A Survey on Cryptography Algorithms

Article *in* International Journal of Scientific and Research Publications (IJSRP) · July 2018

DOI: 10.29322/IJSRP.8.7.2018.p7978

2 authors:

Omar G. Abood
Alexandria University
22 PUBLICATIONS **55** CITATIONS
SEE PROFILE

Shawkat Guirguis
Institute of Graduate Studies & Research, Alexandria University, Egypt
39 PUBLICATIONS **124** CITATIONS
SEE PROFILE

A Survey on Cryptography Algorithms

Omar G. Abood, Shawkat K. Guirguis
Department of Information Technology Institute of Graduate Studies and Researches, Alexandria University, Egypt.
Corresponding author: omar.ghazi88@yahoo.com

DOI: 10.29322/IJSRP.8.7.2018.p7978

http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7978

Abstract- With the major advancements in the field of technology and electronics, one persistent obstacle has proven to be one of the major challenges, namely : Data Security. To get connected securely and quickly through the electronic data transfer through the web, the data should be encrypted. Encryption is the process of transforming plain text into ciphered-text, which cannot be understood or altered easily by undesirable people. It can also be defined as the science that uses mathematics in data encryption and decryption operations. In this paper, we discuss several important algorithms used for the encryption and decryption of data in all fields, to make a comparative study for most important algorithms in terms of data security effectiveness, key size, complexity and time, etc. This research focused on different types of cryptography algorithms that are existing, like AES, DES, TDES, DSA, RSA, ECC, EEE and CR4…etc.

Index Terms- Cryptography, Information Security, Encryption, Decryption.

I. INTRODUCTION

Information security can be summed up to info, a group of steps, procedures, and strategies that are used to stop and observe illegal access, trouble-shooting, revelation, perturbation and adjustment of computer network sources. Enhancing the privacy, eligibility and reliability of the work requires a lot work to strengthen the current methods from constant trials to break them and to improve new ways that are resistant to most kinds of attacks if not all [1].

Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since the ancient days of the Romans who used similar methods to enable security on their valued information and documents. Data encoding is the process of changing the form of the data into certain symbols through the use of meaningless codes. The process of encoding and decoding depends solely on a single key which is known as identical key cryptography. In this process, the same key is used for both the processes of encryption and decryption. A safe channel is needed between the sender and the receiver to commute the secret key. Double cipher modes are tackled by a symmetric algorithm: block cipher and stream ciphers. The block cipher works on fixed-length groups of bits, named blocks, without transformation specified by a symmetric key. A stable

shape is handled by a bunch of block ciphers. It contains of many similar rounds of processing wherein each round, a substitution is done on one half of the information tackled, followed by a permutation that intermingles with the two halves. The basic key becomes larger, so the multi-label keys are used for every round. A symmetric key cryptography points to the cryptographic algorithm that needs two different keys: the first of which is hidden whereas the other is public [1].

Though they are not the same, but they are mathematically connected. The public key is used to encode a plain text, while the private key is used for the decoding of the cipher text. In [2], the asymmetric enciphering strategies are roughly 1,000 times slower than symmetric encoding, which makes it unfeasible upon encoding big amounts of information. Additionally, to have similar security power as the symmetric algorithm, the asymmetric algorithms most use more powerful keys than symmetric enciphering step. The category of main encoding techniques is illustrated in Figure1.

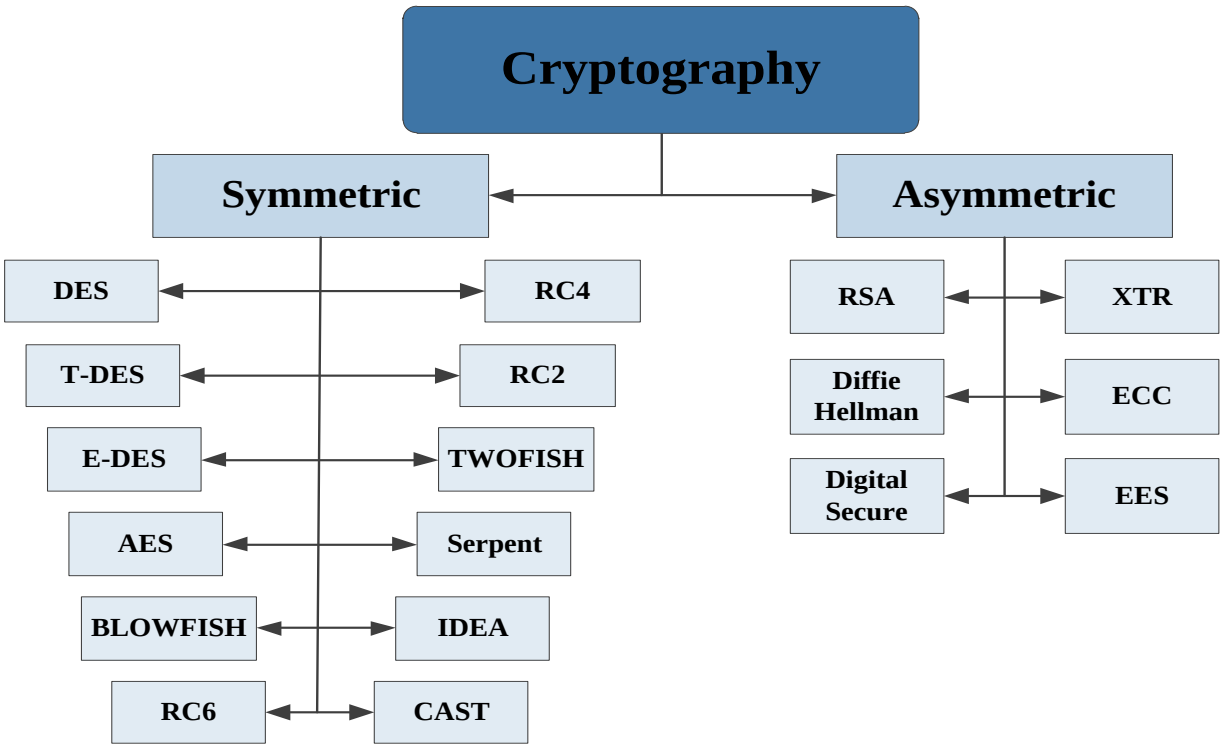


Figure 1: THE CLASSIFICATION OF ENCRYPTION ALGORITHMS

A. Encryption and Decryption:

Encryption is altering the database into non-recordable text. Decryption presents the reverse process of encryption where it converts the cipher text to an ordinary text. A cipher is double algorithms, which invents the encoding and decoding processes.

The extensive process of a cipher is dominated by the algorithm and a key. It is secret, a brief group of symbols, that would decode the encrypted data [3].

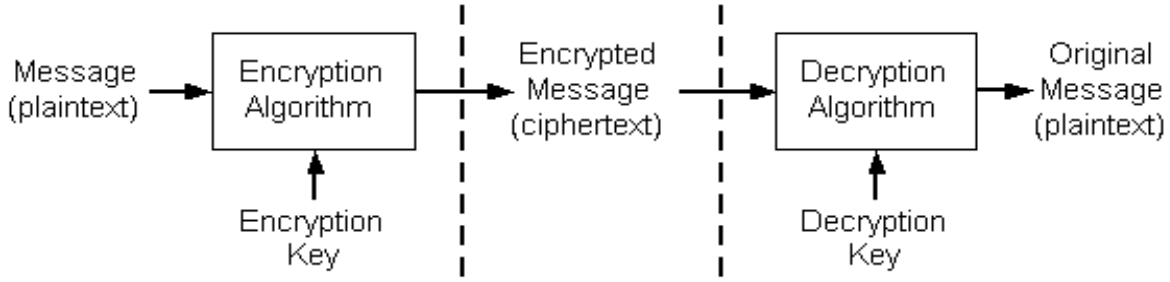


Figure 2: PROCESS OF ENCRYPTION AND DECRYPTION

B. Goals of Cryptography:

Cryptography is used to achieve many goals and some of the goals are the following list shows:

- **Authentication:** is the process of offering identity to a person to break special resource using keys.
- **Confidentiality:** is the ultimate target of encryption that confirms that only the cipher-key owner receives the message.
- **Data Integrity:** is the operation that has the access of modulating the database that belongs to a specific group or person.
- **Non-Repudiation:** ensures that both the sender and receiver acknowledge the delivery of the report.
- **Access Control:** confirms that only the group with correct authentication is eligible to log into the delivered message.

