International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-12, Mar 2018

A Survey Paper On Cryptographic Algorithms For SMART Voting.

[1]Swapnil Randhave, [2]Dr. Ayesha Butalia, [3]Vaibhav Thakare, [4]Sushant Nanaware, [5]Sagar Bhor

[1,2,3,4,5]Department of Computer Engineering PGMCOE, Wagholi, Pune University, Maharashtra, India.

[1]swpnlrandhave@gmail.com, [2]ayeshabutalia@yahoo.co.in, [3]vaibhav.vat@gmail.com, [4]sushant2328@gmail.com, [5]Sagarbhor70@gmail.com

Abstract: Nowadays, digitalization spreads very rapidly. In this digital age, democratic systems increasingly adopt to technology to support, and to transform political processes. There are some ways to tamper existing EVM machine by changing display or by rewriting memory and activating code on machine. So we propose the smart voting system in which hardware is introduced parallel to EVM machine which stores votes on server. Security is the significant concern when the sensitive data is put on server and exchanged over the web where the data is never protected by physical limits. Cryptography is a basic, important part to guarantee the safe communication between the various elements by exchanging unordered data and just the authorized person can have the capacity to get to the data. The correct determination of cryptographic algorithm is important for secure communication that gives greater security, precision and efficiency. In this paper, we look at the security perspectives and procedures associated with the plan and usage of most broadly utilized symmetric encryption algorithms, for example, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Besides, this paper assessed and thought about the execution of these encryption algorithm based on encryption and decryption time, throughput, key size, memory. Therefore, among the current cryptographic algorithm, we pick a suitable encryption algorithm to secure online voting system.

Keywords: Smart Voting, Cryptography, Encryption algorithms, Symmetric, Asymmetric, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish.

I. INTRODUCTION

Election is a process in which voters choose their representatives and give their choice for the way that they will be governed. Correctness, coherence, consistency, security, and transparency of voting are all key requirements for the integrity of an election process [1]. There are various different voting systems that are based on traditional paper ballots, mechanical devices, or electronic ballots. We propose the online voting system in which two results are generated one with EVM machine and other with hardware which contains controller that controller send the votes to server.

Smart Voting Systems Requirements

Smart voting systems requirements satisfy basic functionalities and elements of an online voting system. Authenticity, Freedom, Eligibility, Security, Verifiability, Privacy, Accuracy, Availability, Efficiency are various requirements of smart voting system [1].

There is also possibility of client side and server attacks for hacking online smart voting system for changing the votes Security is an essential part to store data and transmit it over the undefined systems and networks with secure way. Hence, the safe communication is the essential requirement of each transaction over networks and systems. Cryptography is a basic mechanism for secure communication and transmission of data through security administrations like confidentiality, integrity, availability, authentication and authorization. It gives an approach to secure our data by moving it into unreadable format and just the authorized person can able to get to this data converting it into original data. The procedure to change over the plaintext into cipher text with the key is called encryption process and to invert the procedure of encryption is called decryption process. The outline of cryptographic algorithms is secure and productive, minimum effort, require little memory, simple to execute and used on various platforms. Cryptography is part of cryptosystem which contains five tuples which are encryption, decryption, plaintext, cipher text and key. The various types of applications are available to secure cryptographic algorithm using various mathematical and numerical process. It is very hard to create completely secure encryption algorithm because of the difficulties from cryptanalysts who consistently trying to get to any accessible cryptographic system [2],[3],[4]. Cryptographic frameworks can be isolated into deterministic and probabilistic encryption scheme [5].Deterministic encryption allows permits the plaintext is encoded by utilizing keys that dependably give the same cipher text, yet the encryption process is rehashed commonly. In this plan, each plaintext has coordinated association with the keys and cipher text else it will create more than one outcome of specific plaintext at decryption process. Probabilistic Encryption Scheme demonstrates the plaintext has distinctive cipher text with the different keys. The probabilistic encryption is essentially secure than the deterministic encryption since it makes troublesome for a cryptanalyst to get to any important data with respect to plaintext that is taken from cipher text and relating key. Besides, the cryptographic algorithm can be further classified into two classes like keyless cryptosystem and key-based cryptosystem. In the keyless cryptosystem, the connection between the plaintext and cipher text having an alternate form of the message is depends upon the encryption algorithm. The keyless cryptosystem is by and less secure than key-based system since anybody can access the algorithm will have the capacity to decrypt each message that was encoded by using keyless cryptosystem, for example, Caesar cipher [6],[7]. The key-based cryptosystem can be further classifications into symmetric key encryption and asymmetric key encryption.

