A survey on history and working of DES and AES

[1]Mr. Aby Thomas, [2]Mr. Ashok Babu

[1] Mtech Student, School of Computer Sciences Mahatma Gandhi University, Kottayam
[2] Assistant Professor, School of Computer Sciences, Mahatma Gandhi University, Kottayam.

Abstract: From ancient times the idea of hiding the data from unauthorized parties were in practice. The process of hiding and securing that data is called encryption and it was enabled throughout history through various methods. from the ancient arab traders to the present military applications these methods are preferentially used. The IBM has developed a new technological approach called Advanced Encryption Standard and is adopted by NIST, in order to solve the new challenges that had been evolved until 1998. As time passed by, the existing system have also become vulnerable to various attacks like brute force attack, algebraic attacks etc. In this study we will attempt to review the different versions of the AES, the different predecessors of AES, Data Encryption Standard and the broad history that is concerned with the AES and the different challenges of the predecessors of AES that led to the need of AES.

IndexTerms **- Cryptography, AES.**

1. INTRODUCTION

Encryption is the way to guarding your own information while you sent it to another. The historical beginning of encryption is from 600 BC with The antiquated Spartans, where scytale is utilized to send messages during the battles, which was an advanced technology at that time. This comprises of a calfskin lash and the letters on it are negligible when it's unwrapped which is folded over a wooden pole. If the beneficiary has the accurately measured bar then only the message could be decrypted. Also in 60 BC another substitution Cipher was invented for the war efforts of Julius Caesar but the first actual encryption key based cipher was invented by Giovan Battista Bellaso in 1553. The next major invention occurred in 1854 by Charles Wheatstone when he invented play-fair cipher. With the invention of enigma by German engineer Arthur Scherbius caused the need to counter the advantages of this machine done towards the axis powers in world war 2 led towards the creation of its modern version by the allied forces in 1939 by the help of famous cryptographers like Alan Turing from the information gathered from Marian Rejewski, a Polish cryptographer. The starting phase of Modern cryptography began with the publishing of "A mathematical theory of cryptography" by Claude Shannon.

By the 1969 United States based company IBM created Block Cipher to hide consumer data, later they were modified by United States Government and adopted it by the US government agency called NIST in 1973 and thus Data Encryption Standard or DES was born. DES was a secure technology compared to all other technologies and it remained unchecked until 1997.

Triple DES was developed in 1977 during the translation period between DES and AES. Where 3-DES is an electronic machine learning variety of algorithm were block cipher algorithms are applied on each block of information three times. In Triple DES, the key size is boosted to guarantee extra safety via features of encryption. There seem to be 64 bits of keys for each frame of data and the three keys are named as 56-bit bundle keys per key. This technology was also developed by IBM and later adopted by NIST.

NIST developed AES as a successor for DES in 1997, which began to be a brutal force. This appears to be about six times faster than triple DES. AES is a Symmetric key symmetric block cipher, it takes 128-bit data and 128/192/256-bit keys..

2. RELATED WORKS

AES was enabled by NIST as a way to protect the assets of the US government, ie to protect their classified information. The details about regions from which the data is collected is been specified here.

Pachamuthu Rajalakshmi et al [2] have bestowed a compact hardware-software co-design of Advanced coding customary (AES) on the field-programmable gate arrays (FPGA) designed for affordable embedded systems. The computationally intensive operations of the AES area unit enforced in hardware for higher speed. By incorporating the processor within the AES style, the whole range of slices needed to implement the AES algorithmic rule on FPGA is verified to be reduced. The complete AES system style is valid exploitation 460 slices in Spartan-3E XC3S500E, which is one among the affordable FPGAs.

Xinmiao Zhang et al [1] have given varied approaches for economical hardware implementation of the advanced secret writing customary formula. The improvement strategies may be divided into 2 classes: Branch of knowledge improvement and Branch of recursive improvement. Branch of knowledge improvement exploits the strength of pipelining, loop unrolling and sub-pipelining. Speed is magnified by process multiple rounds at the same time at the value of magnified space. Branch of knowledge improvement isn't an efficient resolution in feed-back mode. Loop unrolling is that the sole design which will win a small speed with considerably magnified space. In non-feedback mode, sub pipelining can do most speed up and also the best speed/area magnitude relation. Recursive improvement exploits recursive strength within every spherical unit. Varied strategies to cut back the crucial path and space of every spherical unit are given.