C. Terminology:

Term	Explanation
Plain Text	the ordinary message that will be delivered to the other side
Cipher Text	The original text is encoded into a symbolic format
Encryption	The technique of changing the ordinary text into unreadable message
Decryption	It is the opposite operation of the last one
Key Size	To encode and decode, key is essential, and the length of the key determines the degree of safety the more the key size, the more the security is
Block Cipher	It encrypts a group of plaintext symbols as are block

Stream Cipher	It converts one symbol of plaintext directly into symbol of cipher text
Encryption Time	The of processing the ordinary text into an encrypted one
Decryption Time	The period of decoding the decrypted message into readable text
Throughput	The amount of time passing through enciphering measured in megabytes

D. Description of Cryptographic Algorithms:

There are two kinds of encoding. Those two types are the symmetric and asymmetric encoding algorithms. Several of those algorithms will be included herein such as: AES, DES, 3DES, E-DES, BLOW FISH, SEAL, RC2, RC4 and RC6 which all have to do with bilateral algorithms. In contrast to RSA, ECC, EEE, DH, ELGAMAL ALGORITHM and DSA, which are relevant to unilateral algorithm.

1. DES

DES was first introduced in IBM by Horst Fiestel in the year 1972. The goal of the DES algorithm is to offer a strategy to secure crucial financial database [4]. The encipher instructions are:

- DES receives data of 64-bit long ordinary message and 56 bit key and comes up with 64-bit block.
- The ordinary text block needs to modulate the bits.
- The 8 similar bits are eliminated from the key through exposing the key to its key permutation.

The readable message and the key will be produced as the following steps show:

- ❖ The key is divided in to two 28 halves.
- ❖ The half is rotated by one or two bits, according to the round.
- ❖ The two parts reunite and undergo to the round permutation to decrease the key from 56 bits to 48 bits. These pressed keys are used to encode the round's plaintext block.
- ❖ The shitted key parts from tip 2 are used in the coming round.
- ❖ The database block divides inti two 32-bit parts.
- ❖ A part will be expanded in terms of permutation to raise the size to 48 bits.
- ❖ Result of the sixth step is for OR'ed only, with 48 bit key from tip number three.
- ❖ The outcome of 7^{th} instruction is set s-box, that replaces key bits and cut down the 48-bit block to 32 bits.
- ❖ The consequence of the 8^{th} tip, will be permuted by p-box.
- ❖ The result of the p-box belongs to OR'ed solely, will the next part of the format block. The bipartite format parts are exchanged and form reservoir of the coming stage **[4].**

These steps are clarified in the table below Figure 3.

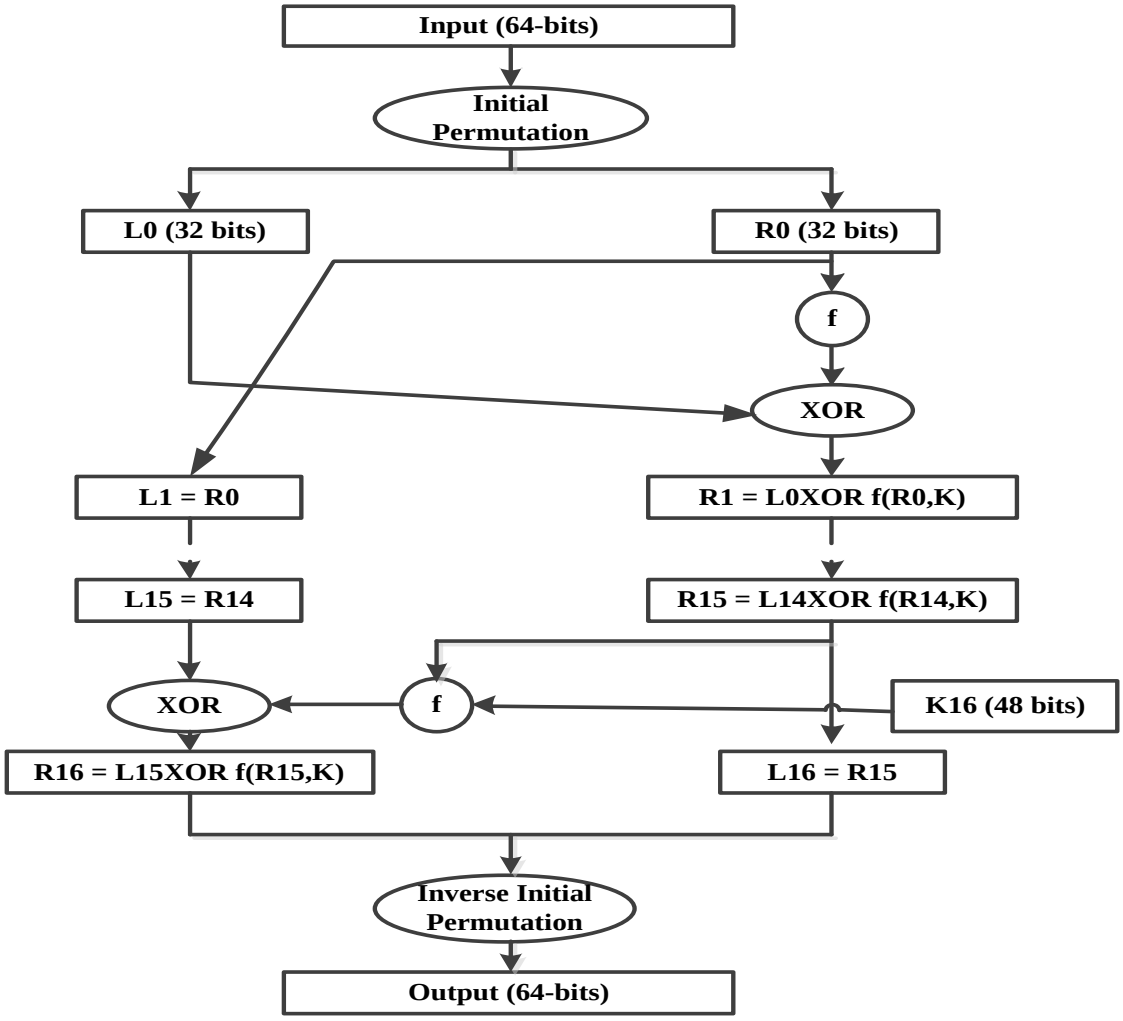


Figure 3: DES ALGORITHM FLOWCHART

2. Advanced Encryption Standard (AES)

AES is an up-to-date ciphering strategy suggested by NIST to substitute DES back in 2001. AES could provide any group of databases [5]. During encryption-decryption, the AES process encodes 10 rounds for 128-bit keys. 12 rounds for 192-bit keys and 14 rounds to 256-bit keys to come out with the last encoded message [6]. AES allows in 128-bit information length that can be split into 4 fundamental active blocks. Those parts are dealt with as a line of bytes and combine a matrix of 4∗4 named “the state”.

For encoding and decoding, the cipher starts with an “Add round key stage”. However, soon before the eventual round, the output encounters 9 basic rounds, through each 4 transformations take place; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns and 4) Add round Key.