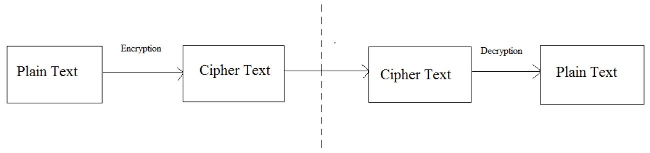

Fig 1. Working of cryptographic algorithms.

The detail of the cryptosystems is discussed after:

A. *Symmetric Key Encryption*

The symmetric key encryption it uses same key for encryption as well as decryption of information. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way [8]. In symmetric-key cryptography, we encode our plain text by mangling it with a secret key. Decryption requires knowledge of the same key, and reverses the mangling.

Cipher text = encrypt (plaintext, key)
Plaintext = decrypt (cipher text, key)

Symmetric key cryptography is useful if you want to encrypt files on your computer, and you intend to decrypt them yourself. It is less useful if you intend to send them to someone else to be decrypted, because in that case you have a "key distribution problem": securely communicating the encryption key to your correspondent may not be much easier than securely communicating the original text. The symmetric key algorithm can divided into block and stream cipher by considering group of message bits [9]. Symmetric key block cipher includes the five main parts: plaintext, cipher text, encryption, decryption and key schedule algorithm as shown in Fig. 2.

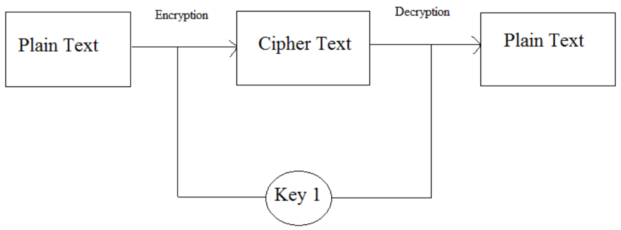

Fig. 2. Symmetric key encryption algorithm

There are various symmetric key encryption algorithms such as DES [10],[11],[13] AES [13],[14],[15],[16] BLOWFISH [18],[19],[20] etc. The encryption process in symmetric block cipher converts the plaintext into cipher text with the secret key that is generated from the key schedule algorithm. cipher text is transferred to the destination is decrypted using decryption process with the same key. The working of the stream cipher is presented in following steps:

1) A one character of plaintext is combined with a single character of key to produce the character of cipher text.
2) The cipher text character from Step 1 sent to the receiver.
3) Step 1 and Step 2 is repeated until the entire message has been sent [13].

B. *Asymmetric Key Encryption*

The asymmetric key encryption is known as public key encryption. In this different keys are utilized for the encryption and decryption purpose. The key used for encryption is also said as the public key and can be utilized to encrypt the message with the key. The key used for decryption purpose is said to as secret or private key and can be used to decrypt the message. The quality of the asymmetric key encryption is utilized with digital signature then it can it can give to the clients through message verification detection [13]. There are number of asymmetric encryption algorithm like RSA, Diffe-

Hellman algorithm, etc. The working of an asymmetric key encryption algorithm is shown in Fig. 3.

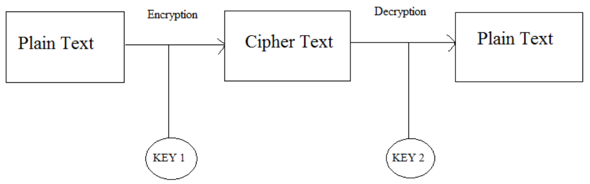

Fig. 3. Asymmetric key encryption algorithm

As in smart voting the result generated by machine is send to secure server. So, there will one to one communication means data is encrypted by one end and also decrypt at same end. In this scenario, the symmetric key encryption algorithm is suitable for secure votes in smart voting system.

II. CRYPTOGRAPHIC ENCRYPTION ALGORITHMS

This part clarifies the survey of existing encryption algorithm that are used to decide the better encryption algorithm suitable for smart voting system.