William Stallings [3] describes in his book wherever he provides a survey of cruciform secret writing, together with classical and trendy algorithms at the stress is on the 2 most vital algorithms-Data Encryption Standard, Advanced Encryption Standard and its intermediary 3-DES

D Coppersmith et al [4] had presented a replacement methodology for 3-DES cryptography. It uses many freelance keys, achieving strength against key exhaustion attacks. In contrast to different modes, it conjointly defends against attacks that supports small block size, particularly lexicon attacks and matching cipher text attacks.

Vedkiran et al[5]in their paper presents a literature survey and study of AES considering speed and AES application in wireless communication devices and this paper had additionally attempted to study the internal methods of AES including the ten steps involved and the procedures in each step are considered during this paper.

Pandya et al [6] in their paper considered the brief history of encryption process from the ancient period to the modern era of data security applications via medieval period. The study by the team prefers all of the essential and relevant pieces of encryption history and united them.

3. GENERAL HISTORY TILL DES

The first noted example of written cryptography was the cipher text, in the form of non-standard hieroglyphs, that was incised on monuments by the Egyptians dated back to 1900 BC.[6] These arrangements failed to offer abundant concealment or security, except for the amusement of history enthusiasts.[6] Another finding emerged which can be dated to the period of 500-600 BC which is a Hebrew scribe came up with an easy substitution cipher referred to as Atbash.[6].

Challenges of Atbash

- It is a weak cipher
- it works based on substitution cipher

By 487 BC, "scytale" was discovered by the Spartans and Greeks to be used for secret communications for the war campaigns.[6]

Challenges of Scytale

- Transferred using leather and similar materials
- It is a weak method as compared to today's techniques.

Another major historical discovery occurred in the time of Julius Caesar where the discovery of simple substitution cypher for the war campaigns.[6] In 1467 AD, the title "Father of Western Cryptology" was entitled to Italian scientist Leon Battista for developing polyalphabetic ciphers.[6].

Challenges of polyalphabetic cipher

- It is a weak method as we can decode it by dividing into cryptograms

By 1518 AD, Johannes Trithemius invented the tabula recta, which was used in polyalphabetic ciphers.[6] But in 1856, Charles Babbage breaked polyalphabetic ciphers.[6]

By the wake of 1935s German military started using Enigma machines which was all set to change the course of history of cryptography altogether. In 1939 using the secrets found by Poland allied forces decoded the enigma technology and that gave the allies victory in war.

Challenges of Enigma machines

- The letter is not coded by its own
- The same set of codes are encoded in a similar way

In 1942, the US Navy won the Battle of Midway by breaking into the JN-25 cryptographic system which was used by Japanese navy for secret communications. After the 2nd world war two kinds of encryption algorithms emerged, symmetric key algorithms and asymmetric key algorithms for encryption process. if encryption key is equivalent for decryption process then it is symmetric if that is not the case, then asymmetric. Advanced Encryption Standard (AES), Data Encryption Standard (DES) are the technologies that we are considering and both will come under Symmetric version of encryption algorithms.

4. DATA ENCRYPTION STANDARD

DES is discovered by IBM and later adopted by the National Institute of Standards and Technology or NIST for securely storing secret digital data. As a symmetric key cypher DES is very easy to use or compile.