In the last tenth round, mix columns transformation is not available [7] [8]. The entire operation is Figured out in Figure 4. Decryption is the opposite process and uses opposite steps **[9]:**

a- Substitute Byte transformation:

AES consists 128-bit data block, that is to say every database item has 16 bytes. In sub-byte transformation, every bite of a data item is changed in other piece by implementing 8-bit substitution box known as the Rijndael s-box.

b- Shift Rows transformation:

This transposition is easy, the bytes in the rest three lines of the state, reliable on the row position, are shifted in a cycle way. In the second line, 1-byte circular left shift is done. While the third and fourth row, two bytes and three byte left circular shifts take place successively.

c- Mix columns transformation:

Here the is counterpart to a multiplication set of every column of the states. A stable matrix is multiplied to every. In this process bytes are dealt with as multi-names.

d- Add round key transformation:

A bit-like XOR between 128-bits of current state and 128-bits of the round key. This transmutation is the opposite.

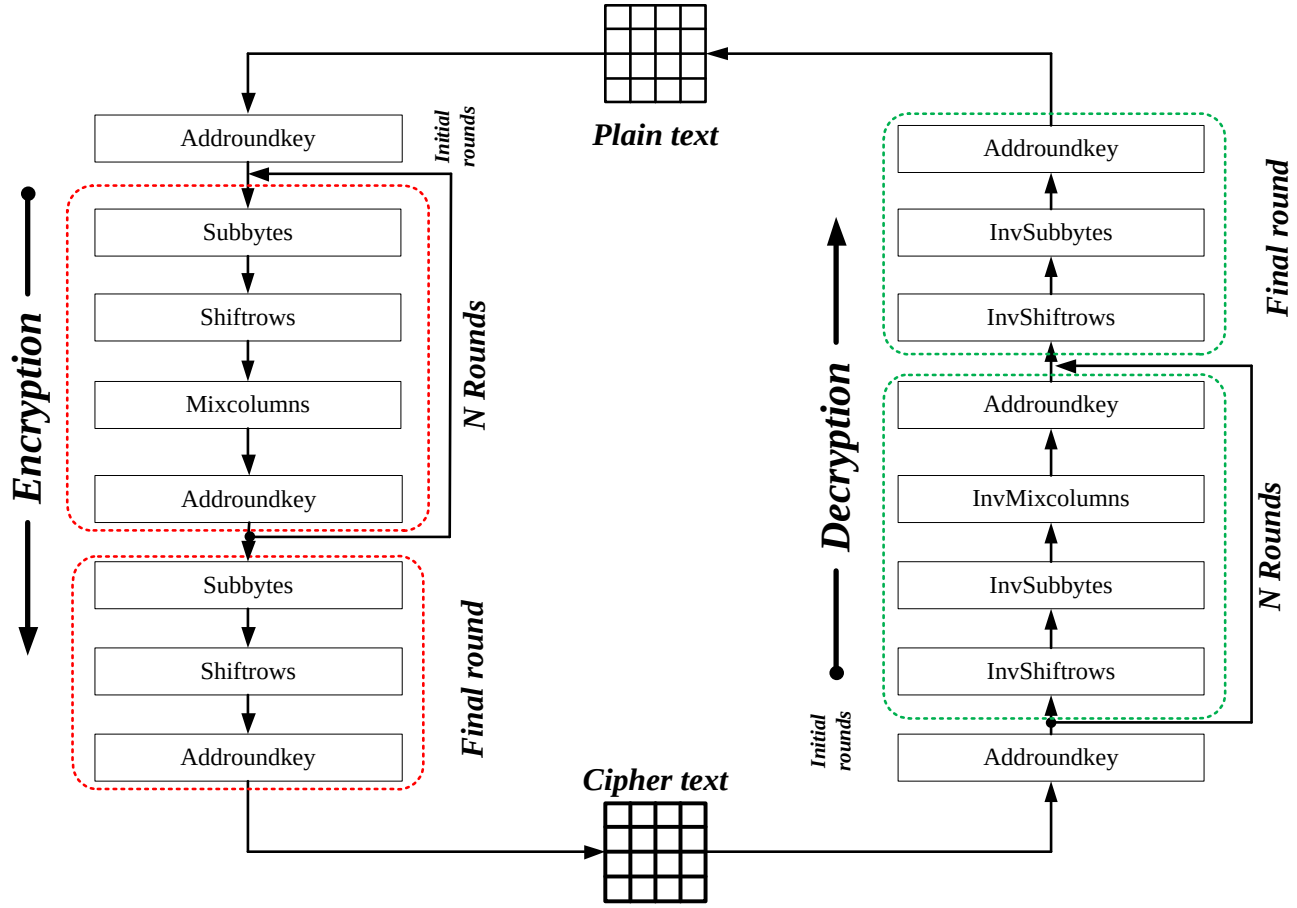


Figure 4: ADVANCED ENCRYPTION STANDARD PROCESS [9]

3. Triple DES (3DES)

The Triple Data Encryption Algorithm (TDEA or 3DES) was developed to tackle the flaws in DES whilst preserving the same cryptography. 3DES key size of DES (56-bit). This is through implementing the algorithm triple successively with 3 multiple keys. The total size is 168 bits. TDEA uses triple 64-bit DEA keys (K1, K2, K3) in the encode-decode-encode (EDE) state [5]. The standards define three major choices:

- The 1st choice is the preferred one (K1≠K2≠K3≠K1).
- The 2nd choice uses dual independent keys (K1≠K2&K3≠K1).
- The 3rd choice uses triple similar keys (K1=K2=K3).

Those choices are equivalent to DES Algorithm. In 3DES, the 3-times iteration is applied to increase the encoded level and average time. It is a known fact that 3DES is slower than other block cipher methods [11].