A. *Data Encryption Standard (DES)*

DES is the symmetric encryption algorithm developed by IBM in 1972 and adopted in 1977 as Federal Information Processing Standard (FIPS) by the National Bureau of Standard (NBS). The NBS is currently the National Institute of Standards and Technology (NIST) that assess that evaluate and implement the standard encryption algorithm. It incorporates 64 bits key that contains 56 bits are specifically used by the calculation as key bits and are arbitrarily created. The remaining 8 bits that are not utilized by algorithm since it is utilized for error detection [10], [11], [13]. DES used the single key for encryption and decryption process, the key length is 56 bits and produce encryption of message utilizing the 64 bits block cipher. So also, the decryption procedure on a 64 bits cipher text by utilizing the same 56 bits key to create the unique 64 bits block of the message is appeared in Fig. 4. The DES algorithm forms the 64 bits input with underlying change, 16 rounds of the key and the last stage. DES is based on the Feistel Cipher, which contains Round function, Key schedule and Initial and final permutation. The initial and final permutations are straight Permutation boxes P − boxes that are inverses of each other. They have no cryptography significance in DES. Round Function is the heart of this cipher in the DES function, f. The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong. First is avalanche effect in this small change in plaintext results in the very grate change in the cipher text. And other one is completeness in this each bit of cipher text depends on many bits of plaintext. DES mostly used in the banking industry, commercial and military secret information sharing purpose. Security is the major concern in DES because it uses the 56 bits key (256) and cryptanalysts are trying to crack an encrypted message by key exhaustion. Brute force attack is possible through parallel machines [12],[13]. DES is cracked in 1998 by using device which is constructed by Electronic Freedom Foundation due to the less number of key lengths and is highly affected to the linear cryptanalysis attacks.

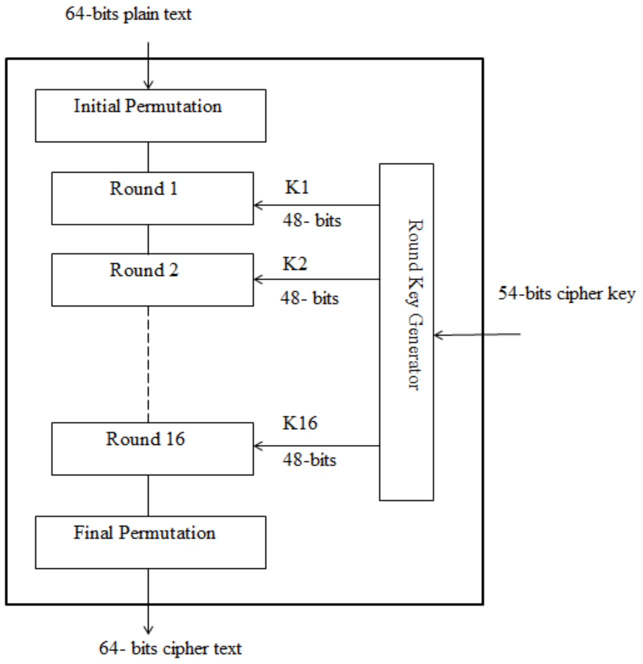

Fig 4. Data Encryption Standard (DES) Algorithm.

B. *Advanced Encryption Standard (AES)*

The more popular and widely adopted symmetric encryption algorithm likely to be encountered now a days is the Advanced Encryption Standard (AES). It is found at least six time faster than DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. AES appears as the recent generation block cipher and significantly increases in the block size up to 128 bits with the key sizes 128 bits, 192 bits and 256 bits. The number of rounds set with respective key size is the 10, 12, 14 for the 128 bits, 192 bits, 256 bits, respectively [14], [15], [16]. The number of AES parameters based on the key length mentioned in Table 2. The parameters Key size, Block size, Number of rounds, Round key size, and expanded key size are represented as Ks, Bs, Nr, Rks, Eks, respectively. AES is an iterative rather than Feistel cipher. It is based on substitution permutation network. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs and others involve shuffling bits around. Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. AES has some important features like Symmetric key symmetric block cipher. 128-bit data, 128/192/256-bit keys. Stronger and faster than DES. Provide full specification and design details. Software implementable in C and Java [13],[17].

