Evaluation of DES and AES Cryptographic Algorithms

Navneet Kaur[1]
Department of Computer Science and Engineering
Lovely Professional University, Punjab.

N Venkat Sai[2]
Department of Computer Science of Engineering
Lovely Professional University, Punjab

G Manikanta Kumar[3]
Department of Computer Science and Engineering
Lovely Professional University, Punjab

Abstract - *we live most of our lives on Internet. It may be for entertainment, online shopping, storing our personal information, or for doing our jobs. present society mainly relies on internet. Increasing dependency on internet means importance of information security is increasing than ever. Every user wants his or her data to be secure. We can keep our data secure by Data encryption. Data encryption is a mathematical technique which converts plane data to encoded data and converting encoded data to original data is called decryption. It is one of the oldest and most used technique. Everyone wants best data encryption algorithms with high performance to secure their data. Example, government websites which stores confidential information like Aadhaar cards needs best security and websites like Discussion forums however it requires good security for user credentials it does not need that high security for discussion inside it. Among various cryptographic algorithms that exists today. Whenever we are talking about data encryption it is never missed to discuss about Data Encryption Standard (DES) and Advanced Encryption Standard (AES). DES and AES are symmetric data encryption and decryption techniques means uses same keys to both encrypt and decrypt data.*

Key Words: **Encryption, Decryption, DES, AES, Cryptography.**

INTRODUCTION

In ancient days messages are sent with help of pigeons. Since then, civilization has been evolved so much and it led to the emergence of different groups, tribes and kingdoms. This emergence raised the idea of battle, politics to attain supremacy and power. The politics and power heightened the need for secret communication between the people which in return initiated the cryptography evolution as well. It all started with some improved techniques of coding and during world war II cryptography has completely became mathematical. There are two main types of cryptographies are using today symmetric or secret key cryptography it is the oldest technique and second is asymmetric or public key cryptography it is started using since late 1970's.

Now with the complete advancement of technology military units, governments and IT sectors started incorporating the cryptographic applications to send sensitive data and guard it from others. Effectiveness of the cryptography has been improved with internet now in the reach of common people.

[8] Symmetric Block Cipher is a process which transforms the plain text into encrypted text. It divides text into blocks with certain size then with the help of a function and a key it encrypts the data. It uses a symmetric key in the encryption process and since it is symmetric key, the same key used to decrypt the data too. Figure 1 shows the Symmetric Block cipher.

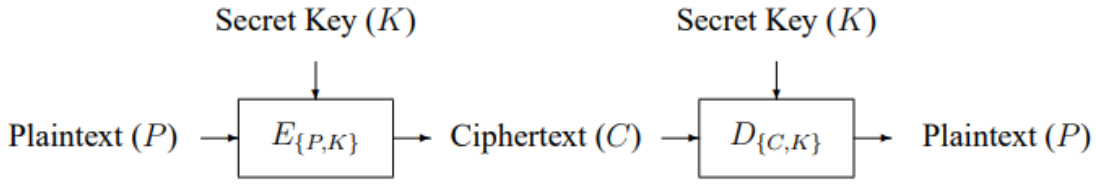

Figure 1 Symmetric Block cipher [2]

[9][10] Data Encryption Standard (DES), Advanced Encryption Standard (AES) are encryption standards works on Feistel cipher algorithms. DES and AES both are symmetric key cipher algorithms. In this encryption and decryption algorithm uses same key.

DES is found by IBM in early 1970s and published by National Institute of Technology (NIST). United States Government in 1977 adopted DES as Federal information processing standard. In DES plain text is converted into 64 bits block each and each block is encrypted into cipher text with secret key of 48 bits by means of permutations and substitutions. DES Encryption process consists of 16 rounds and it uses different key for each round and block in each round depends on previous round.

[1] AES is standardized on 2001 by National Institute of Technology (NIST). Vincent Rijmen and Joan Daemen developed AES. It is a cipher algorithm with different key lengths and block sizes. AES includes AES-128, AES-192, AES-256. cypher encrypt and decrypts data in 128bit blocks using keys of length 128, 192, 256 bits. Data can be classified as Confidential, Secret and Top secret, any key length of AES can be used to protect confidential and secret Data. 192 or 256bit length key is required for top secret data.