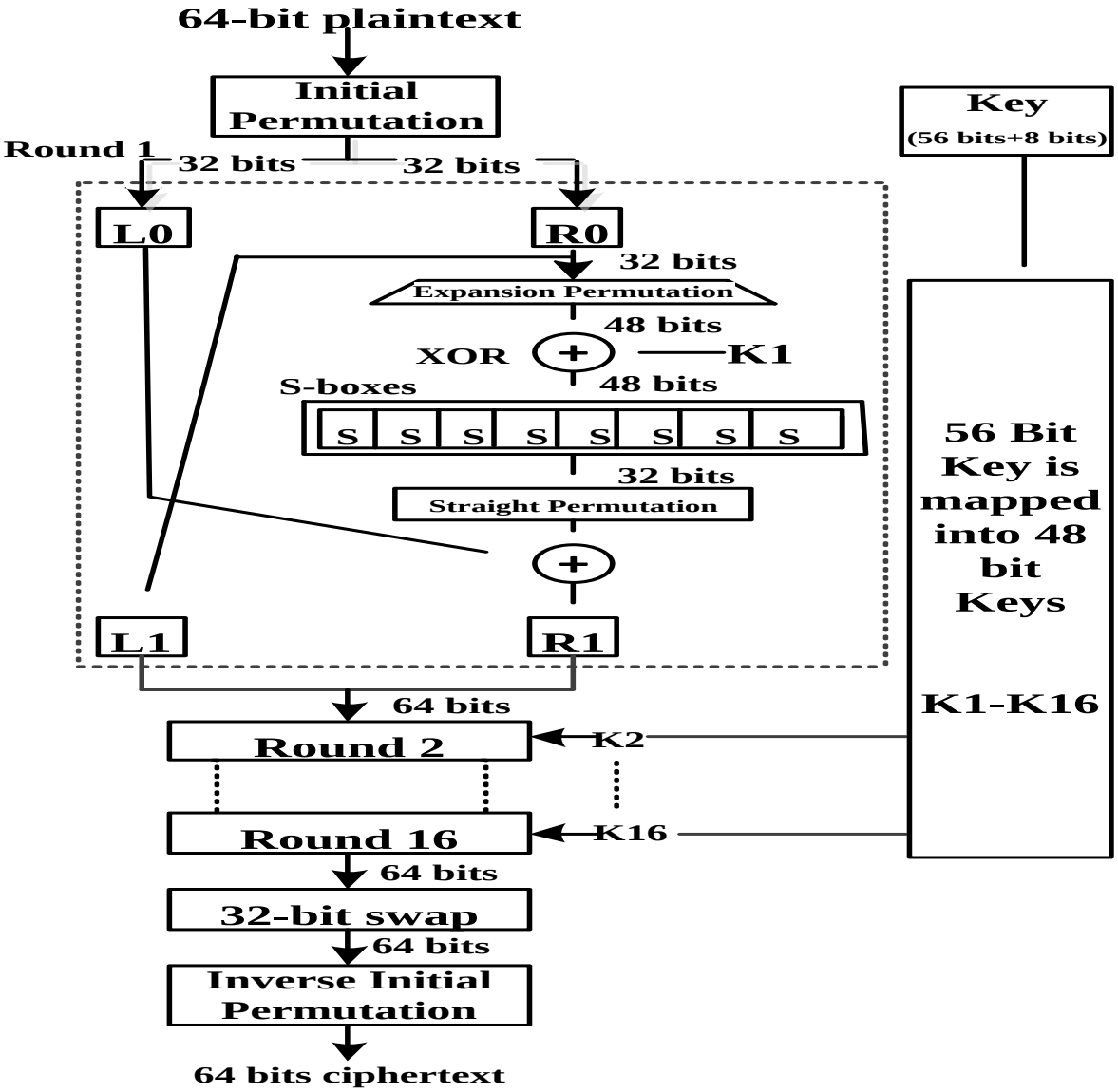


Figure 5: GENERAL DEPICTION OF DES

4. Educational Data Encryption Standard (E-DES)

It is used as a support for DES [10]. The fundamental transformations suggested to apply E-DES, which has larger key and block size a developed F function, enhanced key program and extra complicated permutation tasks [1]. Aside from that, the suggested cipher implements one of the contents from AES, which is the substitution box. E-DES depends mainly on the Feistel

network with sixteen rounds, in which the 1st process is the implementation of the primitive-permutation of the plaintext. After that, each round composes of the following:

1. The permuted plaintext is divided into 2 parts, left and right.
2. The right one shifts to the left straight forward, and the left one is XOR'ed with the output of the function F.

Finally, after sixteen rounds, the opposite primitive permutation is done, coming up with the ciphered text block. This process is explained below Figure [6]. The basic distinction between the recommended S-box in E-DES and the usage of the

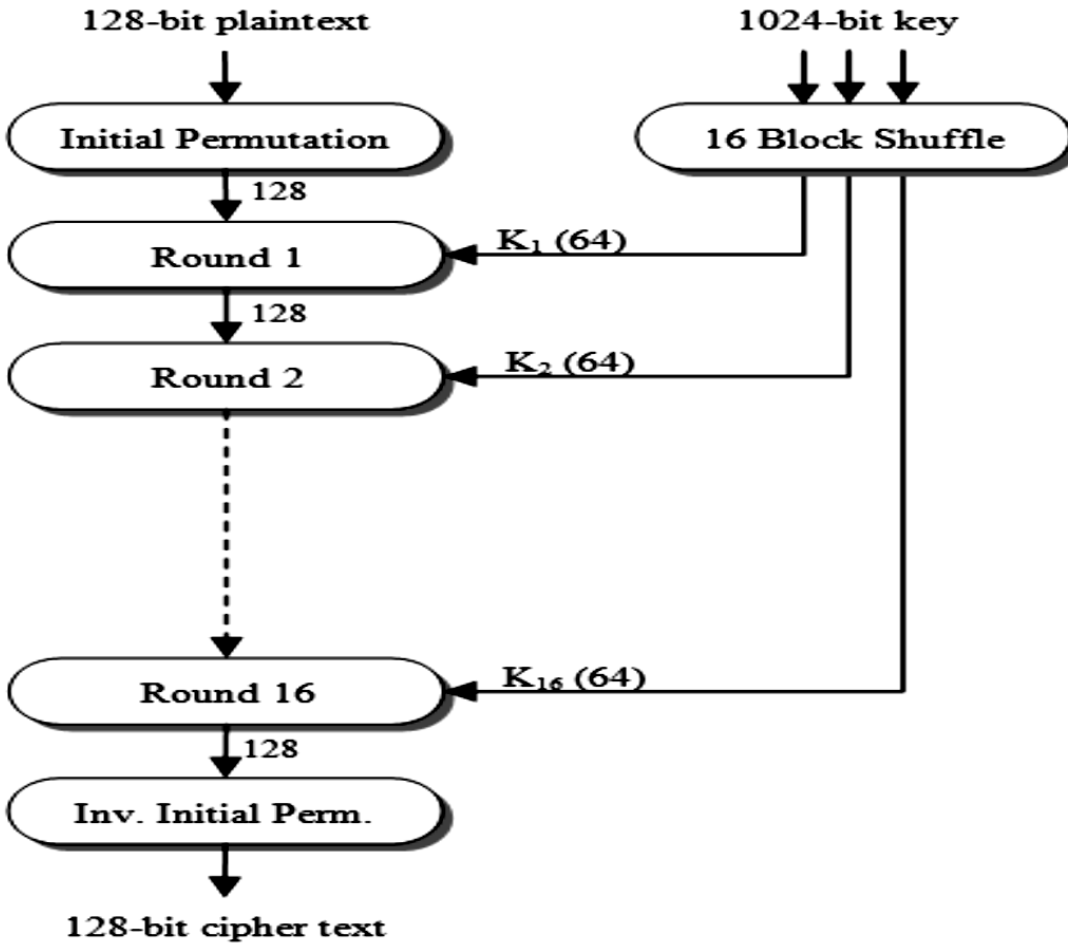
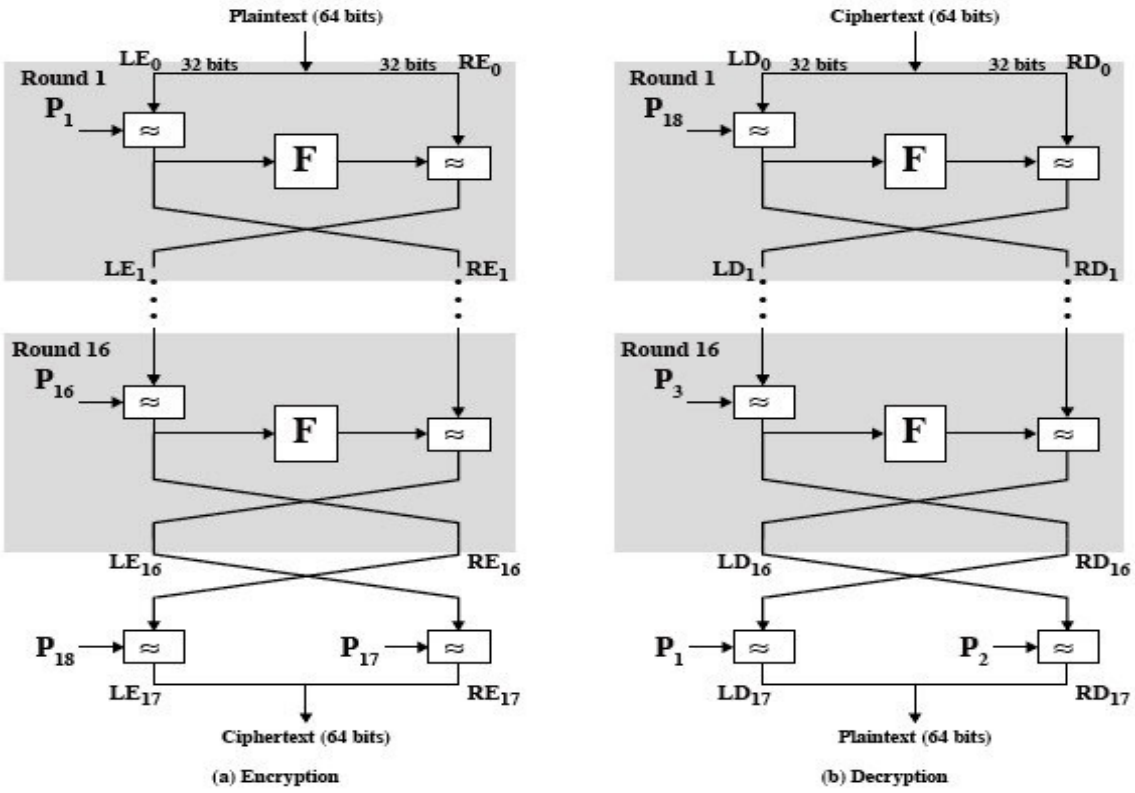


Figure 6: GENERAL ENCRYPTION STRUCTURE

S-box in AES is the reliability between the varied S-box suggested for every 8-bit blocks. Every substitution box, that gets 8-bits input and results in eight bits output, composed of sixteen lines and sixteen columns bytes [1].

