International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 11, November-2020

Comparative Study of Cryptographic Algorithms

Mr. Kumar K
Corresponding Author
Research Scholar, Department of Computer Science,
Vinayaka Mission's Krupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamilnadu, India.

Dr. K. Sasikala
Associate Professor, Department of Computer Science and Engineering,
Vinayaka Mission's Krupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamilnadu, India.

***Abstract*:- This paper pinpoints on the resource utilization and analysis of the performance of different cryptographic algorithms. Security is the most challenging issue that involves computers and communication and has to face prime risks. To overcome this security concern numerous cryptographic encryption procedures exists and do compare seven different algorithms namely DES, Triple DES, Blowfish, Twofish, AES and RSA.**

Keywords:- Cryptography, Symmetric, Asymmetric, Triple DES, Blowfish, Twofish, AES, RSA

1. INTRODUCTION

The conversion of plaintext to cipher text is encryption and the reverse process is decryption. The type and length of the keys depends on the encryption algorithm and the measures of security needed. The use of Single key pertains to encryption and decryption in symmetric else it is asymmetric.

With this key, the message is encrypted by the sender and is decrypted by the recipient, the key security is a challenge.

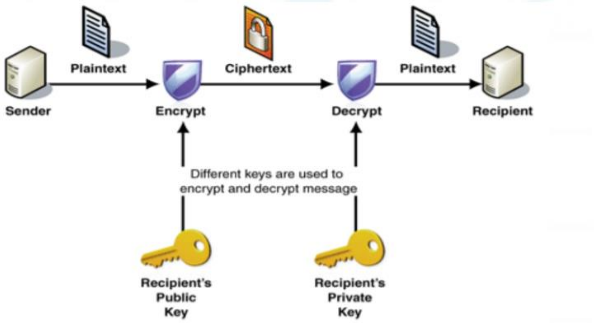

Figure 1: Key schedules for Encryption and Decryption [11]

1.1 Cryptography Goals

The security system secrecy is ensured by a set of security functions which are the aim of the system. The goals are as listed below:

- Authentication - the sender identity and the receiver identity is verified prior to sending and receiving messages.
- Confidentiality - only the people who are authenticated can read and interpret the message.
- Integrity - the message is secure from any modification between sender and receiver.
- Non-repudiation - neither the sender or the receiver cannot mistakenly refuse of sending a message
- Service Reliability and Availability - The availability and the services gets affected when intruders attack the secure systems.

1.2 Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric key block cipher. DES was found in 1972 by IBM using the data encryption algorithm. Apparently no weakness has been found yet and the only risk is brute-force. It was accepted by the government of USA as standard encryption algorithm. It has a key of 64 bits and the size of the block is 64 bits. As restriction has been put by NSA regarding usage of DES with 56-bit key size, so DES avoids 8 bits from the 64 bit keys and then compresses the 56 bit keys derived from 64 bit keys to encrypt data in a block size of 64-bits [6].

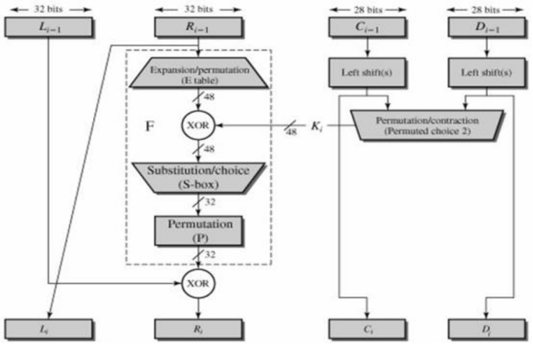

Figure 2: Encryption and Decryption using DES[12]

Algorithm

1. In the initial step, the plain text having 64 bit block is handed over to an Initial Permutation (IP) function.
2. In the plain text the IP is performed.
3. Left Plain Text (LPT) and Right Plain Text (RPT) are the two parts of the permuted block, produced by IP.
4. Each LPT and RPT performs 16 rounds of encoding.
5. At last, LPT and RPT are united and a Final Permutation (FP) is performed on the merged block

6. A 64 bit cipher text is originated.

Due to the technological advancement many intrusions and possibility to break the encrypted code was detected. To improve the security the encryption is performed thrice (3DES).

