ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm

Srinivas B.L [1], Anish Shanbhag[2], Austin Solomon D'Souza[2].

Assistant Professor, Department of IT, AIMIT, St Aloysius College, Mangalore, India

M.Sc.(Software Technology), AIMIT, St Aloysius College, Mangalore, India

ABSTRACT: With the fast change in technologies today, more and more multimedia data are generated and transmitted, leaving our data vulnerable to be edited, modified and duplicated. Because of the significance, accuracy and sensitivity of the information it is a big security and privacy issue, making it necessary to find appropriate solution. Security and privacy has become an important concern. This paper provides comparative analysis of symmetric key cryptography algorithms DES and BLOWFISH with variation of parameters like different data types, data size and key size. The experimental work was performed on DES and BLOWFISH Algorithm, to illustrate the performance of this algorithm by changing some of these parameters. The execution time as a function of the encryption key length and the file size was examined; this has been stated as complexity and security. Various data types were analyzed and the role of the data types was also emphasized.

KEYWORDS: DES, Blowfish, data type, data size, ECB, CFB, encryption time and throughput.

I. INTRODUCTION

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage called Encryption process. The reverse of data encryption process is called data Decryption.

Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography it is widely used today [4].

II. GOALS OF CRYPTOGRAPHY

1. **Confidentiality**
   Nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contact only by the authorized party and not by unauthorized person [5].
2. **Authentication**
   This process is proving a one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from an authorized person or unauthorized person or wrong identity.
3. **Integrity**
   Only the authorized party is modifying the transmitted information or message. Nobody can change the given message.
4. **Non Repudiation**
   This is a mechanism to prove that the sender really sent this message. So if any sender denies that he doesn't send the message; this method not allows doing such type of action to sender.
5. **Access Control**
   Only the authorized parties are capable to contact the given information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

1.2. SECURITY AGAINST ATTACK:

Cryptanalysis is an art and science of breaking the encrypted codes that are created by applying some cryptographic algorithm. Cryptanalysis attacks can classify the following:

1. **Cipher text-only attack**
   In cipher-text only attack, the attacker has a part of the cipher text using available information, the attacker tries to find out the corresponding key and decrypt the plain-text [6].
2. **Known-plaintext attack**
   The known- plaintext attack (KPA) is an attack model for cryptanalytic wherever the criminal has samples of each the plain-text and its encrypted version cipher-text. These will be revealing any secret data like secret keys and code books.
3. **Chosen-plaintext attack**
   A chosen- plain-text attack (CPA) is an associate attack model for cryptography that presumes the potential to decide on arbitrary plain-text to be encrypted and procure the corresponding cipher-text.
4. **Chosen-cipher text attack**
   A chosen- cipher-text attack (CCA) is an attack model for scientific discipline within which the cryptologist gathers data, a minimum of partially, by selecting a cipher-text and getting its decipherment beneath an unknown key.
5. **Chosen-text attack**
   A chosen text attack is a combination of choosing plain-text and chosen cipher-text attack [6].
6. **Brute-force attack**
   This type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. This is the very slow attack. Suppose that message is encrypted using the 56-bit key then the attacker can try all the possibilities up to 255 bit [5].
7. **Dictionary attack**
   The extension to the Brute-force attack is the Dictionary attack. In the Dictionary attack, it will try also same possibilities but take only those key bit whose chances of success is more [5].
8. **Timing attack**
   Timing Attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Each consistent operation in a computer takes time to perform [5].
9. **Man-in-the-middle attack**
   This is the type of active attack. This differs from the above in that it involves tricking individuals into compromise their keys. The attacker is placed in the two parties through communication channel who wish to exchange their keys for secure communication [5].

III. TYPES OF CRYPTOGRAPHY

There are several ways to classify the cryptography algorithms. The most common types are [4]:

- Secret Key Cryptography this is also called as Symmetric Key Cryptography
- Public Key Cryptography this is also called as Asymmetric Key Cryptography

2.1. Symmetric Cryptography:

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. In the block cipher mode the whole data is divided into number of blocks. These data is based on the block length and the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. The performance evaluation is taken place for the following symmetric key encryption techniques such as The DES Algorithm and Blowfish algorithm [7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