5. Blowfish Encryption

Ultimately, the Blowfish ciphering algorithm needs 32-bit microprocessor at an average of one byte for each twenty-six-hour cycles. Blowfish consists of sixteen rounds. Each round has the XOR process and a task. Also, the round contains key



expansion and database encoding. The key for stimulating primitive ingredients of one round and database encoding applies sixteen rounds feiestel network strategies [15]. Figure 7 explains how blowfish algorithm functions.

6. SEAL Algorithm

SEAL is a length-raising "illusive random" that depicts 32-bit string N- to L-bit string SEAL under a hidden 160-bit key. The output length L is intended to be diverse; however, in general bound to 64 kilobytes. It equals 64 kilobytes (214 32-bit words). However, the results can be deducted with a smaller output length [16]. The key usage is to Figure out 3 secret charts: R, S, and T; these charts have 256, 256 and 512 32-bit values respectively that are induced from the Secure Hash Algorithm (SHA)

Figure 7: BLOWFISH ENCRYPTION AND DECRYPTION ALGORITHM [15].

[17] applying a as the hidden key and re-archiving the 160-bit output to 32-bit output words. SEAL is the fruit of the dual shower source clarified. The first generator implements a systematic relies on the deducted charts R and T depicted at Figure 8. It maps the 32-bit string n and the 6-bit counter.