Ks (words/bytes / bits)	Bs (words/bytes / bits)	Nr .	Rks (words/bytes/ b its)	Eks (words / bytes)
4/16/128	4/16/128	10	4/16/128	44/176
6/24/192	4/16/128	12	4/16/128	52/208
8/32/256	4/16/128	14	4/16/128	60/240

TABLE I Advanced Encryption Standard Parameters

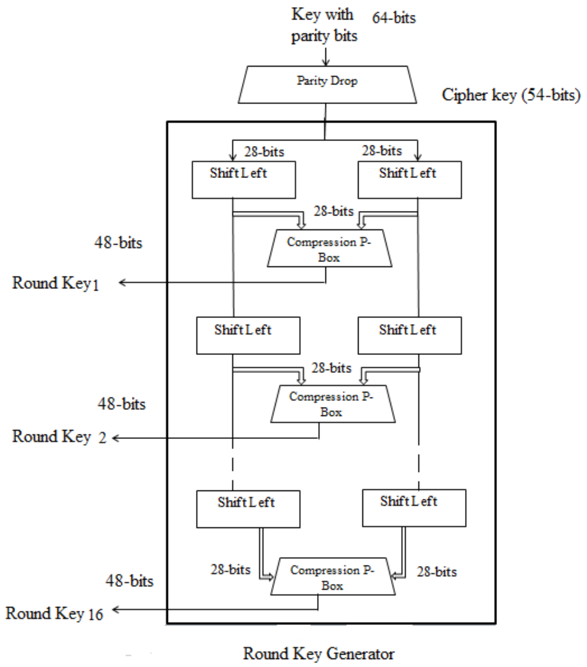

Fig 5.Advanced Encryption Standard (AES) Algorithm.

C. *Blowfish*

World's famous cryptologist Bruce Schneier, composed the algorithm and made it accessible in the general population of world [18][22]. The algorithm was first present in 1993, and has not been broken yet .It is a symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits and having a fiestal organize . It can be advanced in applications like hardware because of its smallness. The algorithm as appeared in Fig.4.consists of two sections: a key-expansion part and an information encryption part. The role of key expansion part is to changes over a key of at most 448 bits into a few sub key clusters of 4168 bytes [18][22]. The information encryption happens by means of a 16-round Feistel organize[19]. It is appropriate for application where the key does not change regularly, similar to communications link or an automatic file encryption. It is fundamentally speedier than most encryption calculations when executed on 32-bit microprocessors with large data caches. The Blowfish is intended to point four criteria known as Fast, Compact, Simple and Variably Secure. Blowfish has some classes of weak keys. For these weak keys, separate rounds end up using the same round-keys. Keys belonging to these classes can be detected only in reduced-rounds versions of the algorithm and not on the full blowfish[A survey on Conventional Encryption Algorithms of Cryptography [21],[22].

Encryption in Blowfish algorithm is done by following steps :

Blowfish uses a large number of sub keys. These keys must be precomputed before any data encryption or decryption.

1. The P-array consists of 18 32-bit sub keys: P_1, P_2 ..... P_{18}.

.2. There are four 32-bit S-boxes with 256 entries each:

Blowfish is a Feistel network consisting of 16 rounds The input is a 64-bit data element, x.

Divide x into two 32-bit halves: x_L, x_R

```
For i = 1 to 16:
        $x_L = x_L$ XOR $P_i$
        $x_R$ = F(XL) XOR $x_R$
        Swap $x_L$ and $x_R$
Swap $x_L$ and $x_R$
$x_R = x_R$ XOR $P_{17}$
$x_L = x_L$ XOR $P_{18}$
Recombine $x_L$ and $x_R$
Function F :
        Divide $x_L$ into four eight-bit parts: a, b, c, and d
```

$F(x_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32})$ XOR $S_{3,c},) + S_{4,d} \bmod 2^{32}$

Decryption process in Blowfish is exactly the same as encryption process, except that P_1, P_2 ..... P_{18} are used in the reverse manner[22].

III. RESULTS ANALYSIS

This section explains the performance of Data Encryption Standards, Advanced encryption standards and Blowfish algorithm with the help of various results and researchers. The performance analysis of mentioned algorithms was considered by different aspects. Which are block size, key length, encryption time, decryption time and throughput. Because of large block size large block of data will be encrypted in one cycle. Small block of data requires more than one cycles for execution. Large key length also affect the performance of cryptology algorithms as they provide more security and privacy. Also the time required for encryption, decryption and throughput also affects the performance of algorithms. There are various calculations carried out by researchers to analyse the result and performance of given algorithms. Following TABLE represents the average time and throughput required by DES, AES and Blowfish algorithm while the text files of various size given as input to algorithm.