Literature survey

Priyadarshini Patil et. al. [3] evaluated DES, 3DES, AES, RSA and Blowfish algorithms not only by theoretically by performance analysis. They evaluated algorithms by using parameters like Encryption time, Decryption time, Memory used, Avalanche effect, Entropy and Number of bits required for encoding optimally. All algorithms take less time for decryption than encryption. AES uses less memory than DES, any application demands algorithm which uses less memory and provides high security. AES requires highest bits than DES to encode optimally, for transmission also it requires highest bandwidth. If cryptographic strength is major factor, we chose AES and if network bandwidth is major factor for any applications, we chose DES.

Yogesh Kumar et. al. [4] made theoretical analysis of symmetric and asymmetric cryptographic algorithms. Every cryptographic algorithm available can be categorized to symmetric or asymmetric keys encryption. There are many strong and weak key cryptographic algorithms like RC2, DES, 3DES, RC6, Blowfish, AES. In this 64bits key is used in RC2, same in DES, and 3 64bit keys are used in 3DES, Key length of 128, 192 or 256 either is used in AES etc. From various symmetric and asymmetric algorithms, they selected DES and RSA. Their analysis says that for decryption prioritized application DES is better option, also stated asymmetric cryptographic algorithms provides best security in all ways. It is predicted due to increasing technology and quantum computing these algorithms may cause threat in coming future.

Hamdan.O.Alanazi et. al. [5] introduced three algorithms namely DES, 3DES and AES for encryption strategies for multimedia. All these techniques were presented by the authors in 9 factors that comprise key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time. Based on all these factors, it was found that AES performs well as compared to the remaining two techniques. AES technique also performs well with small sized devices and also due to its larger block size and long keys, it is more secure. Hence, AES can also be considered as a replacement for 3DES. Therefore, AES has better efficiency.

Bawna Bhat et. al. [6] implemented practical performance of DES and AES. The compared AES and DES on the basis of avalanche effect simulation time and memory used. Cryptography place major role in confidentiality, authentication and integrity maintenance. Memory usage of DES is comparatively more than AES, also avalanche effect or one bit variation is less in DES than in AES. AES provides more improved security than DES.

Data Encryption Standard

[10] DES works on Feistel block cipher. It contains number of rounds in each round consists of non-linear substitutions, exclusive OR operations and bit shuffling. Most symmetric encryption design today are based on Feistel network. DES algorithm expects two inputs a plain text to encrypt and a secret key. As DES is symmetric it uses same key for encryption and decryption, it only operates on 64bit block data at a time.

After receiving a plain text to be encrypted. It is arranged into 64bit blocks for input. If number of bits in message not evenly divisible by 64 then last block will be padded. Many permutations and substitutions are incorporated to increase the complexity of performing cryptanalysis on cipher. It is accepted fact that initial or final permutation offers less or no contribution to security in DES.

DES performs permutation on whole 64bit block data. It is then split into 2, 32bit blocks Left plain text (L) and Right plain text (R) which are passed to 16 rounds. Every round of encryption is identical. At the end L and R blocks are joined and final permutation is performed. Key size used is 56bit at a time. The least significant bit is always used as parity bit. All bits are numbered from left to right so that we can make eighth bit of each bite as parity bit. From this a 48bit subkey is generated in each round by the process of key transformation. Fig 2 shows working of DES.

