International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Study and Comparative Analysis of Cryptographic Algorithms for Various File Formats

M. Meena[1], A. Komathi[2]

[1]M.Phil. Scholar, Nadar Saraswathi College of Arts and Science, Theni, Tamil Nadu, India

[2]Assistant Professor, Nadar Saraswathi College of Arts and Science, TheniTamil Nadu, India

Abstract: ***Cryptography algorithm is the technique used for concealing the content of message from all users except the sender and the receiver and to authenticate the correctness of message to the recipient. Information security could be implemented with many known security algorithms. The most common of these are encryption algorithms. This paper provides a fair comparison between five most common symmetric key cryptography algorithms: DES, SDES, Triple DES, AES and Two Fish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of encryption, decryption and throughput time with the variation of various file features like different data types, data size and key sizes.***

Keywords: Cryptography, Symmetric, Encryption, Decryption, Throughput, Data size

1. Introduction

1.1 Cryptography

Cryptography has become one of the major methods for protection of data in all applications. It allows users to carry over the confidence found in the physical world to the electronic world. It enables the users to do business electronically without bothering of hackers. Earlier wax seals, signatures, and other physical mechanisms were used to assure integrity and data security. People communicate more electronically and upload their data in different fields. Increase of information transmitted through internet has increased the need of privacy and security of user‟s data.

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word „cryptography‟ was coined by combining two Greek words, „Krypto‟ meaning hidden and „graphene‟ meaning writing.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Encryption is the process of converting a message (or plaintext) into an „unintelligible‟ form (called cipher text) and decryption is the reverse process. The cipher text is transmitted by the sender to the intended recipient of the plaintext, across an insecure communication channel (any third party can intercept data that flows through such a channel). The algorithm used for performing encryption and decryption is called the cipher.

2. Literature Review

In this study [5] analyzed the different symmetric key algorithm for various file features like data size and key size, and analyzed the variation of encryption time for different selected cipher algorithms. The encryption and decryption time of different sizes of files are implemented in NetBeans 6.9.1 using java coding for Blowfish, DES, TEA, IDEA symmetric algorithms. The result of the paper was, IDEA algorithm is better for encryption process and blowfish algorithm is better for decryption process.

In [6], cryptography is used to ensure communication secrecy to pass coded messages between parties. The comparative study of various network security algorithms like AES, DES, Triple DES, Triple AES, Kasumi, Blowfish, RSA, RC4,XMODES and TACIT is done successfully with their key size and block size.

In [8], the author concluded that Blowfish is superior to other algorithms: DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms: DES, 3DES, and AES. It is concluded that Blowfish gives better performance than DES, 3DES, and AES in terms of encryption time, decryption time and throughput. 3DES has least performance among all mentioned algorithms.

3. Research Objective

The main objective of this research is to analyze time taken for encryption and decryption by various Symmetric cryptographic algorithms for parameters like data type, data size and key size.

As various symmetric cryptography algorithms exists, the research on the analysis of the algorithms with various file features will help the researchers for their further research on implementing new cryptography algorithms. The analysis is based on various algorithms to be tested with various file formats like text, image, audio and video. The files are analyzed with different data size and key size.

4. Methodology

4.1 Symmetric Key Cryptosystem

Symmetric key encryption uses the same key for encryption

and decryption of message. The necessity with a symmetric cryptosystem is to transfer secret key to both communication parties before secure communication can begin. The establishment of a shared secret key between communication parties had always been a difficult problem because the task needed a secure confidential channel.

Cryptography is based on the idea that factorization is really hard. Symmetric key encryption scheme which are of most used in present security systems are as:

4.1.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data.

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds.

4.1.2 Data Encryption Standard (DES)

The main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (Sboxes) and exclusive OR operations. DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of this cipher. DES is therefore, a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time.

4.1.3 Simplified DES (S-DES)

Simplified DES, developed by Professor Edward Schaefer of Santa Clara University [SCHA96], is an educational rather than a secure encryption algorithm. It has similar properties and structure to DES with much smaller parameters. The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and produces an 8-bit block of cipher text as output. The S-DES decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used to produce that cipher text as input and produces the original 8-bit block of plaintext.