2.1.1. Data Encryption Standard

[16] DES is a symmetric key algorithm which was developed by IBM in 1977. It uses block size 64 bit Key size 56 bits. The DES is a block cipher algorithm which uses 56-bit (with 8-bit additional parity bits) key to encipher the plain text. The key looks like 64-bits, but 1 bit in each octet is used for odd parity so actual key is of 56-bits only [13]. DES uses series of substitutions and permutation on each block of plain text which is of 64-bit in size, which is then EX-OR with input. Above process is repeated 16 times with different sub keys, Sub-keys are the keys formed by taking different order of the key bits each time. Because of 16 rounds the DES algorithm becomes more secure [14]. Decryption is done in a reverse way as that of encryption by using the same key used at the sender's end, since it is symmetric algorithm. Very high throughput rates can be achieved i.e. up to 100Mbits/sec can be implemented on economical hardware. DES is said to be had known key problems. In DES, the key consist of 56 bits which gives space of 256=7.2058 X 1016 elements. In an exhaustive search known plain-text attack, the attacker will obtain the solution after 255 trials on an average. Key used in DES itself can sometimes make work easy for attacker. In situation like when all sub-keys are same then at the end of 16-rounds we will get plain text only instead of cipher text [15]. There are many attacks which can exploit the weaknesses of DES, which makes this algorithm insecure [13]. The number of rounds is exponentially proportional to the amount of time and fined a key using a brute-force attack. Therefore the number of rounds increases then the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks [9].

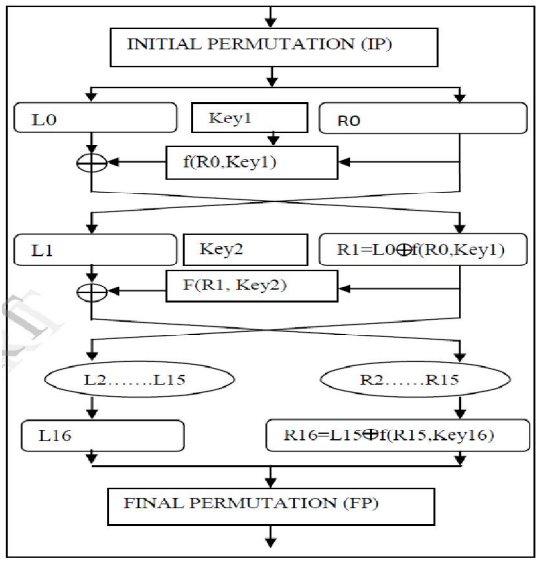


Figure 1: DES algorithm

2.1.2. Blowfish Algorithm

Bruce Schneider designed Blowfish in v as a fast alternative to existing encryption algorithms [16]. Blowfish is a symmetric encryption algorithm, means that it uses the same secret key (private key) to both Encrypt and decrypt messages or data. Blowfish is also called as block cipher, means that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits. Messages which are not multiple of eight bytes in size must be padded. It takes a variable-length key from 32 bits to 448 bits. Blowfish consists of two parts: Data encryption and key-expansion [17]. Blowfish came into existence in order to allow anyone to use encryption free of patents and copyrights. No attack is known to be successful against it. Blowfish has remained in the public domain to this day [18]. Blowfish has 16 rounds. Blowfish Algorithm is a Feistel Network, a simple encryption function is iterated 16 times. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [19]. Due to the speed of the algorithm is more the throughput is also more. The power consumption is also less. Added functionality of key expansion makes it hard to crack. It suffers from weak keys problem. BLOWFISH is better than AES, DES, 3DES in terms of throughput and processing time [8]. BLOWFISH encrypts audio files at less speed. It also encrypts image most efficiently on windows xp, vista and 7 in comparison

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

with AES [20]. The key size is larger as it is difficult to break the code in the blowfish algorithm. Additionally it is exposed to all the attacks apart from the weak key class attack.

Blowfish is designed to meet the following design criteria [24].
1. Fast. Blowfish encrypts data on 32-bit microprocessors at a rate of 26 clock cycles per byte.
2. Compact. Blowfish can run in less than 5K of memory.
3. Simple. Blowfish uses only simple operations: addition, XORs, and table lookups on 32-bit operands. Its design is easy to analyze which makes it resistant to implementation errors.
4. Variably Secure. Blowfish's key length is variable and can be as long as 448 bits. Blowfish is optimized forapplications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than DES when implemented on 32-bit microprocessors with large data caches, such as the
Pentium and the PowerPC.Blowfish is not suitable for applications, such as packet switching, with frequent key changes, or as a one-way hash function. Its large memory requirement makes it infeasible for smart card applications [12].