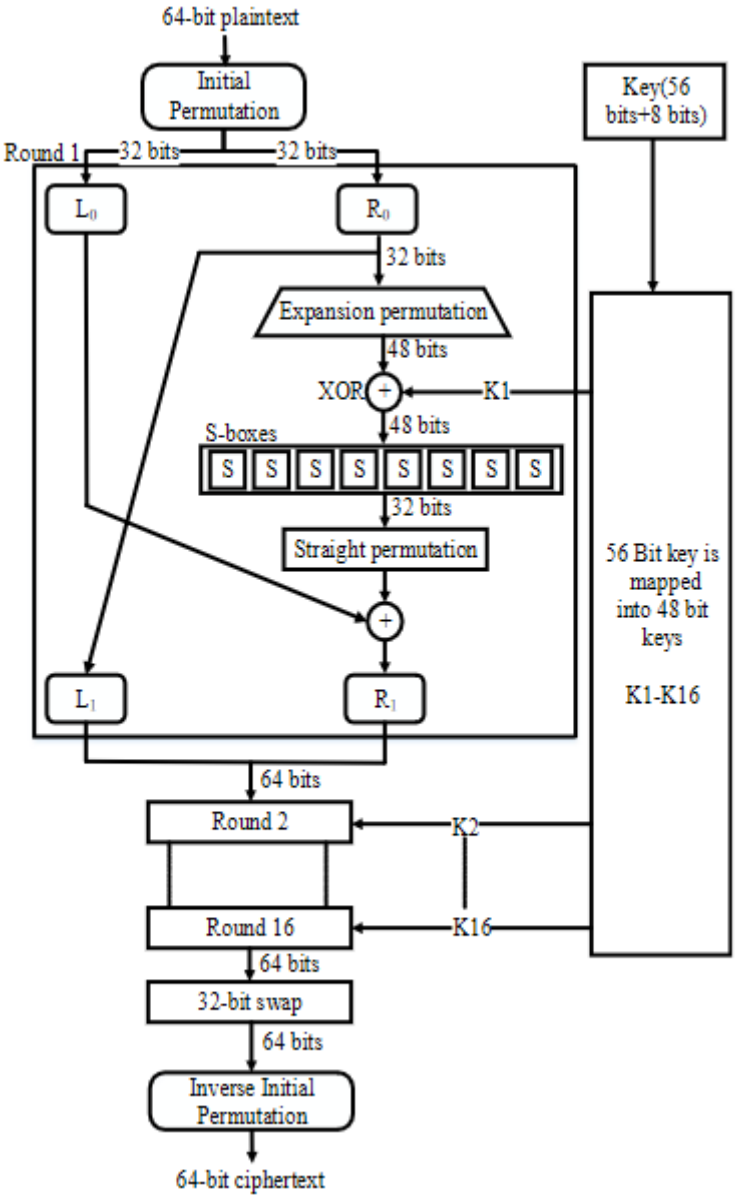

Figure 2 Working of DES algorithm [10]

Decryption of the cipher text in the DES is so simple, in order to decode the message, we just need to inverse the order of the key from upside down.

Advanced Encryption Standard

As AES is different when compared to DES and uses permutation-substitution method, it divides the converted 128 bits message block as 16 bytes. These bytes are represented as a 4x4 matrix with four rows and four columns, this matrix is also known as State Matrix.