1.3 Triple DES

Triple DES was formulated to reinstate the original DES algorithm [4], which hackers learned to defeat with comparative easiness. Earlier, Triple DES, the widely used symmetric algorithm was the recommended standard in the industry. In each 56 bits, Triple DES uses three individual keys. The standard encryption method is similar to the original DES but applied 3 times to increment the encryption level. The attacks of brute force in DES as well as the attack of meet-in-the-middle occurred in 2-DES can be removed. The advantage is proven reliability and longer key size reduces the time taken to break DES and eliminates the shortcut attacks. [6]

Triple Data Encryption Algorithm (TDEA) and the standard ANS X9.52 have Block cipher with secret symmetric key and have a block length of 64 bits and the size of the key is 56 bits, 112 bits or 168 bits.

3DES was designed because DES algorithm, developed in the 1970s uses 56-bits key. The security in effect provided by 3DES is just 112 bits because of the meet-in-the-middle attacks. Triple DES executes three times slower than DES, but security aspects are more if used properly. The procedure for encryption and decrypting is the same, except the reverse execution. In DES, data is encrypted and decrypted in 64 -bit chunks. For DES the input key size is 64 bits and the actual key adopted by DES is of the size 56 bits.

The parity bit is the least significant (right-most) bit in each single byte and is set such that there is everytime an odd number of 1s in each byte. The bits of parity are avoided, so seven of the most significant bits of each byte are used, emanating in a key size of 56 bits. Hence the effective strength of the key for Triple DES is literally 168 bits due to the fact that the three keys contains 8 parity bits each that is not used during the process of encryption.

a. All keys being independent
b. Key 1 and key 2 being independent keys
c. All three keys being identical

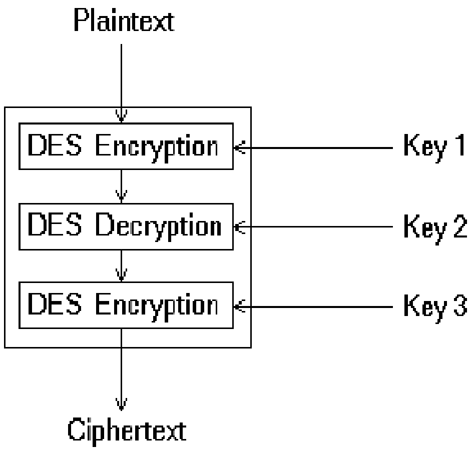

Figure 3. 3 DES algorithm execution steps[13]

Algorithm
Run DES three times:
ECB mode:
If K2 = K3, this is DES
Backwards compatibility
Known not to be just DES with K4 Has 112 bits of security, not 3 x 56 = 168

Triple DES algorithm uses three iterations of common DES cipher. It accepts a secret key of 168 bits that is divided into three keys of 56 bits.

- Encryption adopting the first secret key
- Decryption adopting the second secret key
- Encryption adopting the third secret key

Encryption: c = E3 (D2 (E1 (m)))
Decryption: m = D1 (E2 (D3(c)))

Using decryption in the second step and during encryption the algorithm provides backward compatibility within the usual DES algorithm. In these cases the first and second secret keys or the second and third secret keys are the same key combinations.

c = E3 (D1 (E1 (m))) = E3 (m)
c = E3 (D3 (E1 (m))) = E1 (m)

Hence, it is sensible to apply 3DES cipher with a secret key of 112-bits. In this case first and third secret keys are the same.

c = E1 (D2 (E1 (m)))

Triple DES is beneficial because it has a enormous sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It is derived from the single DES but the method is used in triplicate and includes three sub keys and key padding whenever necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion.[6]

Triple DES has short and weak encryption keys and has shorter block size. AES has a better encryption mechanism and hence the performance.

1.4 Blowfish

Blowfish encryption algorithm needs a 32-bit microprocessor with one byte for each 26 clock cycles. Blowfish holds 16 cycles. Each round consists of XOR operation and a function. Every single round comprise of key expansion and the encryption of data. Key expansion is generally used for making the primary contents of one array and data encryption uses a 16 rounds Feistel network methods. [4] Plain text and key are the inputs of this algorithm. A 64-bit plain text taken is divided into two 32 bits data and at each round the given key is expanded and stored in 18 p-array and gives 32 bits key as input and XORed with previous round data.

```
Then, for j = 1 to 14:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
```

After the sixteen rounds, swap xL and xR again to undo the last swap. Then, xR = xR XOR P15 and xL = xL XOR P16. Finally, merge xL and xR to obtain the ciphertext