These are the following steps of blowfish encryption algorithm-

- X is 64 bits input data
- X is divided into two equal parts x1 and x2
- for i=0 to 15
  x1= x1 xor Pi
  x2– f(x1) xor x2
- swap x1 and x2
- swap x1 and x2 (undo the previous swap)
- x1= x2 xor P18
- x2=x2xor P17
- combine x1 and x2

2.2Asymmetric Cryptograph

Asymmetric key encryption is the technique, in which the different keys are for the encryption and the decryption process. One key is public (published) and second is kept private. They are also called as the public key encryption. If the lock/encryption key is first published then the system enables private communication from the public to the unlocking key's user [8]. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private Algorithm. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted. For the following algorithms the performance factors are evaluate.

3. Modes on Block cipher
Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers [10]. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so called because the scheme encrypts one block of data at a time using the same key on each block. Block ciphers can operate in one of several modes.

3.1 The four most important modes:

3.1.1. Electronic Codebook (ECB): This mode is the simplest and most obvious application. The secret key is used to encrypt the plaintext block to form a cipher text block. Two identical plaintext blocks, then, will always generate the same cipher text block. Although, this is the most common mode of block ciphers, it is vulnerable to a variety of brute-force attacks.
3.1.2. Cipher Block Chaining (CBC): This mode adds a feedback mechanism to the encryption scheme. In CBC, theplaintext is exclusively–OR'ed (XOR'ed) with the previous cipher text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same cipher text.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

3.1.3. Cipher Feedback (CFB): This mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block is transmitted. At the receiving side, the cipher text is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.

3.1.4. Output Feedback (OFB): This mode is a block cipher implementation conceptually similar to a synchronousstream cipher. OFB prevents the same plaintext block from generating the same cipher text block by using an internal feedback mechanism that is independent of both the plaintext and cipher text bit streams [11].

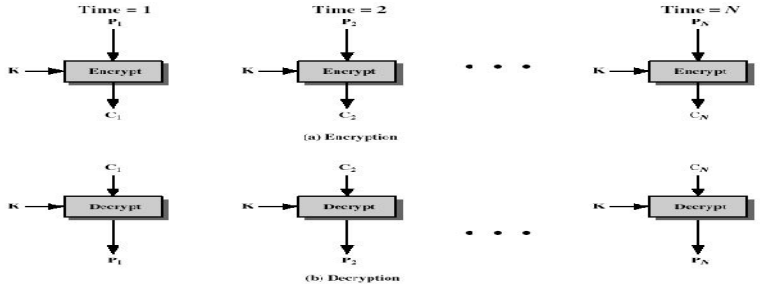
IV. DES USING ECB AND CFB

4.1 ECB (Electronic Codebook)[22]

- Message is broken into independent blocks which are encrypted
- Each block is encoded independently of the other blocks Ci = DESK (Pi)
- Applications
  – secure transmission of single values
  – Databases (retrieval of single fields)

4.1.1 ECB – Pros and Cons

- Weakness - encrypted message blocks are independent
- Strength – in some applications the independence of message blocks is very useful
  – Databases
  – Parallelizing encryption / decryption



4.2 CFB (Cipher Feedback Mode) [22]

- Message is treated as a stream of bits
- Added to the output of the block cipher
- Result is feedback for next stage (hence name)
- Standard allows any number of bit (1, 8 or 64 or whatever) to be feed back
  – denoted CFB-1, CFB-8, CFB-64 etc.
- CFB-64 is used most often (most efficient)
  Ci = Pi XOR DESK (Ci-1)
  C0 = IV
- Applications: stream data encryption, authentication

