytes.
c. MixColumns : Each column of the state array is processed separately to produce a new column. The new column replaces the old one.
d. XorRoundKey :This operation simply takes the existing state array.

Decryption*:* Decryption involves reversing all the steps taken in encryption using inverse functions like InvSubBytes , InvShiftRows , InvMixColumns

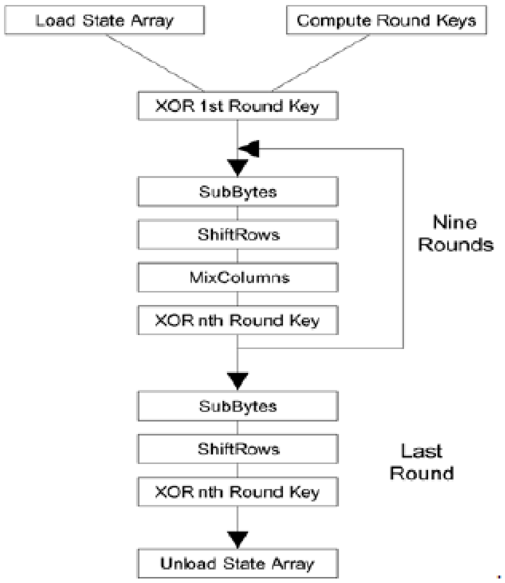


Figure 3. Flow of AES Algorithm

The above diagram is taken from [10]

D. **Blowfish:** Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products.

- Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. [1]
- Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.
- It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.
- It is a 16 round fiestel cipher that uses the large key size. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.[5]

E. **RSA:**This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It is the most popular public-key algorithm. It can be used for both encryption and digital signatures. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0and n1 for some n values. Size of n is considered 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key [15].

RSA algorithm:

- Select two different prime numbers p and q ,for security aim, the integers p and q must be prime numbers.

➢ Compute n = p*q

➢ Let m=(p-1)(q-1)

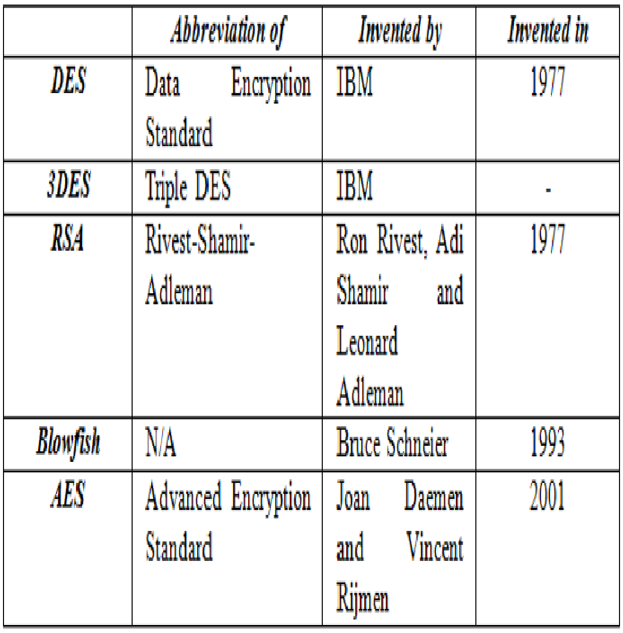
➢ Choose an integer *e*, co prime to m
➢ Compute the secret exponent *d*
➢ Such that de=(1+Nm) for N greater than equal to zero.

d=(1+Nm)/e

➢ The public key is (e,n) and the private key (d, n).
➢ Plain text message=P
➢ Cipher text: C =(P^e)MOD n
➢ Decrypted text=(C^d)MOD n

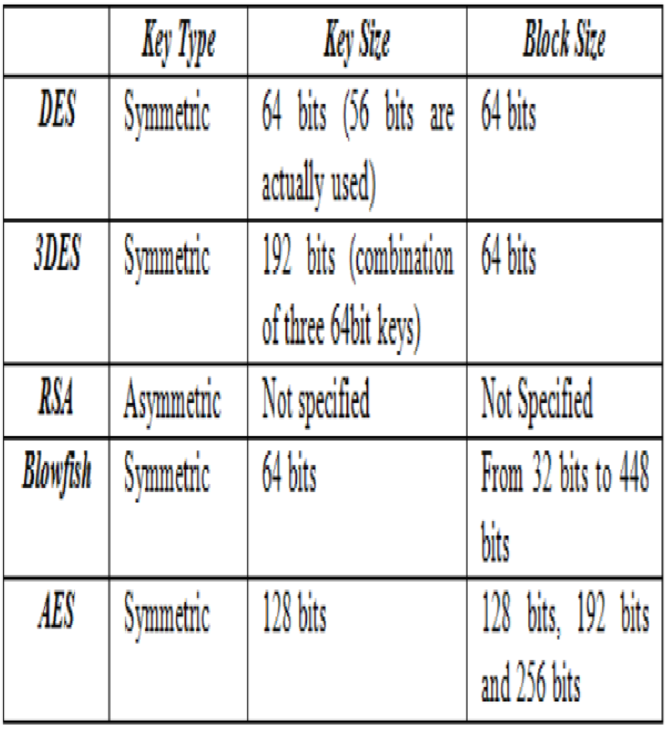
F. **Comparison based on basic Information as well as key and block size: TABLE 2 and TABLE 3 has been taken from[7]**