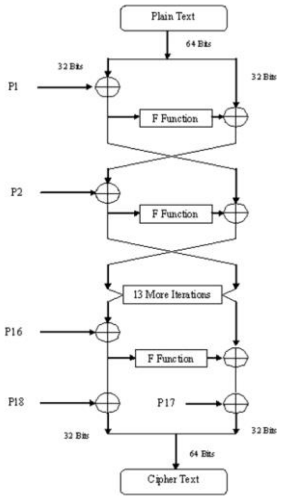

Figure 4: Blowfish encryption and decryption algorithm[14]

The Encryption and Decryption is precisely the same process, except that P1, P2 so on until P18 are applied in the reverse order.

Blowfish algorithm minimized the number of cycles and each single round is introduced new modified. In the blowfish there are 64 bits, the bits are partitioned into 32 bits and there are four s-boxes and each s-box contains 32 bits. The algorithm is designed with two s-boxes connecting with XOR and other two 2 s-boxes connects with XOR and then from the two XORs added then from there get key plain text.

1.5 Twofish

Two fish is a popular algorithm for encryption regularly used in cryptography. Twofish originates from Blowfish algorithm. Twofish is a 128-bits block cipher capable of manipulating variable length key up to 256 bits. [2]

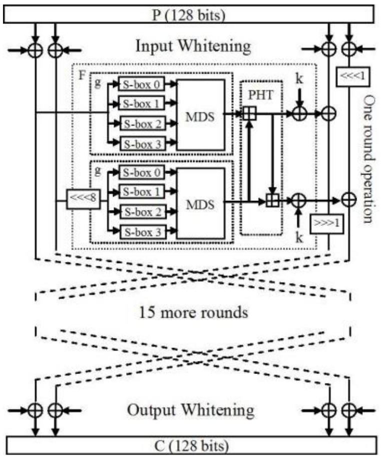

Figure 5: Twofish encryption and decryption algorithm[15]

The phrases used in Twofish are:

1.5.1 Fiestal Network

Functions are transformed to permutations. Horst Fiestal [9] invented this design of Lucifer and propelled by DES. The constituent of Fiestal network is the F-function. It maps an input string to an output string using a key.[2]

1.5.2 Diffusion

A minimal change in the plaintext affects many bits of the ciphertext to maintain convolution between plain and ciphertext. Diffusion is attained by executing a certain permutation and carry out a functional operation. [10]

1.5.3 Confusion

The relationship among the cipher text and sub key can be made complex by creating “confusion” by handling relations. [10]

1.5.4 S-boxes

An S-box is a table-driven non-linear replacement function used in almost all block ciphers. The input size and output size respectively of S-boxes change and will be created randomly or algorithmically. [7]

1.5.5 MDS Matrices

A Maximum Distance Separable (MDS) [7] code is a linear mapping from the elements of the *a* and *b* field over a stipulated field, thereby creating a composite vector of *a* + *b* elements, which has the property of the minimum number of non-zero elements in any vector which is non-zero is atleast b + 1 [8]. Reed-Solomon (RS) error-correcting codes are known as MDS. An inevitable condition for a x b matrix to be MDS is that all mixture of square sub matrices, procured by discarding rows or columns, are non-singular.

1.5.6 Pseudo Hadamard Transforms

A pseudo Hadamard transforms (PHT) [7] is a simple operation that mixes and runs quickly in software. It is applied for diffusion. For given two inputs a & b, the 32-bit PHT is defined as

$$a_0 = a + b \bmod 2^{32} \text{…..(1)}$$
$$b_0 = a + 2b \bmod 2^{32} \qquad \text{…...(2)}$$

1.5.7 Whitening

Whitening [7], the method of XORing key material prior to the first round and beyond the last round. It was observed that whitening substantially increases the difficulty of key search attacks against the remainder of the cipher.

1.6 RSA

This is public key encryption algorithm developed by Ron Rivest, Adi Shamir and Leonard Adelman in 1977. It is the well-known asymmetric key algorithm for cryptography. It may use to provide both secrecy and digital signature. RSA applies the prime number to generate the public and private key based on mathematical fact and taking the product of large numbers together. The algorithm implements the block size data where plaintext and cipher text are integral values between 0 and n1 for some values of n. The length of n is observed to be 1024 bits or 309 decimal digits. Apparently two distinct keys are used for encryption and decryption purposes. The sender knows encryption key and receiver knows decryption key.