4.2.1 CFB – Pros and Cons

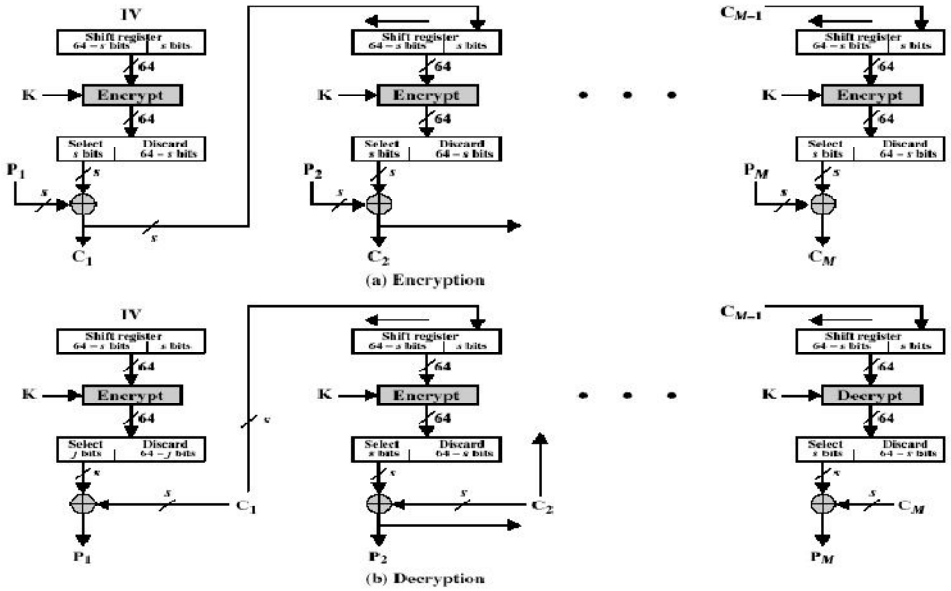
- Appropriate when data arrives in bits/bytes
- Most common stream mode
- Block cipher is used in encryption mode at both ends!
- Errors propagate for several blocks after the error (depending on s**)**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014



V. BLOWFISH USING ECB AND CFB

5.1 ECB (Electronic Codebook) [21]

In ECB mode, each plaintext block is encrypted independently with the block cipher.

Encryption:

Ci ←EK (Bi)

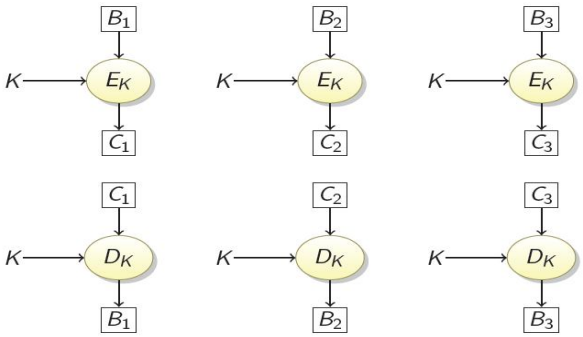
Decryption:

Bi ←DK (Ci)

Notation:

Bi is the i: th plaintext block.

Ci is the i: th cipher text block.



5.1.1 Pros and Cons

Pros:

Simple.

Tolerates blocks lost in transit.

Easy to parallelize**.**

Cons:

Identical plaintext blocks (e.g. blocks of sky in a jpg) result in identical cipher text ⇒ data patterns aren't hidden.

Not suitable for encrypting message longer than one block.

Example [23]: The Phantasy Star Online: Blue Burst online video game uses Blowfish in ECB mode. Before the key exchange system was cracked leading to even easier methods, cheaters repeated encrypted monster killed message packets, each an encrypted Blowfish block, to illegitimately gain experience points quickly.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

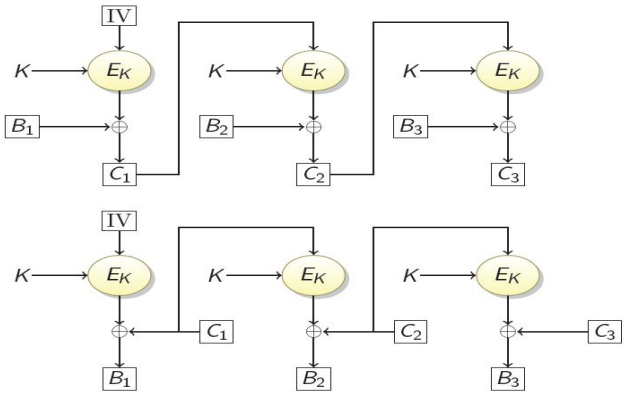
(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

5.2 Cipher-Feedback [21]

In CFB mode, the previous cipher text block is encrypted and the output produced is combined with the plaintext block using XOR to produce the current cipher text block.
CFB can use feedback that is less than one full data block.
An initialization vector IV is used as a seed for the first block.

Initialization:
C0 ← IV
Encryption:
Ci ← EK (Ci−1) ⊕ Bi
Decryption:
Bi ← EK (Ci−1) ⊕ Ci



5.2.1 Pros:
CFB mode is self-synchronizing similar to CBC.
Decryption can be parallelized.
Decryptor is never used.

Cons:
Encryption cannot be parallelized.
When decrypting, a one-bit change in the cipher text corrupts the following 2 plaintext blocks.
When decrypting, a one-bit change in the plaintext block, corrupts 1 following plaintext block.