TABLE 2
BASIC INFORMATION COMPARISON



	Abbreviation of	*Invented by*	*Invented in*
DES	Data Encryption Standard	IBM	1977
3DES	Triple DES	IBM	-
RSA	Rivest-Shamir-Adleman	Ron Rivest, Adi Shamir and Leonard Adleman	1977
Blowfish	N/A	Bruce Schneier	1993
AES	Advanced Encryption Standard	Joan Daemen and Vincent Rijmen	2001

TABLE 3
KEY AND BLOCK COMPARISON



	Key Type	*Key Size*	*Block Size*
DES	Symmetric	64 bits (56 bits are actually used)	64 bits
3DES	Symmetric	192 bits (combination of three 64bit keys)	64 bits
RSA	Asymmetric	Not specified	Not Specified
Blowfish	Symmetric	64 bits	From 32 bits to 448 bits
AES	Symmetric	128 bits	128 bits, 192 bits and 256 bits

IV. PERFORMANCE FACTORS

In this paper, the following factors are used as the performance criteria, such as data size, the Encryption and decryption speed, Throughput of Encryption and Decryption and power consumption.

i. Input Size
ii. Encryption Time
iii. Decryption Time
iv. Throughput of Encryption of an Algorithm
v. Throughput of Decryption of an Algorithm
vi. Power Consumption

Experiments are conducted on different sizes of data in KB. A cryptographic tool is used for conducting such experiments.

© 2013 IJAIR. ALL RIGHTS RESERVED

Encryption time: The time which an algorithm takes to convert plain text to a cipher text is called encryption time.
Decryption time: The time which an algorithm takes to get plain text from a cipher text is called decryption time.

Throughput of an encryption: It is defined as total plain text in bytes divided by total encryption time.

Throughput of a decryption: It is defined as total plain text in bytes divided by total decryption time.

If throughput value of an encryption is increased then power consumption of that encryption is decreased.
Similarly if throughput of an encryption is decreased then power consumption of that encryption is increased and hence the battery consumption is also increased.

V. EXPERIMENTAL RESULTS & ANALYSIS

Experimental results for Encryption algorithms DES, 3DES, AES, BLOWFISH and RSA are shown in Table1 and Table 2.

Table 1: Comparisons of 3DES, DES, AES, BLOWFISH and RSA based on Encryption Time

Input Size (KB)	3DES	DES	AES	BLOWFISH	RSA
101	80	65	58	25	91
140	78	70	55	28	89
255	121	80	75	50	125
910	280	240	210	70	305
1000	310	270	205	69	410
5400	1302	1289	1250	150	1430
7350	1801	1705	1450	170	1910
Throughput	3.81	4.07	4.58	26.96	3.47

Table 2: Comparisons of 3DES, DES, AES, BLOWFISH and RSA based on Decryption Time

Input Size (KB)	3DES	DES	AES	BLOWFISH	RSA
101	70	58	50	22	82
140	80	56	55	30	79
255	98	71	65	41	112
910	230	210	190	58	260
1000	251	241	211	68	310
5400	1120	1020	945	125	980
7350	1502	1410	1140	135	1560
Throughput	4.52	4.94	5.70	31.64	4.48

Table 1 shows the encryption time of different algorithms based on input data of different sizes. In this table encryption throughput of different algorithms is also calculated.

Table 2 shows the decryption time of different algorithms based on input data of different sizes.
In this table decryption throughput of different algorithm is calculated.

After analyzing Table1 and Table 2, it is concluded that encryption and decryption time of RSA algorithm is much higher than encryption and decryption time of AES, DES, 3DES and BLOWFISH algorithm. We also noticed here that encryption and decryption time of BLOWFISH algorithm is the lowest as compared to AES, DES, 3DES and RSA.