4.1.4 Triple DES (3DES)

In cryptography, **Triple DES** (**3DES**) is the common name for the **Triple Data Encryption Algorithm** (**TDEA** or **Triple DEA**) symmetric-key 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 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 Data Encryption Standard (DES) shall consist of the following Data Encryption Algorithm (DES) [*sic*] and Triple Data Encryption Algorithm (TDEA, as described in ANSI X9.52). The TDEA is commonly known as Triple DES (Data Encryption Standard). TDEA is a symmetric block cipher with a block size of 64 bits. Key lengths can be 168, 112 or 56 bits (keying option 1, 2, 3 respectively). It uses 48 DES-equivalent rounds.

4.1.5 TwoFish

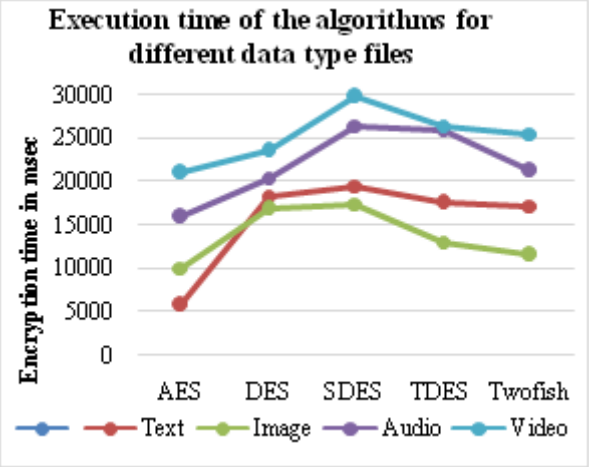
In cryptography, **Twofish** is a symmetric key block cipher with a block size of 128 bits ad key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish. Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay. Two Fish is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128, 192 or 256 bits. It uses 16 rounds.

5. Results and Discussion

An analysis of different symmetric key cryptographic algorithm has been done on the basis of various parameters like encryption time, decryption time and throughput for different data types, data sizes and key sizes.

5.1 Files with different Data types

This parameter has taken to check whether the encryption has dependency on type of data. Different data type files like text, image, audio 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, with varying parameter data type and constant parameters key size. The key size of AES (128), DES (64), SDES (10), TDES (168) and Twofish (128).

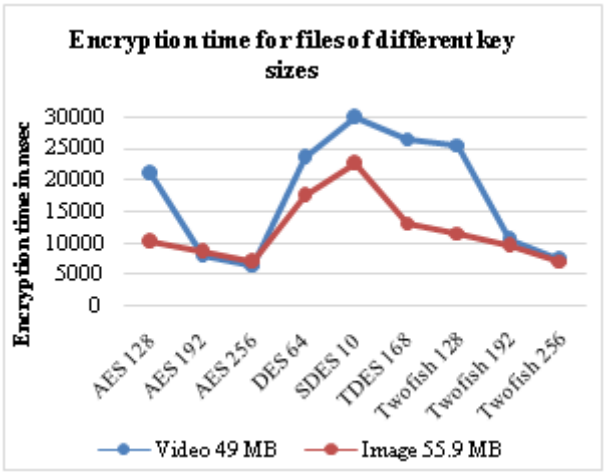


Graph 1: Execution time of the algorithms for different data type files

Observation: In Graph 1 it can be clearly seen that encryption time for all the data type is almostsame. 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. Encryption time of AES is fastest among the cipher algorithms tested.

5.2 Encryption Algorithms with different key sizes

This is to analyze the effect of changing the size of encryption key on encryption time. MP4 file of 49 MB and JPEG file of 55.9 MB is taken and different cipher algorithms are executed for different size of keys. The various key sizes are used during experimentation. Graph 2 shows the result of execution for key size variation.



Graph 2: Encryption time for files of different key sizes

Observation: The execution results shown that for all ciphers algorithms, the encryption time varieswith the change in the size of the key. Encryption time decreases with increase in key size for block ciphers. The variation in time is very small. AES with 256 key size is fastest among all algorithms tested.

5.3 Performance Evaluation Parameters

Performance measurement criteria are time taken by the algorithms to perform the encryption and decryption of the input text file that is encryption computation time and decryption computation time.

