7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Triple Data Encryption Standard Algorithm (3DES): A Survey

Shriya Narvekar[1], Ameya Patil[2], Jagruti Patil[3], Prof. Saniket Kudoo[4]

Department of Computer Engineering, Mumbai University, INDIA

Abstract*—Data is the fuel that drives everyone from an individual to a global company to do anything. To avoid any attacks it is necessary to secure the data by data encryption devices to preserve the data privacy and authentication. Cryptography plays a very important role in securing the data. On symmetric encryption algorithm Triple Data Encryption Standards (3DES) uniquely defines mathematical steps to transform data into a cryptographic cipher and also transforms the cipher back to the original form. The Triple DES Algorithm is one of the ways to secure and protect the sensitive data from any attacks.*

***Keywords—Cipher, Cryptography, Encryption, Secure, Triple DES*.**

I. INTRODUCTION

Today's connected society requires a secure data encryption devices to preserve data privacy. In modern days the data encryption are data privacy and authentication. Now a days society has become more connected and hence more information is available, there is a need for safeguards which bring data integrity, data secrecy and authentication in critical applications. 3DES or the Triple Data Encryption Algorithm (TDEA) was implemented to maintain such secrecy. It was developed to address the obvious flaws in DES without designing a whole new cryptosystem. The DES and TDES devices are used by the federal department and other government agencies for cryptographic protection of classified information data.

Cryptography plays a very important role in securing the data. On symmetric encryption algorithm Triple Data Encryption Standards (3DES) uniquely defines mathematical steps to transform data into a cryptographic cipher and also transforms the cipher back to the original form. By using block cipher based on two cryptographic algorithms the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA) the secret message is encrypted which may be used by Federal organizations to protect sensitive data. Triple DES Algorithm is used to develop such a system which stores data in cipher form. In this paper modern encryption algorithms such as DES and 3DES has been compared.

Three different VLSI implementations of the Triple-DES Block Cipher are presented. The two of them are based on the pipeline technique and are suitable for high-speed application needs. The other is based on the consecutive iterations and is preferred in the case that the minimized allocated resources are the major demand. Firefox and Mozilla Thunderbird use Triple DES in CBC mode to encrypt website authentication login credentials when using a master password [11].

II. RELATED WORK

A. Arya [1] described about Triple DES Algorithm has proven itself to be more secure than DES Algorithm for securing the data. With its significant key size, it is very effective against brute force attack. Triple DES Algorithm is one of the ways to achieve the satisfaction that our data is secured from any preying eyes. In this paper author use algorithm which uniquely defines the mathematical steps to transform data into cryptographic cipher and the cipher back to the original form source. R.N.S. et.al. [2] To afford the security to the network and data different encryption methods are used. Author work on different algorithms eg.DES, AES. To sum up, all the techniques which are useful for real-time Encryption.A. J. Amalraj

et.al. [3]The main objective of this approach is awareness of email security and its requirements to the common computer users. There are number techniques of cryptographic are developed for achieving secure communication. Author proposed mailing system which is secure against standard security model. Author surveyed about the existing works on the encryption techniques and also presents the performance evaluation of selected symmetric algorithms. Chris J. Mitchell [4] in this paper, the security offered by 2keytripleDES, an encryption technique that remains widely used despite recently being de-standardized by NIST.

7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

III. TRIPLE DES (3 DES) BLOCK CIPHER

3.1 DES:

Data Encryption Standard (DES) is the block cipher which coverts 64-bit plain text into 64-bit cipher text using 56-bit key. It is fixed-length string of plaintext bits and transforms into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and/or decrypt the data. In addition to preserving confidentiality, cryptography can be used for authentication, integrity, non-repudiation. Authentication means the receiver of the message can ascertain its origin, in integrity the receiver can verify if the message was modified during the transmission, the sender cannot deny the sent message in Non-repudiation.