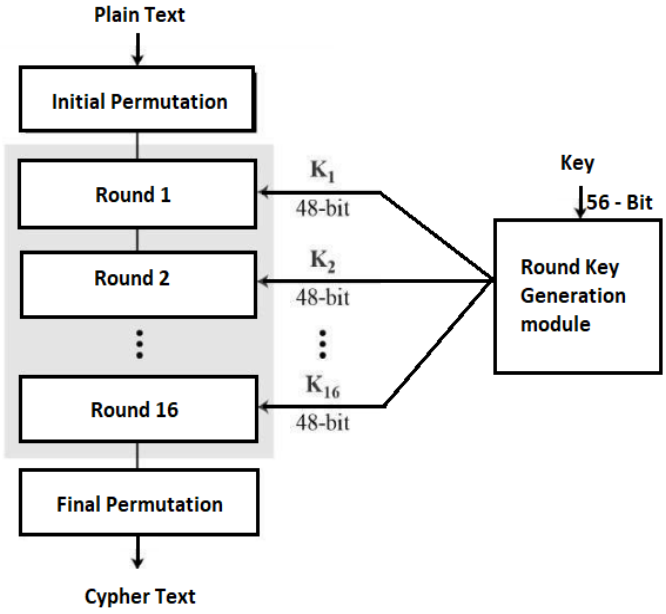


Fig 4.1 Working of DES

It takes 64 bit keys and it is also an example of feistel cypher. It take 64 bit plain text and 64 bit key but it only uses 56 bit of the 64 bit key so the key is specified as 56 bits also. The initial and final permutations have no cryptographic significance in DES and they are exact inverse of each other they work with the help of permutation boxes. The 16 rounds are the heart of DES the working of each round is similar and each of them require a 48 bit round key developed by round key generator and those keys are non-similar to each other. During the 16 rounds the operations are similar they involve Expansive Permutation, XOR operation, application of S-Box, and Permutation operation. During Expansive Permutation process 32 bit key is expanded to 48 bit and also

a permutation or changing of order will also takes place. After that an XOR operation is performed on the 48 bit output of Expansive Permutation resulting in another 48 bit output. With the application of a prefixed S-Box the details are then altered forever until decryption where first bit is used to find the row of S-Box and the other bit for finding the column number and using the specified value from S-Box the plain text content is altered. For an added safety another Permutation operation is also performed on the output of the result of S-Box.

5. ADVANCED ENCRYPTION STANDARD

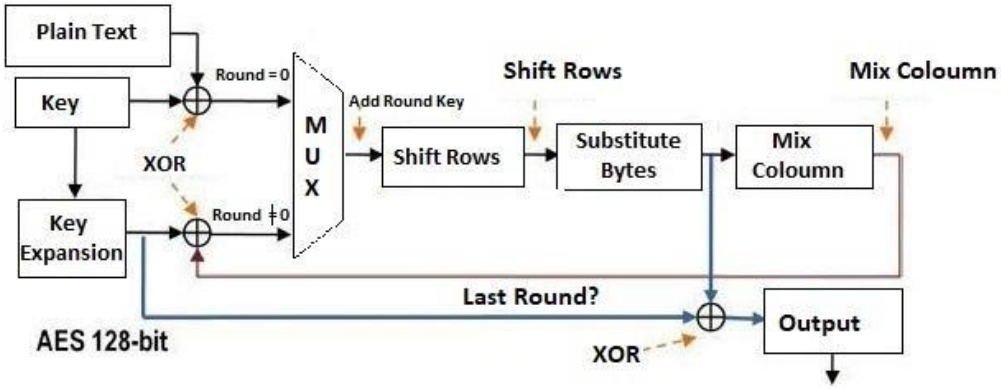
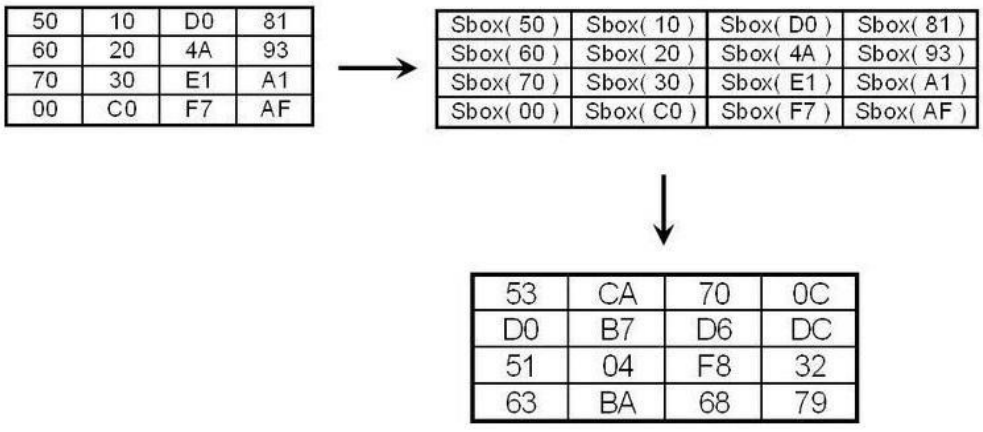