VI. SUMMARY TABLE ON SYMMETRIC ALGORITHMS OF DES AND BLOWFISH

FACTORS	DES	BLOWFISH
KEY LENGTH	56 BITS	32-448 BITS
CIPHER TYPE	SYMMETRIC BLOCK CIPHER	SYMMETRIC CIPHER ALGORITHM
BLOCK SIZE	64 BITS	64 BITS
DEVELOPED	1977	LEAKED IN 1996, DESIGNED IN 1987
CRYPTANALYST RESISTANCE	VULNERABLE TO DIFFERENTIAL AND LINEAR CRYPTANALYSIS: WEEK SUBSTITUTION TABLES BRUTEFORCE ATTACK	VULNERABLE TO DIFFERENTIAL, BRUTE FORCE ATTACKER,DICTIONARY ATTACK
SECURITY	PROVEN INADEQUATE	VULNUERABLE
POSSIBLE KEYS	2^{56}	2^{32},2^{448}
POSSIBLE ASCII PRINTABLE CHARACTER KEYS	95^{7}	95^{4},95^{56}
TIME REQUIRED TO CHECL ALL POSSIBLE KEYS AT 50 BILLION KEYS PER SECOND	FOR A 56-BIT KEY 400 DAYS	FOR A 448-BIT KEY 10^{116} YEARS
ROUNDS	16	16
THROUGHPUT	LOWER THAN BLOWFISH	VERY HIGH
KEY(S)	SINGLE	PUBLIC
ENCRYPTION RATIO	HIGH	HIGH
POWER CONSUMPTION	HIGH	VERY LOW
SPEED	FAST	FAST
#S BOXES	8	4

Table 1: Summary of DES and Blowfish algorithm with different Factors.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

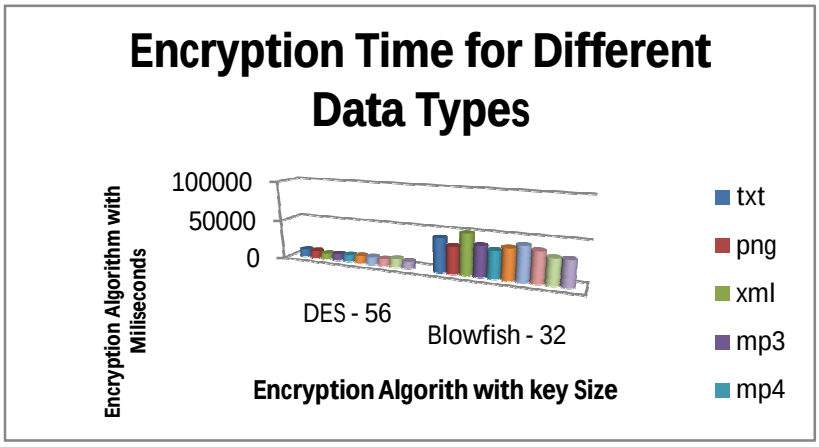
VII. EXPERIMENTAL SETUP AND TESTING

The execution results are taken on machine having Intel® Core™ i3-3120M (2.50 GHz) processor with Intel® Q65 Express 4 GB 1333 MHz DDR3 (RAM) and Microsoft Windows8.1 Pro operating System. The Eclipse IDE is used for implementation.JCE (Java Cryptography Extension) and JCA (Java Cryptography Architecture) are used for cipher algorithm implementation. The JCA is a major platform that contains ”provider" architecture and the set of APIs for encryption (symmetric ciphers, asymmetric ciphers, block ciphers, stream ciphers), message digests (hash), digital signatures, certificates and certificate validation, key generation and secure random number generation. Here we have used sun and Bouncy Castel provider for implementing cryptographic algorithms.

The brief analysis of different symmetric key cryptographic algorithm for various parameters is as follows [23]:

7.1 Files with different data types.

This case study has taken to check whether the encryption has dependency on type of data. Different data type files like audio, image, textual and video of nearly 50MB in size are chosen and encryption time of different cipher algorithms is calculated for these data types. For all executions of a specific cipher algorithm, varying parameter is data type and constant parameters are key size and block cipher mode. Key size and block mode are at kept at bare minimal parameters. The key size of DES and Blowfish are kept at minimum values as 128, 56, 112, 40, 32, 80 and 40 bits respectively. Block cipher mode used is ECB with PKCS#5 padding scheme. Fig. 1 shows the execution time of the algorithms for different data type files.



Observation: The result shows that the encryption time does not vary according to the type of the data. Encryption depends only on the number of bytes in the file and not on the type of file. DES works faster than other block ciphers. DES with key size 56 is fastest among the algorithms tested.