Table 1: Execution Parameters for files of different size

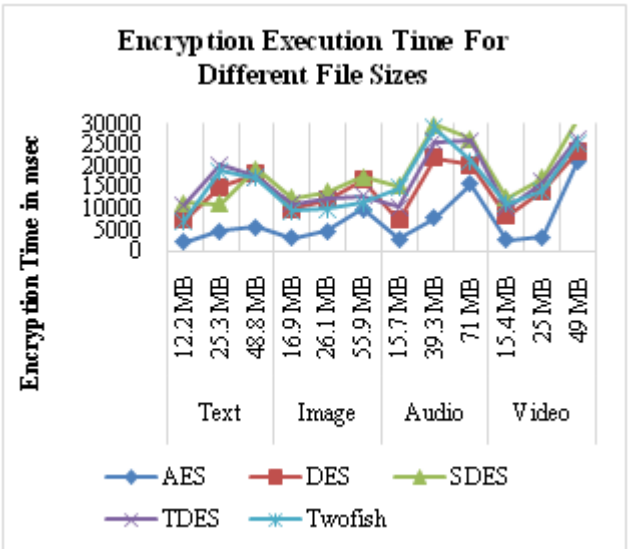
File Type	*Varying Parameters (Data Size)*	*Constant Parameters*
Text	12.2 MB, 25.3 MB and 48.8 MB	Data Type and Key Size
Image	16.9 MB, 26.1 MB and 32.9 MB	
Audio	15.7 MB, 39.3 MB and 71 MB	
Video	15.4 MB, 25 MB and 49 MB	

5.4 Encryption Computation Time

The encryption computation time is the timewhich is taken by the algorithms to produce the cipher text from the plain text. The encryption time can be used to calculate the encryption throughput of the algorithms.

Table 2: Encryption Execution Time for Different File Sizes

Input File	Size in MB	Encryption Execution Time (msec)				
		AES	DES	SDES	TDES	Twofish
		128	64	64	168	128
Text	12.2	2200	7450	11300	10820	7110
	25.3	4700	15090	11160	20450	19020
	48.8	5810	18340	19500	17510	17250
Image	16.9	3210	9920	12550	11160	9520
	26.1	4910	12080	13900	12270	10050
	55.9	10100	16900	17430	13100	11500
Audio	15.7	3000	7460	15400	10490	14880
	39.3	7880	21910	29880	25880	29110
	71	15910	20460	26480	25960	21210
Video	15.4	2600	8400	12600	10150	11100
	25	3320	14310	17400	16400	14200
	49	20960	23500	29800	26460	25500



Graph 3: Encryption Execution Time for Different File Sizes

Observation: For each encryption algorithm same parameters are used for files of different sizes.Table 5 shows Execution Parameters for files of different size. From the results in Table 6 and Graph 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.

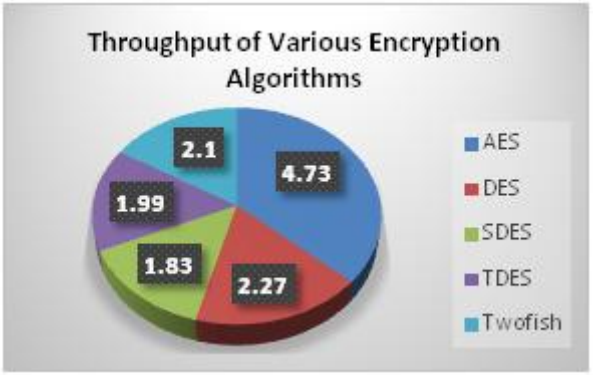
5.5 Encryption Throughput

Calculation of Encryption Throughput
Encryption Throughput (Kb/sec) = Σ Input File Size/Σ Encryption Execution Time

Table 3: Encryption Throughput Value

Algorithm	AES	DES	SDES	TDES	Twofish
Encryption Throughput Value	4.73	2.27	1.83	1.99	2.1

From the above calculated values of throughput; it is clear that AES algorithm provides optimized results in comparison to other encryption algorithms and shown in graph 4.