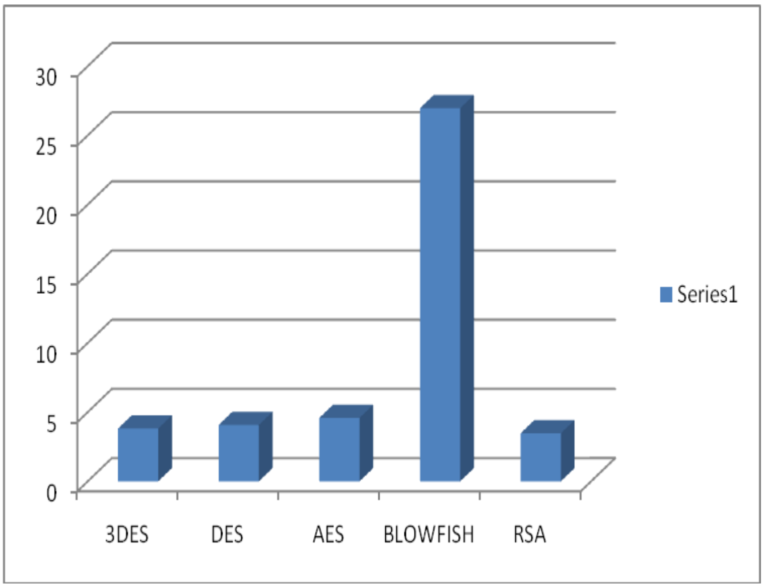


Fig. 1 Throughput of each Encryption Algorithm (Kilobytes/Second)

After analyzing Fig 1 we conclude that throughput of BLOWFISH algorithm is higher than throughput of all other algorithms like 3DES, DES, AES and RSA. It is also noticed here that AES algorithm has advantage over DES, 3DES and RSA algorithm in terms of the processing time.

© 2013 IJAIR. ALL RIGHTS RESERVED

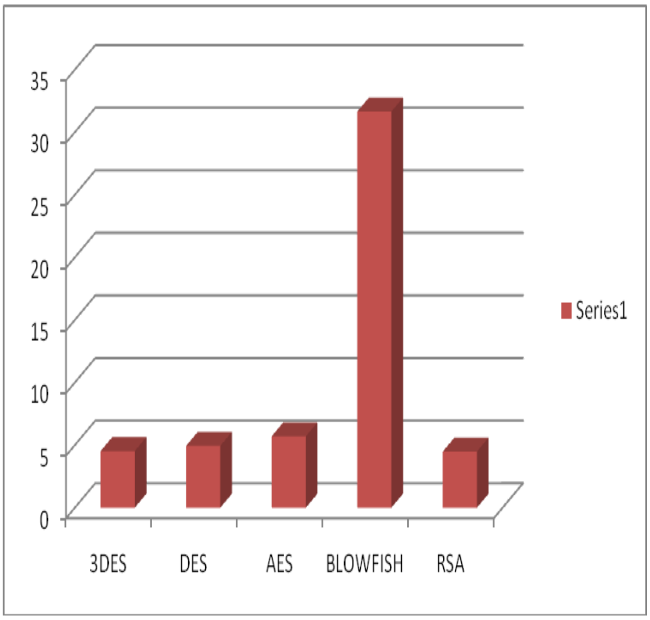


Fig. 2 Throughput of each Decryption Algorithm (Kilobytes/Second)

By analyzing fig. 2, it is noticed here that BLOWFISH algorithm is far better than other algorithms (3DES, DES, AES and RSA) based on throughput value. It is also noticed that DES is better than 3DES. Throughput value of AES is higher than DES, 3DES and RSA algorithm but lesser than BLOWFISH algorithm.

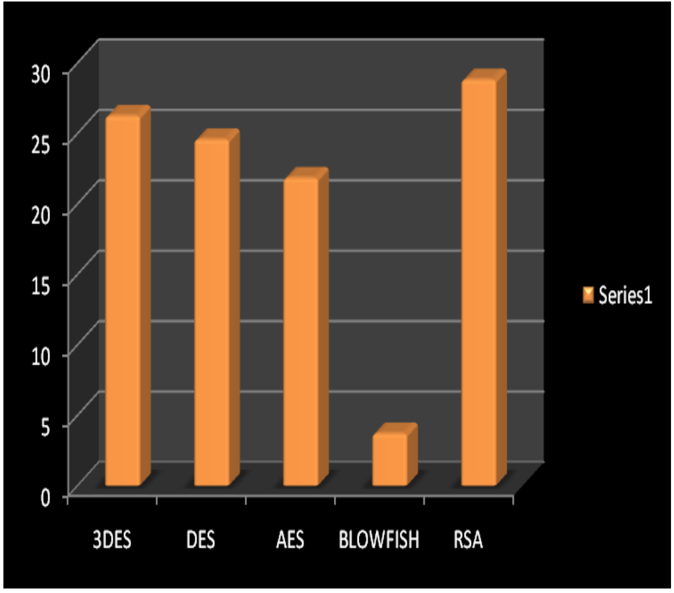


Fig. 3 Power consumption (μ Joule / Byte)