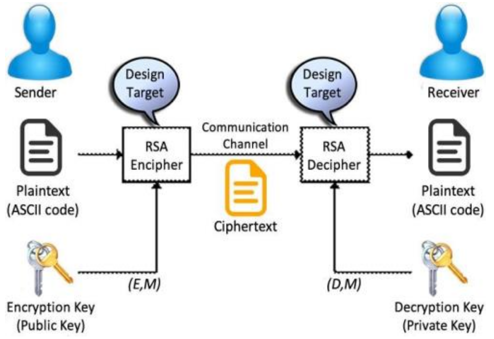

Figure 6. RSA encryption and decryption algorithm[16]

Algorithm:

Choose large prime numbers r and s such that r~=s.
Compute n=r*s
Compute φ (rs) = (r-1)*(s-1)
Choose the public key e such that
gcd (φ (n), e) =1; 1<e< φ (n)
Select the private key d such that
d*e mod φ (n) =1
So in RSA algorithm encryption and decryption are performed as-
Encryption
Calculate cipher text CT from plaintext message M such that
CT=M ^e mod n
Decryption M=CT^d mod n=M^ed mod n

1.7 Advanced Encryption Standard (AES)

U.S. Government and different other organizations have acquired the Advanced Encryption Standard (AES) algorithm as a reliable standard. [1] It is highly efficient in 128-bit form, the algorithm uses keys of 192 and 256 bits for heavy duty encryption purposes is quite considered sealed to all attacks, with the exclusion of brute force, which strive to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. The experts of security trust that AES will be finally addressed as the actual standard for encryption of data in private sector.[1][5]

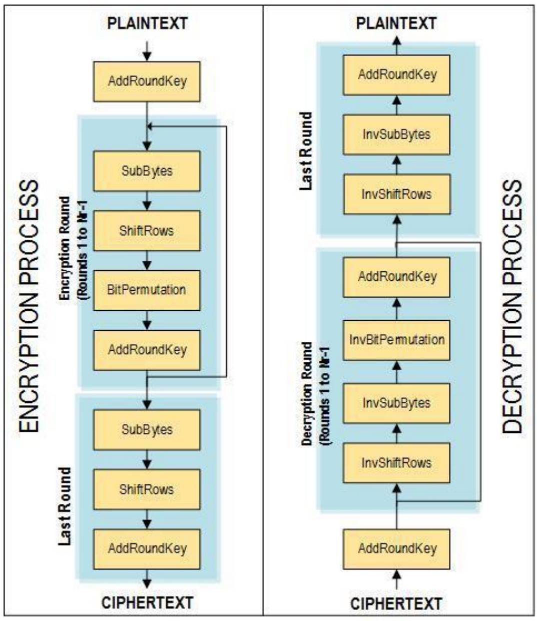

Figure 7. AES algorithm processing steps[17]

Algorithm

1. “SubBytes”, a non-linear transformation is a substitution of bytes for each byte of the block.
2. “ShiftRows” transformation iteratively shifts (permutes) the bytes inside the block
3. “MixColumns” transformation binds the 4-bytes together thereby forming the 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1).
4. “AddRoundKey” transformation along with the data block will add the round key.

The iterated transform (or round), in most ciphers, generally have a Feistel Structure. Normally, in this structure, the transitional state bits are transposed without changing the value to another position (permutation). AES lacks a Feistel structure but have three distinct invertible transforms based on the Wide Trial Strategy design method.