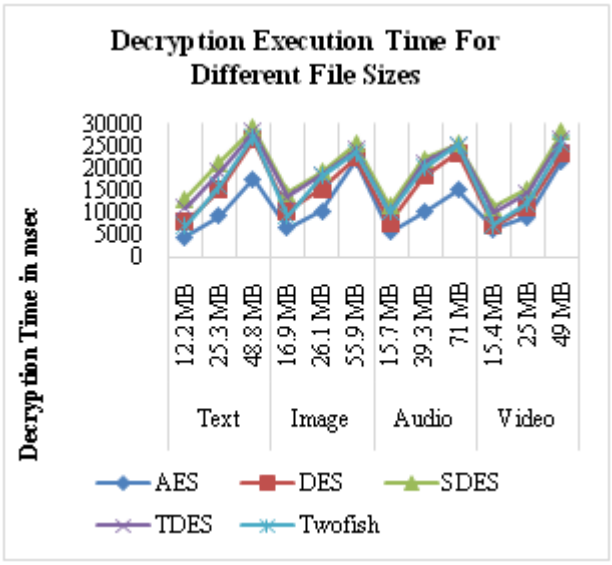
Graph 4: Throughput of Various Encryption Algorithms

5.6 Decryption Computation Time

The decryption computation time is the timetaken by the algorithms to produce the plain text from the cipher text. The decryption time can be used to calculate the decryption throughput of the algorithms.

Table 4: Decryption Execution Time for Different File Sizes

Input File	Size in MB	Decryption Execution Time (msec)				
		AES	DES	SDES	TDES	Twofish
		128	64	64	168	128
Text	12.2	4580	8000	13100	11210	7020
	25.3	9260	15050	21200	19250	16020
	48.8	17590	26470	29100	28120	27150
Image	16.9	6610	10500	14450	13520	9230
	26.1	10490	15480	19320	18450	18250
	55.9	21820	22440	25580	24120	23410
Audio	15.7	5710	7820	11470	10210	10250
	39.3	10160	18290	22190	21250	20150
	71	15240	23520	25460	25260	25390
Video	15.4	6280	7150	11350	10240	7240
	25	9040	11250	15410	14540	12280
	49	21580	23250	28150	26590	25490



Graph 5: Decryption Execution Time for Different File Sizes

Observation: For each decryption algorithm same parameters are used for files of different sizes.Table 5 shows Execution Parameters for files of different size. From the results in Table 7 and Graph 5 we can find that the result for different size of data varies proportional to the size of data file. Decryption time increases as file size increases in multiples of data size.

5.7 Decryption Throughput

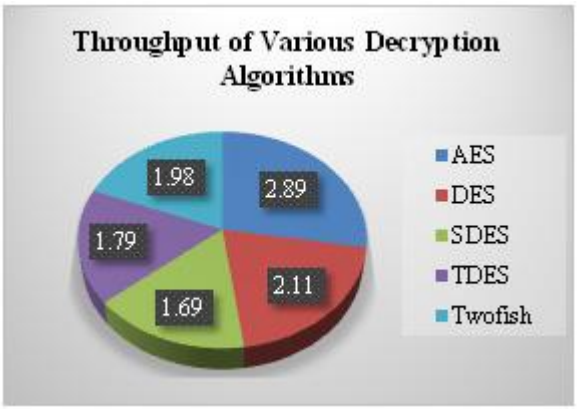
Calculation of Decryption Throughput

Decryption Throughput (Kb/sec) = Σ Input File Size/Σ Decryption Execution Time

Table 5: Decryption Throughput Value

Algorithm	AES	DES	SDES	TDES	Twofish
Decryption Throughput Value	2.89	2.11	1.69	1.79	1.98

From the above calculated values of throughput; it is clear that AES algorithm provides optimized results in comparison to other decryption algorithms and shown in graph 6



Graph 6: Throughput of Various Decryption Algorithms

6. Conclusion

In this research paper, different symmetric key cryptographic algorithms have been analyzed for various file features like different data type, data size, key size, and analyzed the variation of encryption time, decryption time and throughput time for different selected symmetric key cryptographic algorithms. From the simulated results it is concluded that encryption and decryption time does not dependent upon data type but only depends upon the number of bytes present in the file. As the size of data increases, the encryption and decryption time also increases proportional to data size. For all algorithms that are analyzed, with increase in key size, encryption time also increases, decryption time also increases but reduces with increase in key size for AES and Twofish. AES appears to be fastest symmetric key cryptographic algorithm with encryption throughput rate of 4.73 kb/sec and decryption throughput rate of 2.89 kb/sec comes out to be fastest among all analyzed symmetric key cryptographic algorithms.