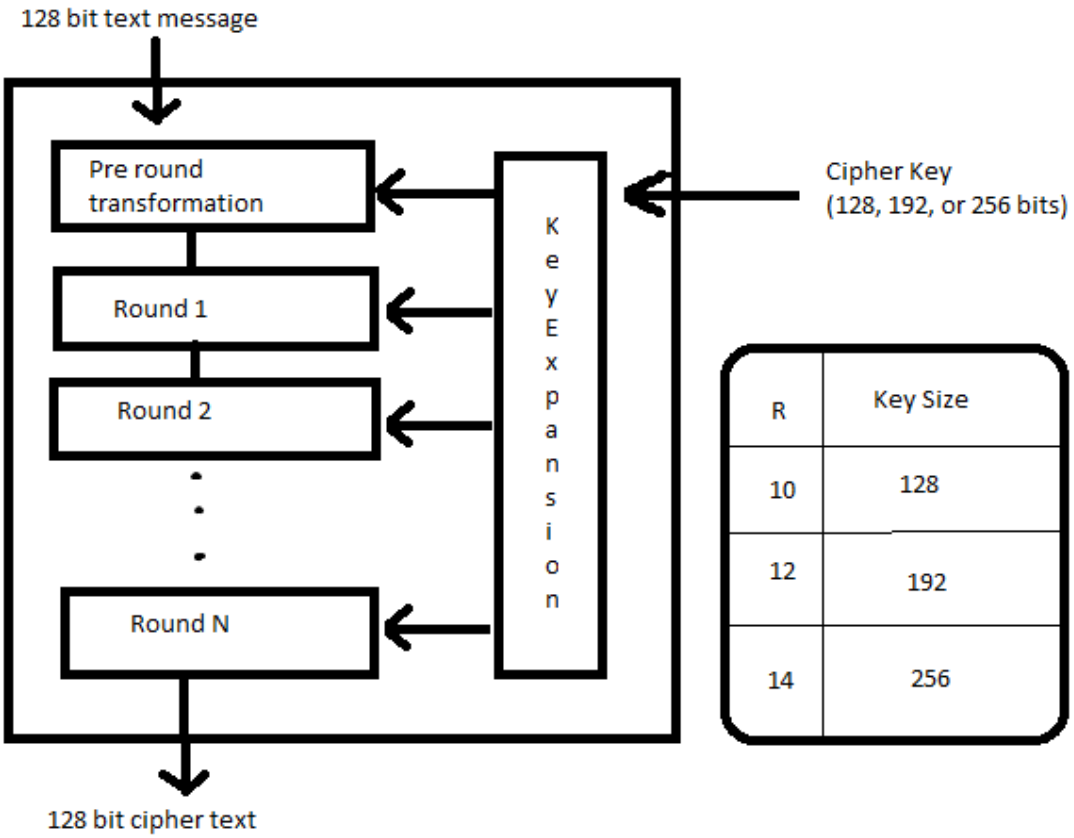

Figure 3 Advanced Encryption algorithm

The above image Fig 3 is the representation for 128-bit key size, which is one among the three variant key sizes AES can use.

Encryption

[7] [10] Each and every round in AES has its own sub operations. Actually, AES encryption has been represented in three steps with sub steps for each one.

1. Initial Round – AddRoundKey or PreRound Transformation.
2. Main Rounds – SubBytes, ShiftRows, Mix Columns, AddRoundKey.
3. Final Round – SubBytes, ShiftRows, AddRoundKey.

Initial Round –

The AddRoundKey is the only operation phase that directly operates with the AES round key in AES encryption.

MainRounds –

There are 4 sub operations in the main rounds of the encryption process. Fig 4 explains sub operations

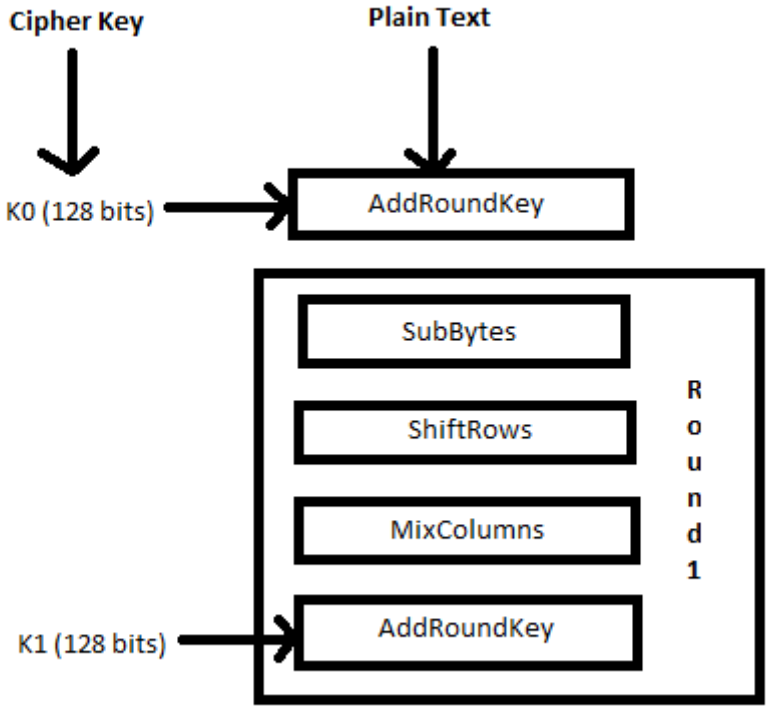

Figure 4 Working of AES algorithm

- SubBytes – In the phase of SubBytes the input bytes are substituted with the help of a fixed or pre-defined table know as S-Box. After the completion of the substitution process the result is stored in a 4x4 matrix.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 5 Fixed AES S-Box