Fig. 5.1 Flowchart of AES

Advanced Encryption Standard is a symmetric key cypher widely used by United States government to store their classified documents digitally secure. The Data management unit and the Key management unit are the two main components of AES.[5] The Data processing units have four main modules which includes Substitute Byte, shift row operation, mix column and add round key and also the Key Expansion unit is used for the generation of the round key that need to be used in the next round. The AES is mainly a 128 bit algorithm so it operates on 128-bit data. The algorithm can encrypt and decrypt using keys. The key can be of different sizes mainly 128, 192, or 256 bits. Key size depends mainly on the security level of consideration as high level security involving data requires high bit rate on the key.

5.1. Substitute byte



50	10	D0	81
60	20	4A	93
70	30	E1	A1
00	C0	F7	AF

Sbox(50)	Sbox(10)	Sbox(D0)	Sbox(81)
Sbox(60)	Sbox(20)	Sbox(4A)	Sbox(93)
Sbox(70)	Sbox(30)	Sbox(E1)	Sbox(A1)
Sbox(00)	Sbox(C0)	Sbox(F7)	Sbox(AF)

53	CA	70	0C
D0	B7	D6	DC
51	04	F8	32
63	BA	68	79

Fig 4.2 Simple application of S-Box

Substitute byte or Bit Transformation operation is mainly applied using Substitution Boxes or S-Boxes. It substitutes for all positions of the state array using a 4 x 4 matrix called Substitution box. The transformation that this module causes is called an affine transformation. This step will increase the security of the text or part of the text that is being considered for the purpose of providing the security.

5.2. Shift Row Transformation

The first row of the 4 x 4 state matrix will be allowed to remain unchanged. The 2nd row will be left circularly shifted one time, the 3rd row will be left circularly shifted two times, and the 4th and last row will be left circularly shifted three times

5.3. Mix Column

All entries of the state array are transformed into a new content using a selected mathematical function or mathematical transformation.

5.4. Add Round Key

We will generate a round key for each of the rounds and will be logically added to the state array. as logical addition is equivalent to XOR operation we will perform it. and the resultant is considered. The resultant obtained after 10 rounds is known as cipher Text.

6. Conclusion

In this study we had considered the ancient history of encryption, the medieval history of encryption and the modern history of encryption. We specifically studied the need and evolution details of AES, DES and also both AES and DES have been subjected towards a detailed study about their working patterns, their strengths major transformations used etc.

References

[1] Xinmiao Zhang and Keshab K. Parhi "Implementation Approaches for the Advanced Encryption Standard Algorithm" IEEE 2002.

[2] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM, pp. 1445-1449, 2003.

[3] William Stallings, "Cryptography and Network Security", Fifth Edition, Pearson, 2011, ISBN 978-81-317-6166-3.

[4] D. Coppersmith, D. B. Johnson and S. M. Matyas, "A proposed mode for triple-DES encryption," in IBM Journal of Research and Development, vol. 40, no. 2, pp. 253-262, March 1996.

[5] Saini, Parvinder Bangar, Harjeet Singh Chauhan, Vedkiran. (2014). "Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application".

[6] Pandya, Dwiti & Khushboo, Ram & , Narayan & Thakkar, Sneha & Madhekar, Tanvi & Thakare, Bhushan. (2015). "Brief History of Encryption" International Journal of Computer Applications. 131. 10.5120/ijca2015907390.