7.2 Data files of same type with different size

This case study is taken to ensure once again the observations obtained in case study 1. Case study 1 revealed that encryption time depends on number of bytes in the file. To ensure this another study is made in which different files of same types but different sizes are given for encryption and estimated the encryption time. For all executions key size and block mode are kept at bare minimal parameters. Table 2 gives the details about the files used for all executions and Fig. 2 and 3 show the execution results.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

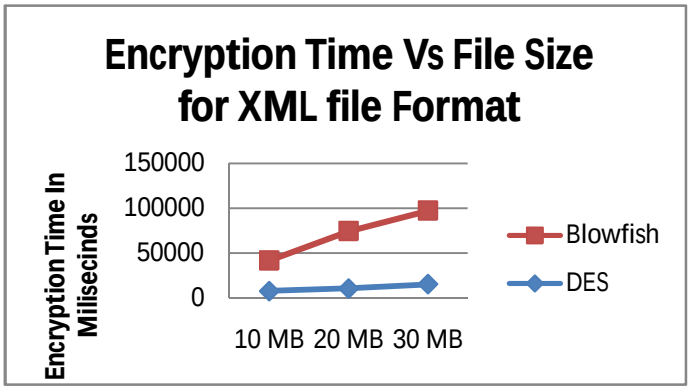
International Journal of Innovative Research in Computer and Communication Engineering

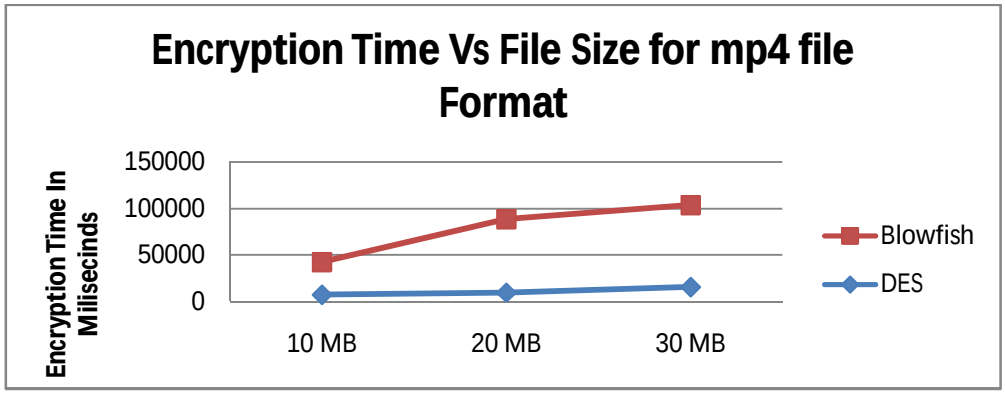
(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

Table 2.Execution Parameters for files of different size

File Type	Varying Parameters (Data Size)	Constant Parameters
XML	10MB, 20MB, 30MB	Data Type, Key Size
MP4		





File Type	Size (In MB)	Encryption Time in Millisecond	
		DES	Blowfish
	key	56	32
XML	10	7566	34010
	20	10424	64195
	30	15211	82230
MP4	10	7714	34917
	20	9858	78684
	30	15807	87877

Table 3: Files of Different Sizes and its execution time.

Observation: From the results in Table 3 and Fig. 2 and 3 we can find that the result for different size of data varies proportional to the size of data file. Encryption time increases as file size increases in multiples of data size. For each encryption algorithm same parameters are used for files of different sizes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

7.3 Encryption algorithm with different key sizes

This case study is to analyse the effect of changing the size of encryption key on encryption time. WAV file of 50MB is taken and different cipher algorithms are executed for different size of keys supported by them in ECB mode with PKCS#5 padding scheme. The various key sizes mentioned in Table 1 are used during experimentation. Fig. 4 shows the result of execution for key size variation