- ShiftRows – In ShiftRows the resulted 4x4 matrix form SubBytes shit the rows to the left in a particular manner.
    1. The 0th row will be fixed and will not shift
    2. The 1st row will be shifted to left one time.
    3. The 2nd row is shifted to left 2 times.
    4. The 3rd row will be shifted to left 3 times.

  By resulting a new matrix with shifted values with 16 bytes in it.

- MixColumns – In MIxColumns the resulted matrix from the ShiftRows is multiplied with a mathematical term for each and every column resulting a new block of code. This makes it more complicated and makes it hard for the attacker to decipher it.
- AddRoundKey – Now the new block of code is considered as 128-bits, an XOR operation is applied to the 128-bits new block and 128-bits key from key expansion of AES encryption until it reaches the last round and the last result of the last round is the 128-bit cipher text of the 128-bit plain text.

Decryption

There is no much difference in the encryption and decryption of the AES, the decryption process is just the inverse of the encryption process of the AES. Fig 6 explains process of encryption and decryption.

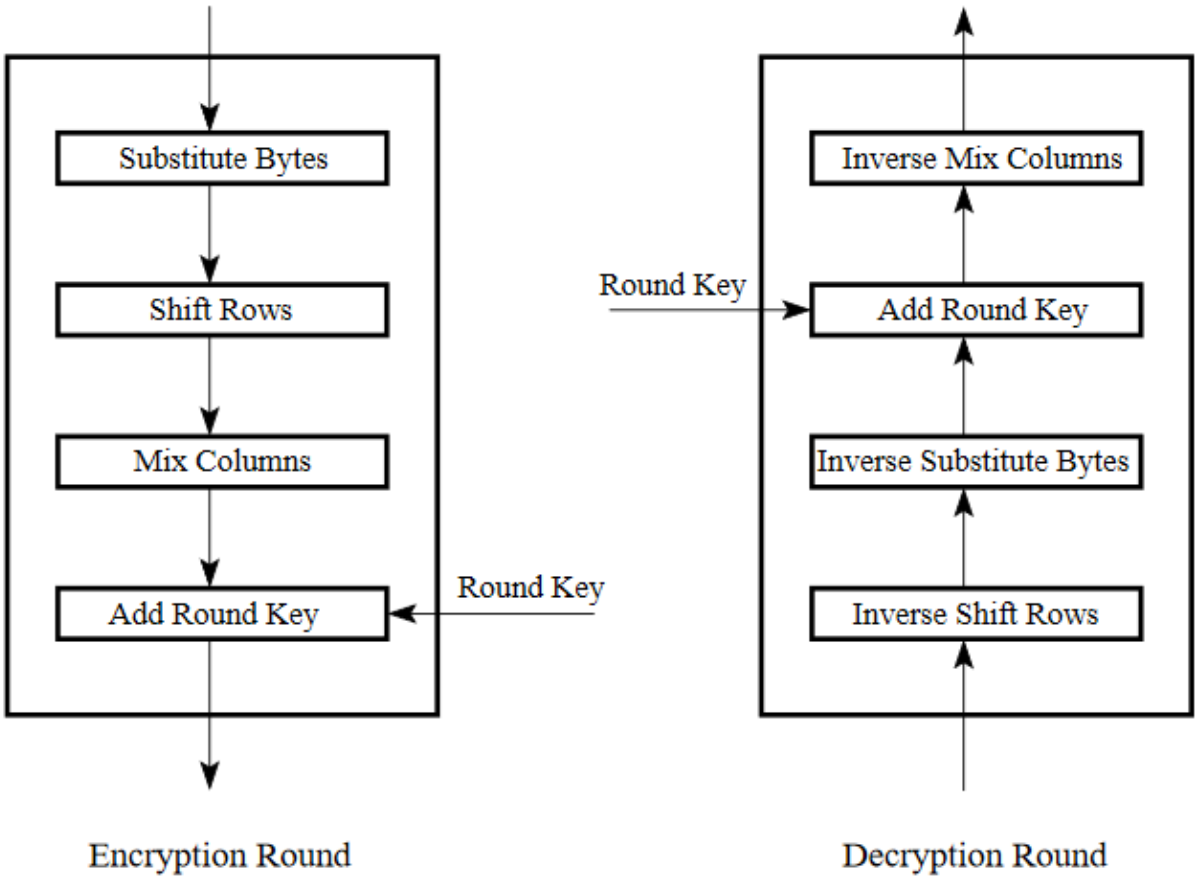

Figure 6 AES encryption and decryption

Table 1 depicts the evaluation by factors and Table 2 depicts the evaluation by methods

Table 1: Evaluation by factors

Factors	**DES**	**AES**
Developed	1977	2000
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block length	64 bits	128, 192 or 256 bits
Key Length	56 bits	128, 192 or 256 bits
Security	Moderate	More secured

Table 2: Evaluation by methods

Methods	**DES**	**AES**
Encryption	Slower	Faster
Decryption	Slower	Faster
Key Distribution	Difficult	Difficult
Complexity	O (log N)	O (N)
Vulnerability cause	Brute Forced, Linear and differential cryptanalysis Attack	Proper Linear Attack
Nature	Closed	Open
Principle	Feistel structure	Substitution and permutation
Rounds	16	10 for 128 bits, 12 for 192 bits, 14 for 256 bits.

Conclusion