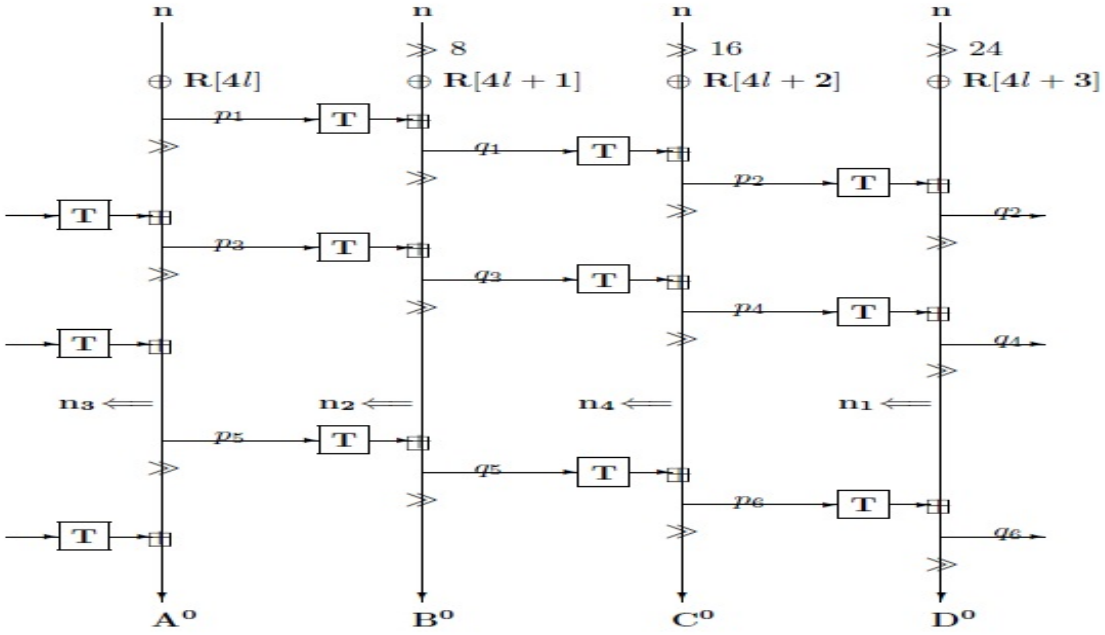


Figure 9: THE FIRST GENERATOR OF SEAL

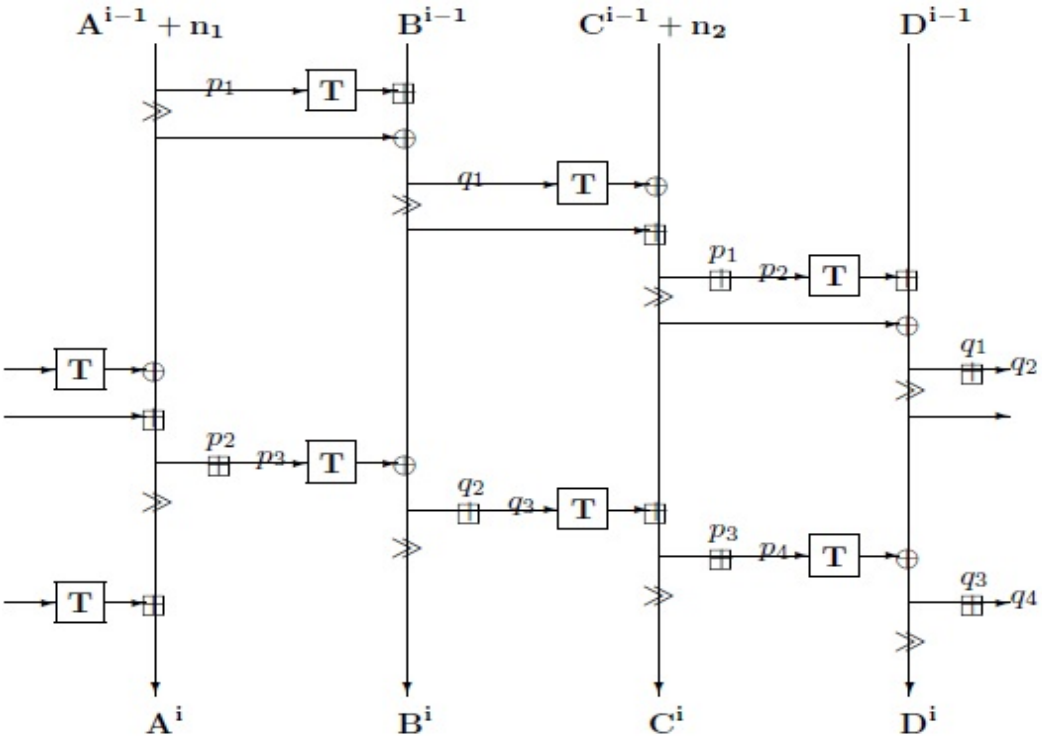


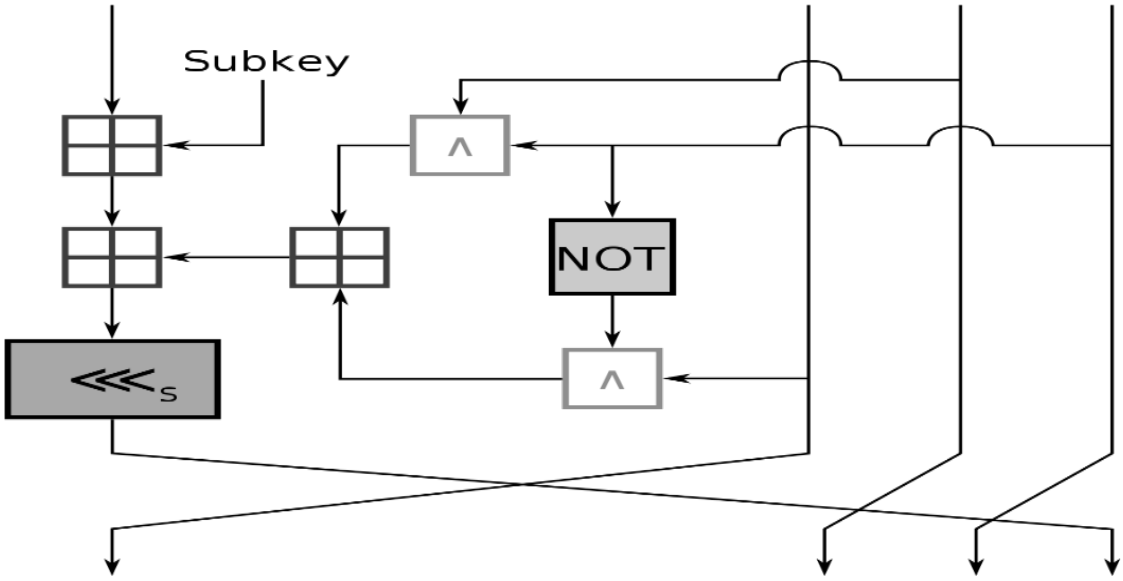
Figure 8: THE SECOND GENERATOR OF SEAL (ITH ITERATION)

The second source applies a system, relying on the deducted charts depicted at Figure 9. There are extra explanation of SEAL and details in [17] [18]. The algorithms have 3 steps:

1. The interior charts under the secret key (a) are computed.
2. A0, B0, C0, n1, n2, n3, and n4 from n1 and chart R are computed.
3. The 2nd source moves the Ai, Bi, Ci, and Di blocks.

7. RC2

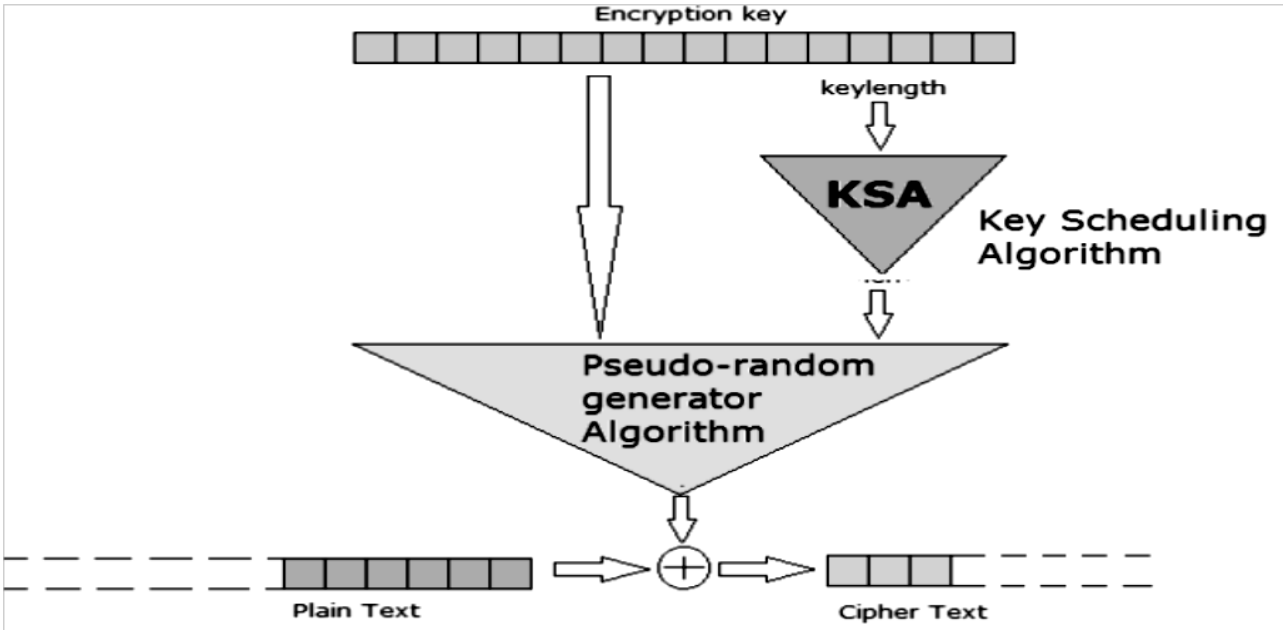
RC2 is a block encoding algorithm that was introduced all the way back in the year 1987. It is meant to replace the DES. RC2 applies exclusive size key from 1 byte to 128 bytes. Both the input and output block size of 64-bit per one. This algorithm



was set to apply on 16-bit microprocessors. In the case having the encoding already done, the algorithm would work twice as fast as the DES on IBM [19].

8. RC4

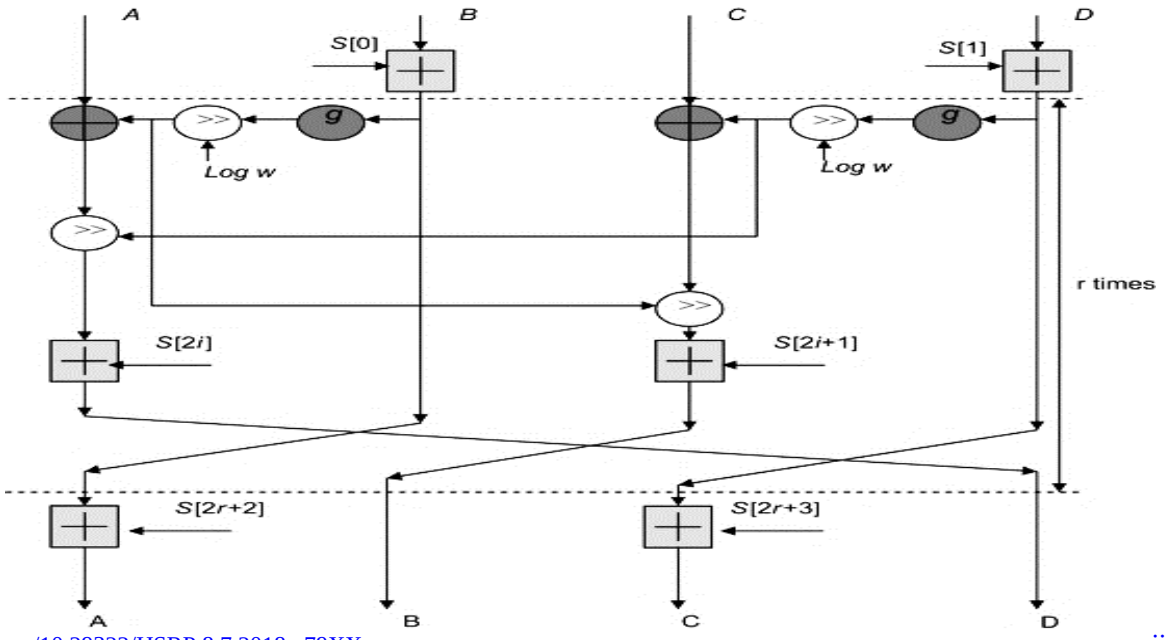
It is a stream cipher, symmetric key encoding algorithm. The algorithm is mutual for both encoding and decoding. The database stream is XORed with group of generated keys. The key stream does not rely on plaintext ever. Vernam stream cipher



is quite common, because of its simplicity. It is used in SSL and WEP. The WEP stands for Wireless Equivalent Privacy which is protocol also used the RC4 algorithm for confidentiality. It was counted safe till it was violated by BEAST attack [19].

9. RC6

RC6 was introduced in 1997. It is a block cipher that applies 128-bit block size and provides 128, 192 and 256-bit key



sizes. Additionally, RC6 aims to meet the demands of AES. It is proven to be better than the RC5 algorithm as it offers more security from attacks. RC6 uses four registers. It also needs less rounds and give more throughout [19].