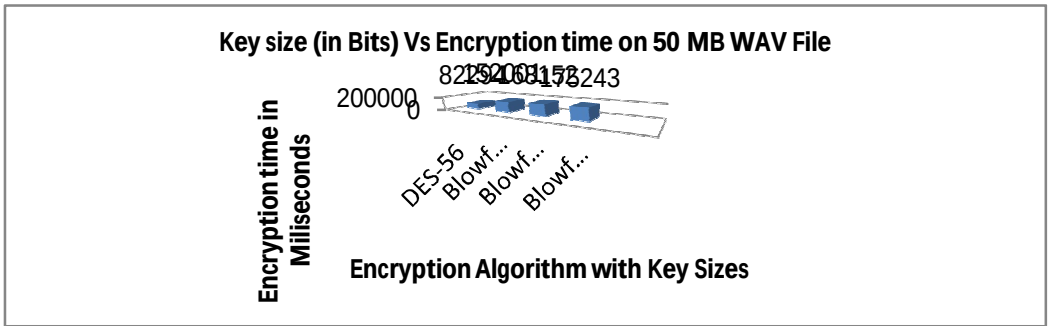


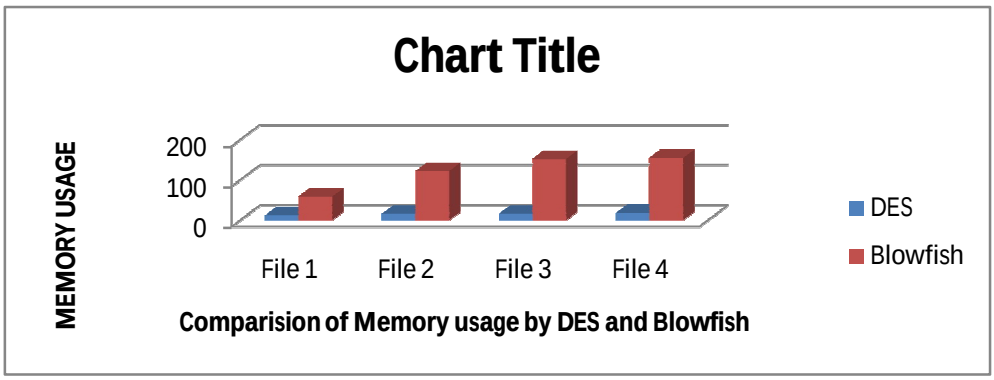
Figure 4: Variation of key sizes for different cipher Algorithm

Observation: The execution results show that for all ciphers algorithms, the encryption time varies with the change in the size of the key. Encryption time increases with increase in key size for block ciphers. The variation in time is very small. DES dominates in the block cipher. DES-56 is fastest among all algorithms tested.

7.4 comparison of memory usage:

Fig. 2 which show memory usages by DES and Blowfish algorithm. It is notice that DES algorithm memory usages are highest for all sizes of text file while memory usage is least.

DATA	ALGO	TIME (SEC)	MEMORY (MB)
FILE 1 (20MB)	DES	12	5
	Blowfish	59	4
FILE 2 (30 MB)	DES	16	3
	Blowfish	122	5
FILE 3 (40 MB)	DES	16	7
	Blowfish	152	3
FILE 4 (50 MB)	DES	18	14
	Blowfish	155	13



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

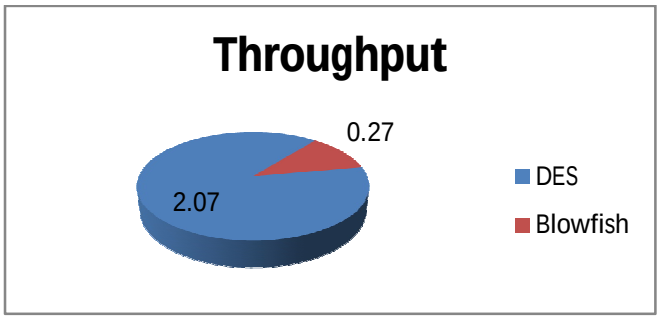
7.5 Throughput:

The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme .The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased .Similar procedure has been followed to calculate the throughput of decryption scheme. For my experiment, I have used Intel Core i3-3120M CPU of 2.50 GHz CPU speed with 4 GB RAM. In this experiment the text files sizes range from 50 KB to 22300 KB. The performance metrics are analysed by (a) Encryption/decryption time. (b) CPU process time – in the form of throughput.

Throughput = Plain Text (MB) / Encryption or decryption time (Sec.)

Input Size (MB)	DES	Blowfish
10	12	52
20	12	59
30	16	122
40	16	152
50	18	155
Avg Time	14.8	108
Throughput	2.07	0.27

Table 4: Throughput of DES and Blowfish with different file size (MB/Sec)



VIII. CONCLUSION AND FUTURE WORK

In this paper two symmetric key algorithm have been analyzed on ECB modes, various parameters like different data type, data size, data density, key size, cipher block modes and tested how the encryption time varies for different algorithms. From the execution results it is concluded that encryption time is independent of data type and data density. The research shown that, encryption time only depends upon the number of bytes of the file. It also revealed that encryption time varies proportionally according to the size of data. For all block cipher algorithms that are analyzed, with increase in key size, encryption time also increases, but reduces with increase in key size for DES. Blowfish is fastest block cipher, but DES appears to be fastest among all analyzed ciphers. In future we are trying to do research on CFB mode and ECB mode comparison and analyzing the performance based on above criteria varies for two algorithms.