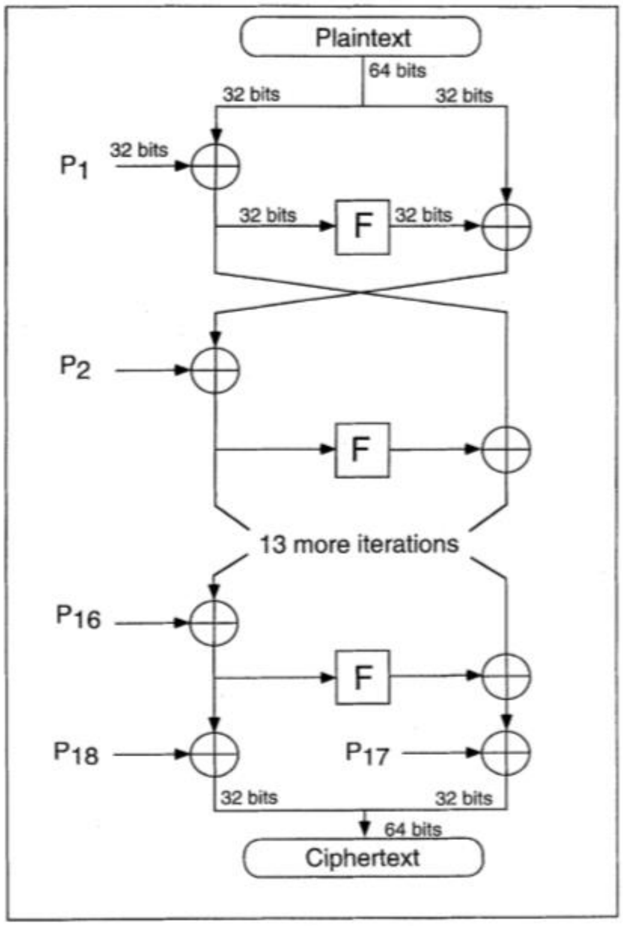

Fig.6. Blowfish Encryption Algorithm[21].

FILE	DES (in msec)	AES (in msec)	BLOWFISH (in msec)
1MB	136	80	133
2MB	269	154	192
5MB	665	376	373
10MB	1236	683	702
Avg Time	1379	1293	1400
Throughput (KB/msec)	7.60	13.30	11.40

TABLE II Data table for Throughput of Text File[22].

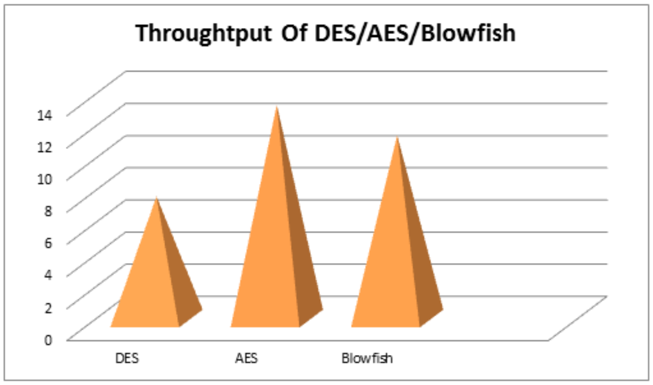

Fig.7. Throughput of text file for DES/AES/Blowfish algorithm

Parameters for Algorithms	DES	AES	Blowfish
Developed by	IBM	Vincent Rijmen, Joan Daeman	Bruce Schneier
Published	1977	2001	1993
Algorithm Structure	Feistel	Substitution Permutation	Feistel
Key Length	56 bits	128 bits, 192 bits and 256 bits.	32-448 bits
Block cipher	Binary	Binary	Binary
Flexibility	No	YES, 256 key size is multiple of 64	YES, 64-448 key size in multiple of 32
Number of Rounds	16	10,12,14	16
Block size	64 bits	128 bits	64 bits
Throughput	Lower than Blowfish	Greater than Blowfish and DES	Lower than AES

Level of Security	Sufficient security	Good security	Good security
Encryption Speed	Slow	Fast	Fast
Effectiveness	Slow in both software and hardware	Effective in both software and hardware	Effective in both software
Attacks	Brute force attack	Side channel attack	Dictionary attack

TABLE III Comparison of DES/AES/BLOWFISH [13].