10. RSA

RSA was invented by Ron Rivest, Adi Shamir and Leonard Adleman back in 1978. It is one of prominent public key encoding systems for key exchange, digital signatures or encryption of blocks of database. The RSA algorithm implements different size encoding block and a variable size key. It is an asymmetric encoding system that relies on numeral synthesis. It employs two basic numbers to come up with both the public and private keys. Sender encipher the message by receiver public key, then the message delivered to receiver. Hence fore he decrypts it using his personal private key [13, 14]. RSA has three steps; key generation, encoding and decoding. On the other hand, RSA has many faults, that is why it is not good for commerce. [11]. Figure 13 showcases the order of steps followed by RSA algorithm for the cryptography of multiple blocks.

a) Key Generation **Figure 12: THE RC6 ENCRYPTION ALGORITHM**

Choose two distinct large random prime numbers p and q such that $p \neq q$.

Compute $n = p \times q$.

Calculate: phi (n) = (p-1) (q-1).

Choose an integer e such that $1<e<\text{phi}(n)$

Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as private key exponent.

The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

b) Encryption

Plaintext: $P < n$

Cipher text: $C = Pe \bmod n$.

c) Decryption

Cipher text: C

Plaintext: $P = Cd \bmod n$.

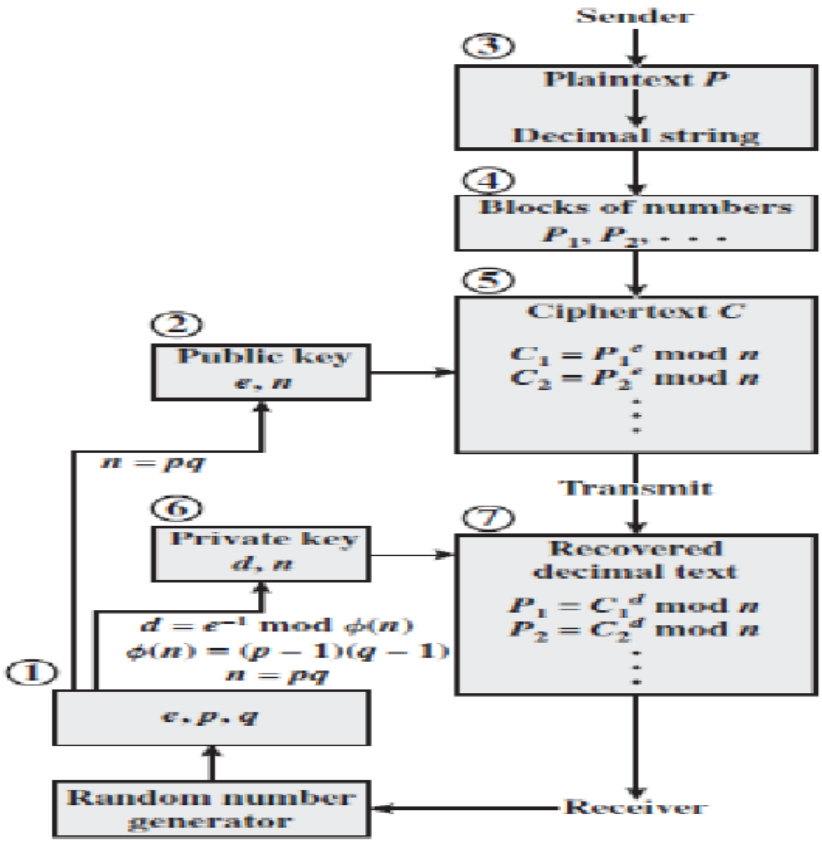


Figure 13: WORKFLOW OF RSA ALGORITHM [7]

11. ECC

Elliptic Curve Cryptography is an asymmetric algorithm that utilizes varied keys to encode and decode. It was invented by V. Miller (IBM) and N. Koblitz (University of Washington) in 1985. ECC was founded on algebraic structures of left-shaped carves in limited domains. It is effective enough to ensure security with a 164-bit key. That system demands a 1024 bit key to fulfil security. ECC affords the ultimate security with the same bit sizes. It is good for battery backup, too since it consumes less energy [5]. The main advantage of ECC is that its utilization of small key lengths which results in quick encoding and consuming minimal energy. On the contrary, of its disadvantages is inducing the size of the ciphered text and needs extremely sophisticated equations. Finally, the complexity of encoding algorithm rises.

12. ElGamal Encryption System

Elgamal Encryption System relies on the complexity of the unique algorithm problem, in which, it is easy increase numbers of grand powers. However, it is more difficult to do the opposite computation of the distinctive logarithm. ElGamal Encryption is

based on specific parameters that have the effect on the process, pace and safety of the algorithm. It is one of varied encoding plans that use Adhoc system in the encoding operation [5].

13. Diffie-Hellman

This algorithm was established by Diffie-Hellman in 1976. In this algorithm, every group comes up with a key pair and distributes the public key. The Diffie-Hellman algorithm offers two users to find a shared secret key and get in touch over an insecure communications channel. However, one of the main disadvantages of this algorithm is that the communication is performed through it which means that it can be violated in the middle of the attack [3].

14. DSA

A Digital Signature Algorithm (DSA) is a public key encoding algorithm established to secure the privacy of numeral text. The DSA was founded by NIST. A text is signed by a secret key to invent a signature and the signature is checked opposite to the text by a public key. Likewise, any group can check the authenticity signatures; however, only the party with the secret key could sign the texts. An available numeral signature offers a recipient a cause to think that the message was invented by a known sender who has the secret key, and that it was not modulated in transferring [4].

II. LITERATURE SURVEY

Several works in the past have attempted to discover which algorithm would work best for encryption and decryption. The work presented by Singh et al. [20] is a prime example of that as it compared between the different symmetric algorithms including the DES, 3DES, AES and the Blowfish algorithms. The work found that Blowfish was the best amongst the other methods despite their popularity in the field of encoding and decoding. Accordingly, it was found that the AES algorithm was not proficient enough in comparison to other algorithm, for it needs higher processing time.

Similarly, the work presented by Cornwell [21] found that the Blowfish algorithm had the ability to support security for a relatively long time without any suspicious violations of the code. According to the researcher, the Blowfish algorithm is superior in terms of security and efficiency. However, further research should be carried on in order to re-estimate the results discussed by the Cornwell research on Blowfish to provide more evidence on the results.

In other study that was presented by Tamimi [22], two modes of performance were employed, namely the ECB and CBC. Those modes are used to compare the time it takes for each of them to be run and processed. According to the work and in

what agrees with all of the previous studies aforementioned, Blowfish has proven to be the best out of the compared algorithms in the work due to the lack of efficiency in time when it comes to the AES and the need to processing more data.

Many authors and researchers have found in Blowfish an ideal method for encryption and decryption including Nadeem [23] that found the in the many advantages of Blowfish a mean to overcome the competition in other algorithms. Additionally, the work presented by Nadeem concluded that AES is far more developed than DES and 3DES. It was also found that DES is far better than 3DES where the latter requires thrice the time when it comes to processing information.

In another work offered by Dhawan [24], it was found that AES carried out other algorithms in number demanding operations a second in varied user load and in the reacting time with multiple user load circumstances.

Singh et al. [25] presented a work that ran a comparison between the most popular encoding algorithms. According to the work, the most popular algorithms were AES, DES, 3DES and Blowfish in the terms of security and energy consumption. The results of the comparison contrasted with the some of the previous studies and showed that AES is better than the basic form of the Blowfish algorithms. However, to make BA stronger against every type of attack, extra keys could be added to substitute the old XOR with a new operation.

In the work presented by Agrawal et al. [26] after long research about DES, 3DES, AES, and Blowfish, they confirmed the superiority of the Blowfish algorithms, in terms of key size and security. Blowfish algorithm F function enhances supreme stage of security to encode the 64-bit plaintext database. Besides, Blowfish algorithm works quicker than the rest common in identical key encoding algorithms.