7. Future Enhancement

Symmetric cryptology is an old but still a strong security mechanism that is most widely used. Proposed work can be further extended if randomized padding schemes are used for strong bit security level.More secured results can be obtained if the key size is further increased.

References

[1] Ritu Tripathi, Sanjay Agrawal, “Comparative study of symmetric and asymmetric cryptography techniques”, International journal of advance foundation and researchin computer (IJAFRC), June 2014.
[2] Kirti Aggarwal, Jaspal Kaur Saini , Harsh K. Verma, “performance evaluation of rc6, blowfish, des, idea, cast-128 block ciphers” International journal of computer applications, April 2013.
[3] Srinivas B.L, Anish Shanbhag, Austin Solomon D‟Souza, “A comparative performance analysis of des and blowfish symmetric algorithm”, International journal of innovative research in computerand communication engineering, October 2014.
[4] Chaitali Haldankar, Sonia Kuwelkar, “Implementation of AES and blowfish algorithm”, International journal of research in engineering and technology IJRET, May2014.
[5] G.Sindhu, P.Krithika „Analysis and comparison of symmetric key algorithms (Blowfish, DES, TEA, IDEA) in cryptography‟ International Journal for Science and Research in Technology (IJSART) [Volume 1, Issue 11 –NOVEMBER 2015] ISSN [ONLINE]: 2395-1052 Page 67 – 72.
[6] Nitin Gupta, Dr.Manoj Kumar „Comparative study of different authentication and identification algorithms in secured cryptography‟ International journal of engineering sciences & research technology [January 2015] ISSN: 2277-9655 Pg. No: 221 – 228.
[7] K.Saranya, K.Mohanapriya, J.Udhayan „A review on symmetric key encryption techniques in cryptography‟ International journal of science, engineering and technology research (IJSETR) [March 2014]
[8] Narender Tyagi, Anita Ganpati „Comparative analysis of symmetric key encryption algorithms‟ International journal of advanced research in Computer science and software engineering, [Volume 4, Issue 8, August 2014], ISSN: 2277 128X, pp. 348 – 354.
[9] Rajdeep Bhanot, Rahul Hans, „A Review and Comparative Analysis of Various Encryption Algorithms‟ International Journal of Security and its Applications [Volume 9, Issue 4, 2015], pp. 289-306.
[10] Gurpreet Singh, Supriya „A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security‟ International Journal of Computer Applications [ISSN: 0975 – 8887, Volume 67, No.19, April 2013] pp: 33 – 38
[11] Jawahar Thakur, Nagesh Kumar „DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis‟ International Journal of Emerging Technology and Advanced Engineering [ISSN 2250-2459, Volume 1, Issue 2, December 2011] pp: 6 - 12
[12] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, „Performance Evaluation of Symmetric Encryption Algorithms‟ IJCSNS International Journal of Computer Science and Network Security, [VOL.8 No.12, December 2008], pp. 280-286.

Author Profile

Meenais an M.Phil Scholar and completed her MCA degree in Madurai Kamaraj University. She already published a paper in a journal and presented a paper at conference. Her area of interest is Network Security.

Komathicompleted her M.C.A., M.Phil. now doing Ph.D. in Bharathiar University. Now she is working as Vice Principal, Head and Assistant professor in Department of CS&IT, Nadar Saraswathi College of Arts and Science, Theni. Her area of interestsis Data Structure, Biometric Authentication, Data Compression and Wireless Sensor Network. She organized and also attended many conferences, seminars and workshops. So far presented 18 papers in international conference and published 12 papers in the international journals. She is member of staff selection committee in NSCAS, Board of studies member in MTWU. Her area of research is Wireless Sensor Network. She served as research supervisor for M.Phil. Scholars.