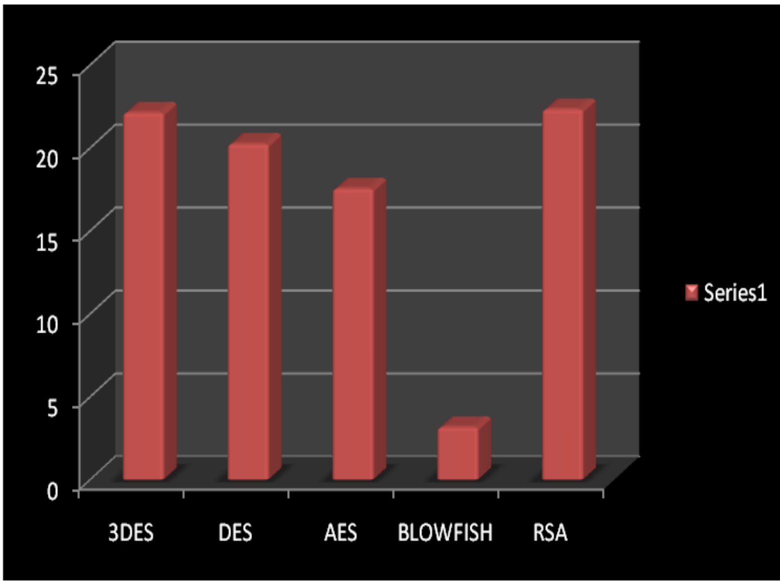


Fig. 4 Power consumption (% Battery consumed)

By analyzing Fig. 3 and 4, we conclude here that power consumption and battery consumed value of BLOWFISH algorithm is the lowest as compared to 3DES, DES, AES and RSA algorithms. It is also noticed here that power consumption and battery consumed value of RSA algorithm is the highest.

VI. Conclusions

This paper is the comparative analysis of existing Encryption algorithms like DES, 3DES, AES, RSA and BLOWFISH. By analyzing experimental results it was concluded that BLOWFISH algorithm takes least encryption and decryption time as compared to DES, 3DES, AES and RSA algorithms. Throughput value of BLOWFISH is the highest as compared to DES, 3DES, AES and RSA algorithms. Power consumption value of AES is higher than BLOWFISH but lesser than DES, 3DES and RSA algorithms. Encryption and decryption time as well as power consumption value of RSA algorithm is the highest as compared to DES, 3DES, AES and BLOWFISH algorithm. When we compare DES with 3DES than we find that DES is better than 3DES.

From the experimental results, we finally conclude that BLOWFISH algorithm is better than all other algorithms discussed here like DES, 3DES, AES and RSA.

© 2013 IJAIR. ALL RIGHTS RESERVED

ACKNOWLEDGMENT

The author would like to thank to all authors that are listed below in the reference lists as well as anonymous reviewers for their valuable comments and suggestions that improved the presentation of this paper.

REFERENCES

[1] Bruce Schneier. The Blowfish Encryption Algorithm, Retrieved October 25, 2008,http://www.schneier.com/blowfish.html

[2] W. Stallings. Cryptography and Network Security, Prentice Hall, 1995.

[3] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader,Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.

[4] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, vol 2,no.1,January 2011.

[5]AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram" COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS " International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

[6] Shasi Mehlrotra seth, Rajan Mishra " Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011

[7] Ali Makhmali, Hajar Mat Jani" Comparative Study On Encryption Algorithms And Proposing A Data Management Structure"INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 6, JUNE 2013 ISSN 2277-8616

[8] Pratap Chnadra Mandal' Superiority of Blowfish Algorithm" International Journal of Advenced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201

[9] . http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[10]B. Padmavathi1, S. Ranjitha Kumari2 "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064Volume 2 Issue 4, April 2013 www.ijsr.net

[11] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers" International Journal of Engineering and Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66

[12] RSA Cryptography Specifications http://www.rsa.com http://www.ietf.org

[13] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs – September 27-28, 2001- Newton, Massachusetts.

[14] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."I BM Journal of Research and Development, May 1994,pp. 243 -250.

[15] Atul Kahte"Cryptography and Network Security, 2nd Ed"