Table of Comparison

Algorithm	DES	Triple DES	Blow Fish	Two Fish	AES	RSA
Author	IBMers	Diffie and Hellman	Bruce Schneier	Bruce Schneier	Vincent Rijmen and Joan Daemen	Ron Rivest, Adi Shamir, Leonard Adleman
Developed	1977	1995	1993	1998	2001	1977
Cipher Type	Symmetric block	Symmetric block	Symmetric block	Symmetric block	Symmetric block	Asymmetric block
Key Length (Bits)	54	56, 112 or 168	32 - 448	128, 192 or 256	128	1024 - 4096
Block Size (Bits)	64	64	64	128	128	Variable
Mathematical operation	XOR ,Fixed S-boxes	XOR ,Fixed S-boxes	Logical XOR,Addition,Modulo Arithmetic	XOR	Substitution byte, Shift row, Mix-column and Addround key	Exponentiation and Modulo Arithemetic
No: of rounds	16	48	16	16	10, 12 or 14	1
No: of sub keys	16	48	18	-	16	-
Structure	Feistel	Feistel	Feistel	Feistel	Substitution-permutation	Factorization
Speed	Slow	Very Slow	Fast	Fast	Fast	Slow
Power Consumption	Low	Low	Low	Low	Low	High
Security	Not Secure Enough	Not Secure Enough	Least Secure	More secure	Adequately Secure	Least Secure
Features	Most Common, Not Strong Enough	Modification of DES ,Adequate Security	Excellent Security		Replacement of DES, Excellent Security	
Flexibility	No	Yes	Yes	Yes	Yes	Yes
Type of Attacks	Brute Force Attack	Brute Force Attack, Chosen Plaintext, Known Plaintext	Dictionary Attack	Impossible Differential Attack	Side Channel Attack	Factoring the public key

3. CONCLUSION

Cryptographic techniques and tools do play a vital role in designing emerging network security technologies. Among the discussed five algorithms AES is best in terms of energy consumption, performance and resource utilization. AES algorithm is brisky, and is best adapted for use in both hardware and software environments.

REFERENCES

[1] "Advanced Encryption Standard", http://en.wikipedia.org/wiki/Advanced_Encryption_ Standard". (accessed on November 8, 2015).

[2] Verma, Harsh Kumar, and Ravindra Kumar Singh. "Performance analysis of RC6, Twofish and Rijndael block cipher algorithms." International Journal of Computer Applications 42, no. 16 (2012): 1-7.

[3] Munoz, Pedro Sanchez, Nam Tran, Brandon Craig, Behnam Dezfouli, and Yuhong Liu. "Analyzing the resource utilization of AES encryption on IoT devices." In 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 1200-1207. IEEE, 2018.

[4] Gowthami Saranya, R., and A. Kousalya. "A comparative analysis of security algorithms using cryptographic techniques in cloud computing." Int J Comput Sci Inf Technol 8, no. 2 (2017): 306-310.

[5] Landge, A. R., and A. H. Ansari. "RSA algorithm realization on FPGA." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2 (2013).

[6] Karthik, S., and A. Muruganandam. "Data Encryption and Decryption by using Triple DES and performance analysis of crypto system." International Journal of Scientific Engineering and Research 2, no. 11 (2014): 24-31.

[7] Schneier, Bruce, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. "Twofish: A 128-bit block cipher." NIST AES Proposal 15, no. 1 (1998): 23-91.

[8] MacWilliams, Florence Jessie, and Neil James Alexander Sloane. The theory of error-correcting codes. Vol. 16. Elsevier, 1977.

[9] Feistel, Horst, William A. Notz , and J. Lynn Smith. "Some cryptographic techniques for machine-to-machine data communications." Proceedings of the IEEE 63, no. 11 (1975): 1545-1554.

[10] Su, Shun-Lung, Lih-Chyau Wuu, and Jhih-Wei Jhang. "A new 256-bits block cipher 耩 Twofish256." In 2007 International Conference on Computer Engineering & Systems, pp. 166-171. IEEE, 2007.

[11] https://www.semanticscholar.org/paper/Data-Encryption-and-Decryption-by-Using-Triple-DES-Karthik/e5754799bc8ae8b3ab8e1bb803c12fba95e38a4a/figure/1

[12] https://www.thecrazyprogrammer.com/ wp-content/uploads/2019/01/Single-Round-of-DES-Algorithm.png

[13] https://www.researchgate.net/profile/ Ugrasen_Suman/publication/281448815/figure/fig1/AS:284461158682624@1444832233072/Triple-DES-Algorithm.png

[14] https://www.sciencedirect.com/science/article/abs/pii/S0026269210000595

[15] https://www.intechopen.com/books/data-acquisition-applications/reconfigurable-systems-for-cryptography-and-multimedia-applications

[16] https://www.researchgate.net/profile/Hueseyin_Bodur/publication/298298027/figure/fig2/AS:339820552441867@1458030941634/RSA-algorithm-structure.png

[17] https://www.researchgate.net/profile/Isaac_Kofi_Nti/publication/314368854/figure/fig1/AS:469924452802560@1489050128453/Overall-Structure-of-AES-Algorithm-Source.ppm