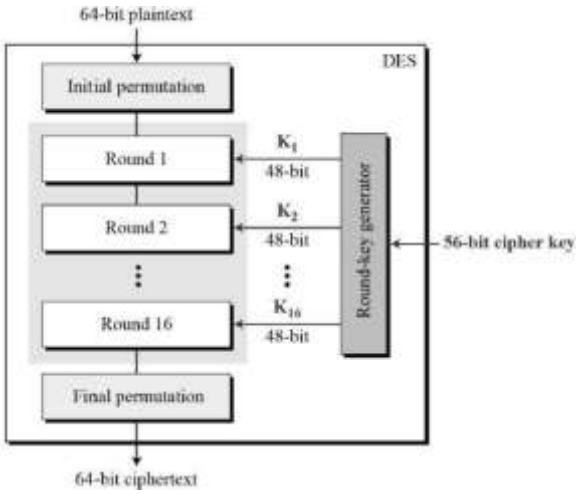

FIG.1. DES Encryption and Decryption Block Diagram

Fig.1. shows, encryption and decryption of DES.DES is a block cipher which is a symmetric key cipher which operates on fixed-length groups of bits termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 64-bit block of plaintext as input, and outputs a corresponding 64-bit block of cipher text. The secret key is use as a second input to control the exact transformation. Decryption is similar the decryption algorithm takes, in this example, a 64-bit block of cipher text together with the secret key, and yields the original 64-bit block of plaintext. To encrypt messages longer than the block size (64 bits in the above example), a mode of operation is used.

Data encryption is applied for different field, inprimarily

Electronic financial transactions: Automatic Teller Machines (devices limited to the issuance of cash or travelers checks, acceptance of deposits, or account balance reporting). Secure data communications, paving the road for e-commerce. Secure video surveillance systems. Encrypted data storage and proprietary software protection. Access control: Software or hardware which protects passwords or Personal Identification Numbers (PINs) against unauthorized access

3.2 3DES:

The DES algorithm is popular and in wide use today because it is still reasonably secure and fast. There is no feasible way to break DES, however because DES is only a 64-bit (eight characters) block cipher, an exhaustive search of 255 steps on average, can retrieve the key used in the encryption. For this reason, it is a common practice to protect critical data using something more powerful than DES. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. It is considered much safer than the plain DES and like DES, TDES is a block cipher operating on 64-bit data blocks.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

There are several forms, each of which use the DES cipher three times. Some forms of TDES use two 56-bit keys, while others use three. Triple DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. In general TDES was introduced to have three keys. Having a key length of 168 bits: three 56-bit DES keys. When it was discovered that a 56-bit key of DES is not enough to protect from attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. TDES can however work with one, two or three 56-bit keys. With one key TDES = DES. The TDES can be implemented using three DES blocks in serial with some combination logic or using three DES blocks in parallel. The parallel implementation improves performance and reduces gate count. Using standard DES encryption, TDES encrypts data three times and uses a different key for at least one of the three passes.

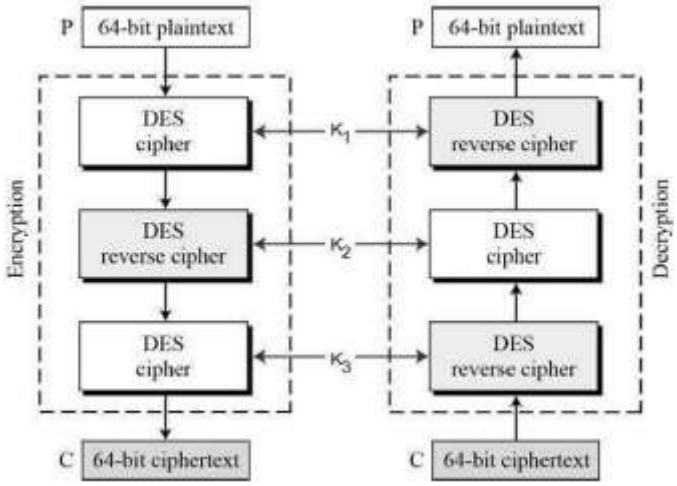

FIG. 2. 3DES Encryption and Decryption Block Diagram

The DES "modes of operation" may also be used with triple-DES. This 192-bit (24 characters) cipher uses three separate 64-bit keys and encrypts data using the DES algorithm three times. While anything less than that can be considered reasonably secure only the 192 bit (24 characters) encryption can provide true security. One variation that takes a single 192 bit (24 characters) key and then: encrypts data using first 64 bits (eight characters), decrypts same data using second 64 bits (eight characters), and encrypts same data using the last 64 bits (eight characters).Triple des is DES with three times.it comes in two flavors one that uses three keys and other that uses two keys. Triple des with three keys is used quite extensively in many products, including PGP and S/MIME to decrypt the cipher text C and obtain the plain text P. K1, K2, K3 are the DES keys each of 56 bit (excluding the parity bits).