[8] This paper presents theoretical performance analysis of DES and AES algorithms. It also explained with working mechanism of both algorithms. Our final thoughts on both encryption standards are that AES is more secure than compared to DES. After the approval of DES to be used to protect the sensitive data of US government it is widely adopted throughout the world and it led to the scrutiny of DES. Its shorter key length has become one of the most concern. To test its capability many competitions are conducted. In the very first challenge, which is DES-I conducted in 1997 took 84 days to decrypt it. In DES-II it took 30 days in 1998. In DES-III it only took 22 hours and 15 minutes to decrypt it. By this result it has fallen under the list of insecure algorithms. And then 3DES came into the existence in 1999 but light did not shine on it for long, 3DES is found to be vulnerable to Sweet32 Vulnerability. DES is suitable for applications which requires less security and AES is used for highly secured applications. AES is more secure than DES because unlike DES it uses substitution and permutation method to encrypt and its varying key lengths of 128, 192 and 256 makes it so hard to break. It provides increasing amount of security.

References

[1] M.Pitchaiah, Philemon Daniel, Praveen Implementation of Advanced Encryption Standard Algorithm.

[2] Sourav Chapter 2 The data encryption standards http://www.facweb.iitkgp.ac.in/~sourav/DES.pdf

[3] Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish.

[4] Yogesh Kumar, Rajiv Munjal, Harsh Sharma Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures.

[5] Hamdan O Alanazi, B Zaidan, A Zaidan, Hamid Jalab, M Shabbir and Al Nabhani New Comparative Study Between DES, 3DES and AES within Nine Factors.

[6] Bawna Bhat, Abdul Wahid Ali, Apurva Gupta DES and AES Performance Evaluation.

[7] Advanced Encryption Standard – Tutorialspoint

https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm.

[8] DES vs AES – InfoSec Insights by SECTIGO Store https://sectigostore.com/blog/des-vs-aes-everything-to-know-about-aes-256-and-des-encryption/.

[9] Shaza D. Rihan, Ahmed Khalid, Saife Eldin F. Osman A Performance Comparison of Encryption Algorithms AES and DES.

[10] Gurpreet Singh, Supriya A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security.