IV. CONCLUSION

The encryption algorithms has very important role in security. For securing the vote generated by machine which is stored on server those encryption algorithms are very useful. Out of symmetric and asymmetric algorithms, symmetric algorithms are effective in case of only one side required encryption and decryption i.e. one to one communication. This paper present performance evaluation of selected symmetric algorithms. At the end we conclude that out of DES, AES and Blowfish algorithm AES algorithm has more performance than DES and Blowfish. So, we use AES algorithm for securing SMART Voting system.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to our guide Dr. Ayesha Butalia as well as Prof. Shreekant Dhamdhere sir for giving me correct guidance for writing this paper. I would also say thanks to my parents and friends for supporting me.

REFERENCES

[1] Abdalla Al-Ameen , Samani A. Talab “E-Voting Systems Security Issues” in Proceeding of International Journal of Networked Computing and Advanced Information Management(IJNCM) Volume3, Number1,April 2013

[2] K. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES,” in Proceeding of the IEEE Students' Conference on Electrical, Electronics and Computer Science: Innovation for Humanity (SCEECS), 2012.

[3] M. Ebrahim, S. Khan, and U. bin Khalid, “Symmetric algorithm survey: A comparative analysis,” International Journal of Computer Applications, vol. 61, no. 20, pp. 12–19, 2013.

[4] V. V Palagushin and A. D. Khomonenko, “Evaluation of cryptographic primitives security based on proximity to the latin square,” in Proceeding of the IEEE 18th conference of fruct association, pp. 266– 271, 2016.

[5] S. Goldwasser and M. Bellare, Lecture Notes on Cryptography, Cambridge, Massachusetts, 2008.

[6] A. Kaushik, M. Barnela, and A. Kumar, “Keyless user defined optimal security encryption,” International Journal of Computer and Electrical Engineering, vol. 4, no. 2, pp. 2–6, 2012.

[7] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” Journal of Cryptology, vol. 26, no. 1, pp. 80–101, 2013.

[8] Symmetric Key Cryptography

https://www.webopedia.com/TERM/S/symmetric_key_cryptography.html

[9] Symmetric Key Cryptography

https://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/symmetric-key.html

[10] N. I. of S. and T. NIST, “Data Encryption Standard (DES),” Federal Information Processing Standards Publication (FIPS PUB 46-3), vol. 25, no. 10, pp. 1–22, 1999.

[11] M. E. Smid and D. K. Branstad, “Data Encryption Standard: past and future,” Proceedings of the IEEE, vol. 76, no. 5, pp. 550–559, 1988.

[12] Bawna Bhat, Abdul Wahid Ali, Apurva Gupta “DES and AES Performance Evaluation” in Proceeding of International Conference on Computing, Communication and Automation (ICCCA2015).

[13] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina et al.” A Survey on the Cryptographic Encryption Algorithms” in Proceeding of (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.

[14] N. I. of Standards-(NIST), Advanced Encryption Standard (AES). Federal Information Processing Standards Publication197, 2001.

[15] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, “Strengthening the key schedule of the AES,” Proceedings of the 7th Australian Conference on Information Security and Privacy, pp. 226– 240, 2002.

[16] Soufiane Oukili, Seddik Bri “High speed efficient Advanced Encryption Standard implementation” in Proceeding of Networks, Computers and Communications (ISNCC), 2017.

[17] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, “Report on the development

of the advanced encryption standard (AES)," National Institute of Standards and Technology, pp. 1– 116, 2000.

[18] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008.

http://www.schneier.com/blowfish.html

[19] BLOWFISHalgorithm"

http://pocketbrief.net/related/BlowfishEncryption.pdf

[20] Tingyuan Nie, Teng Zhang "A Study of DES and Blowfish Encryption Algorithm" in Proceeding of TENCON 2009 - 2009 IEEE Region 10 Conference.

[21] [20] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in Proceedings of the Fast Software Encryption: Cambridge Security Workshop Cambridge, U. K., pp. 191–204, 1994.

[22] Madhumita Panda, "Performance Analysis of Encryption Algorithms for Security" in Proceeding of International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.