3.3 ALGORITHM:

1. Encryption is done using first secret key K_1.
2. Decryption is done using second secret key K_2.
3. Encryption is done using third secret key K_3.
4. Cipher text (c) = $E_3 (D_2 (E_1(\text{plain text}(m))))$
   DES encrypt with K_1, DES decrypt with K_2, DES encrypt with K_3.
5. Plain text (m) = $D_1(E_2(D_3(\text{cipher text}(c))))$
   DES decrypt with K_3, DES decrypt with K_2, DES decrypt with K_1.

In each the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2 and provides backward compatibility with DES with keying option 3.

Keying option 1: all three keys are independent. 3*56= 168 independent key bits.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Keying option 2: $K_3 = K_1$, where K_1 and K_2 are independent. Provides shorter length key of 112 bits.

Keying option 3: $K_1 = K_2 = K_3$. This is backward compatible with DES.

IV. COMPARATIVE ANALYSIS

Table.1. shows the comparison was performed on the following algorithms: DES, Triple DES (3DES).

TABLE 1
COMPARISON BETWEEN 3DES, DES

Factor	3DES	DES
Key Length	(k1,k2and k3)168 bits (k1 and k2 is same)112 bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block size	64 bits	64 bits
Developed	1978	1977
Cryptanalysis resistance	Vulnerable to differential, brute force attacker could be analyse plain text using differential cryptanalysis	Vulnerable to differential and linear cryptanalysis
Security	One only weak which is Exit DES	Proven inadequate
Possible keys	95^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{14} or 95^{21}	95^{7}
Time required to check possible keys at 50 billion keysper sec	For a 112-bit key:800 Days	For a 56-bit key:400 Days

V. DISCUSSION

3DES is easy to implement in both hardware and software. It is ubiquitous: most systems, libraries, and protocols include support for it. DES is also an ANSI and ISO standard anyone can learn the details and implement it. DES run on long time hardware. It is relatively fast in software also fast in hardware. It is backward compatible with respect to single-key DES encryption. Using one key value for all three key inputs results in the same output as a single-DES encryption. It has limited error propagation. If one block of cipher text is corrupted, only two blocks of recovered plaintext will be corrupted. This is known as the self-healing or self-synchronizing property of CBC encryption. It is resistant to cryptanalytic exhaustive key search attacks. Altogether, 3DES turned out to be large and resource demanding.

VI. CONCLUSION AND FUTURE WORK

In today's era internet usage and network system is growing rapidly. Because of increase in network uses frauds also increase which leads to insecurity, so need some additional requirements to secure the data transmitted over different networks using different services. To afford the security to the network and data different encryption methods are used. In this paper, a survey on the existing paper works on the Encryption techniques like AES, DES has been done. According to research done and literature survey it can be found that 3DES algorithm is most efficient in terms of speed, time, and throughput effect. If more than one algorithm is applied to data Security provided by these algorithms can be enhanced. Triple DES Algorithm has proven itself to be more secure than DES Algorithm for securing our data. With its significant key size, it is very effective against brute force attack. So it is recommended to use Triple DES Algorithm as encryption algorithm. The used Vertex chip can be proved as well suited for the algorithm. The comparisons between the implementation are presented.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

REFERENCES

[1] A. Arya , "Security Enhancement Using Triple Des Algorithm" ,IJCSMC, Vol. 6, Issue. 4, April 2017.

[2] R.N.S et. al., "Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Cryptosystem", IJIRCCE Vol. 4, Issue 3, March 2016.

[3] R. DEBNATH et.al. , "DES, AES AND TRIPLE DES: Symmetric Key Cryptography Algorithm", IJSETR Volume 3, Issue 3, March 2014.

[4] Chris J. Mitchell, "On the Security of 2-key Triple DES", IJCSMC, Vol. 5, Issue. 8, 2016.

[5] H.O. Alanazi,et.al. , "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3.

[6] A.Azad , "Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA",International Journal of Computer Applications ,Volume 44– No16.

[7] G.Singh, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security",International Journal of Scientific & Engineering Research, Volume 4, Issue 7.

[8] R. DEBNATH et.al. , "DES, AES AND TRIPLE DES: SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM",IJSETR, Volume 3, Issue 3.

[9] Z. Yingbing et.al. "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES" IEEE, 2014.

[10] G. Singh, et.al. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security",International Journal of Computer Applications, Volume 67– No.19.

[11] https://en.wikipedia.org/wiki/Triple_DES , Last accessed on: 22nd Feb. 2019.