REFERENCES.

[1] “Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES”, MilindMathur, AysuhKesarwani, Proceedings of national conference on new horizons in IT- NCNHIT 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

[2] "Dynamic selection of symmetric key cryptography algorithms for securing data based on various parameters", RanjeetMasram, vivekshahare, jibi Abraham, rajnimoona, pradeepsinha, gaur sunder, prashantbendale and sayalipophalkar, department of computer engineering and information technology, COEP, india.
[3] "Evaluation of the RC4 Algorithm for data encryption", allammousa and ahmadhamad, electrical engineering department an-najah university, Nablus, Palestine systems engineer paltel company, Nablus, Palestine.
[4] "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", Ritu Tripathi1, Sanjay Agrawal2. National Institute of Technical Teachers' Training and Research Bhopal, India.
[5] "Survey on Modular Attack on RSA Algorithm", International Journal of Computational Engineering& Management, ISSN: 2230- 7893, Satish N .chalurkari ,Nileshkhochare ,B.B. mashram.
[6] Cryptography and network security, Express Learning, ITL Education Solution ltd.
[7] "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, ISSN 0975-8887,Mohit Mittal.
[8] "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, E .Thambiraja ,G. Ramesh ,Dr. R. Umarani.
[9] "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies, ISSN: 2231-5268, Yogesh Kumar, Rajiv Munjal, Harsh Sharma.
[10] "A Survey on Different Secret Key Cryptographic Algorithms", Harshala B. Pethe1 and Dr. S. R. Pande2 ,Department of Electronics & Comp. Sc. RTMNU, Nagpur (India).IBMRD's Journal of Management and Research, Print ISSN: 2277-7830, Online ISSN: 2348-5922
[11] "A field manual for collecting, examining and preserving evidence of computer crimes", Marcella, A. J., Menendez D., (2008), Cyber Forensics,2nd ed. Auerbach Publications.
[12] International Data Encryption Algorithm (Idea)-A Typical Illustration, Journal of Global Research in Computer Science, 2(7), Basu, S (2011).
[13]"DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011, ISSN2250-2459,Jawahar Thakur and Nagesh Kumar.
[14] "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, PP: 464-465,Sombir Singh, Sunil K. Maakar and Dr. Sudesh Kumar, June 2013, Volume 3, Issue 6.
[15] "Optimized DES Algorithm Using Xnor Operand Upto 4 Round on Spartan3", International Journal of Computational Engineering Research (ijceronline.com), PoojaRathore, Jaikarn Singh, Mukesh Tiwari and Sanjay Rathore ISSN 2250-3005(online), PP: 193-198, December 2012, Volume 2, Issue 8.
[16] A Review of Various Encryption Techniques Harshraj N. Shinde1, Aniruddha S. Raut2, Shubham R. Vidhale3, Rohit V. Sawant4, Vijay A. Kotkar
[17] "Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2Ms. Neha Khatri Valmik and Prof. V. K Kshirsagar, Ver. X (Mar-Apr. 2014), PP: 80-83, www.iosrjournals.org, e-ISSN:2278-0661, ISSN:2278-8727.
[18] "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software EngineeringPratapChnadra Mandal, Volume 2, Issue 9, September 2012 ISSN:2277 128X.
[19] "Blowfish Algorithm", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013 ISSN: 2319-7080, Tanjyot Aurora and Parul Arora.
[20] "A Survey on Various Most Common Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering , E. Thambiraja, G. Ramesh and Dr. R. Umarani, , Volume 2, Issue 7, July 2012 ISSN: 2277 128X.
[21] CSc 466/566Computer Security5 : Cryptography — BasicsVersion: 2012/03/03 10:44:26Department of Computer ScienceUniversity of Arizonacollberg@gmail.comCopyright c 2012 Christian Collberg
[22]Symmetric CiphersMahalingamRamkumar(Sections 3.2, 3.3, 3.7 and 6.5)
[23] en.wikipedia.org/wiki/Block_cipher_modes_of_operation
[24]http://www.slideshare.net/csandit/dynamic-selection-of-symmetric-key-cryptographic-algorithms-for-securing-data-based-on-various-parameters