Similarly, Seth et al. [27] compared three algorithms: DES, AES and RSA. They inferred that RSA requires the longest encoding time and higher memory than the other two algorithms; however, with minimal output byte in RSA algorithm. Meanwhile, they also found that DES utilizes minimum enciphering time while AES requires the smallest storage memory. Furthermore, encoding time in both AES algorithm and DES algorithm is almost the same.

Mandal et al. [28] Figured out that the AES is distinctive over the other 3DES and DES in throughput and decoding time in their work.

Apoorva et al. [29] concluded that blowfish in the best algorithm to be used in terms of security and time to process because it consumes little time in comparison to the rest.

In the work presented by Abdul et al. [30], numerous algorithms were studied including: AES, DES, 3DES, RC2, BLOWFISH and RC6. The conclusion of the comparison ran at the work was that no dramatic difference in hexadecimal base encryption or base 64 ciphering. Also, Blowfish has proven to perform better than the rest when transforming the pocket size. In

addition, the work showed that the performance of 3DES is mediocre when compared to DES algorithm. All in all, the big key size could provide considerable improvement in the battery and time passed.

Thakur et al. [31] ran a comparison between DES, AES and Blowfish moderately where the outcome proved that Blowfish is the best and ideal algorithm out of the three when it is in the terms of performance.

Marwah et al. [32] also compared three algorithms, namely: DES, 3DES and RSA. The result is that the privacy ensured by 3DES is better than that of DES and RSA. DES is economical in energy memory required as well as fast in encoding and decoding database time. DES is vulnerable though, in comparison to 3DES and RSA.

The work of Alam et al. [33] has proved that 3DES requires more energy and processes less input than those of DES, this is because of its triple time feature. However, RC2 proved to be quicker due to smaller sizes of the throughput if contrasted to Blowfish. Blowfish input value is bigger than 3DES, DES, CAST-128, IDEA and RC2. Blowfish consumes the least power. Eventually, it turns out that Blowfish is the best, in terms of time, throughput and power.

Saini [34] sums up that the superior algorithms are prominent for their popularity. An efficient cryptography achieves two parts of an equation, possibility and acceptability.

III. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

The table 1 gives the comparison between all algorithms previously discussed in this paper with respect to create by, year, key size, block size, round, structure, flexible, and features.

Table1 COMPARISON BETWEEN ALL CRYPTOGRAPHY ALGORITHMS PREVIOUSLY DISCUSSED

Algorithm	Created By	Year	Key Size	Block Size	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64bits	16	Festial	No	Not Strong Enough
DH	Whitfield Diffie and Martin Hellman	1976	Variable	-	-	Public key Algorithm	Yes	Good Security and Low Speed
E-DES	IBM	1977	1024 bits	128 bits	16	Festial	-	Good Security and fast Speed
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Low Speed
T-DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security and fast
ECC	Neal Koblitz and Victor Miller	1985	More than symmetric and variable	Variable	1	Public Key Algorithm	Yes	Excellent Security and fast Speed
EEE	Taher Elgamal	1985	1024 bits	-	-	Public Key Algorithm	Yes	Enough secured and fast Speed
RC4	Ron Rivest	1987	Variable	40-2048	256	Festiel Stream	Yes	fast Cipher
RC2	Ron Rivest	1987	8,128,64 by	64 bits	16	Festiel	-	Good and fast Security

			default					
BLOWFISH	Bruce Schneier	1993	32-448	64 bits	16	Festiel	Yes	Fast Cipher in SSL
SEAL	Phillip Rogaway and Don Coppersmith	1994	160 bits	32 bits	2	Public Key Algorithm	Yes	Not Strong and fast Speed
DSA	NIST	1997	variable	-	-	Public Key Algorithm	Yes	Good Security and fast Speed
RC6	Ron Rivest et.al	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	Good Security
AES	Joan Daeman & Incent Rijmen	1998	128,192,256 bits	128 bits	10,12, 14	Substitution Permutation	Yes	Security is excellent. It is best in security and Encryption performance

IV. Result and Discussion

From the above, the comparisons of the algorithms are based on creator year, key size, block size, round, structure, flexibility and features. The results showcase that the algorithms AES, Blowfish, RC4, E-DES and TDES are the fastest in encryption time, speed, flexibility. The results also prove that the AES algorithm is the best in security, flexibility and encryption performance strongest. It is most efficient when compared to others.

V. Conclusion

This paper presents a survey of the most important cryptography algorithms up to date. These cryptographic algorithms are studied and analyzed well in order to help in enhancing the performance of the current cryptographic methods.

The result shows the techniques that are useful for real-time encryption. All encryption methods have proven to have their advantages and setbacks and have proven to be appropriate for different applications. The comparison between Symmetric and Asymmetric algorithms shows that Symmetric algorithms are faster than their Asymmetric counterparts. Through the previous studies and the result of comparison, we find that the most reliable algorithm is AES in term of speed encryption, decoding, complexity, the length of the key, structure and flexibility.

Acknowledgment: This work has been language revised by Amr A. Abbas, eraconia@gmail.com.

References

1- RIMAN, C., and Abi-Char, P. E.: Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud, Vol.3, No.1, 1-7, (2015).

2- Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M.: Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security, Vol.8, No.12, 280-286, (2008).

3- Omar G. A., Elsadd, M. A., & Guirguis, S. K.: Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid. In Power Systems Conference (MEPCON), 2017 Nineteenth International Middle East, IEEE, 644-649, (December 2017).

4- Sridevi, C.: A Survey on Network Security. Global Journal of Computer Science and Technology (2018).

5- Singh, G.: A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications, Vol. 67, No. 19, (2013).

6- Singh, M. G., Singla, M. A., & Sandha, M. K.: Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System. International Journal of Multidisciplinary Research, Vol. 1, No. 4, 143-151, (2011).

7- William, S.: Cryptography and Network Security: principles and practices. Pearson Education India (2006).

8- Chowdhury, Z. J., Pishva, D., & Nishantha, G. G. D.: AES and Confidentiality from the Inside Out. In Advanced Communication Technology (ICACT), 2010 The 12th International Conference on IEEE, Vol. 2, 1587-1591, (February 2010).

9- Mandal, A. K., Parakash, C., & Tiwari, A.: Performance Evaluation of Cryptographic Algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, 1-5, (March 2012).

10- Adhie, R. P., Hutama, Y., Ahmar, A. S., & Setiawan, M. I.: Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). In Journal of Physics: Conference Series, Vol. 954, No. 1, (January 2018).

11- Koko, S. O. A. F. M., & Babiker, A.: Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication. IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, No. 1, 62-69, (2015).

12- Kumar, A., Jakhar, D. S., & Makkar, M. S.: Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 7, 386-391, (2012).

13- Zhou, X., & Tang, X.: Research and Implementation of RSA Algorithm for Encryption and Decryption. In Strategic Technology (IFOST), 2011 6th International Forum on IEEE, Vol. 2, 1118-1121, (August 2011).

14- Somani, U., Lakhani, K., & Mundra, M.: Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing. In Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on IEEE, 211-216, (October 2010).

15- Manku, S., & Vasanth, K.: Blowfish Encryption Algorithm for Information Security. ARPN Journal of Engineering and Applied Sciences, Vol.10, No.10, 4717-4719, (2015).

16- Handschuh, H., & Gilbert, H.: χ 2 Cryptanalysis of the SEAL Encryption Algorithm. In International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, 1-12, (January 1997).

17- Schneier, B.: Applied Cryptography Second Edition: Protocols, Algorithms, and Source. Beijing: China MachinePress, 239-252, (2000).

18- Rogaway, P., & Coppersmith, D. A.: Software-Optimized Encryption Algorithm. Journal of Cryptology, Vol. 11, No. 4, 273-287, (1998).

19- Charbathia, S., & Sharma, S.: A Comparative Study of Rivest Cipher Algorithms. International Journal of Information & Computation Technology. ISSN 0974-2239 Vol. 4, 1831-1838, (2014).

20- Singh, G., Kumar, A., & Sandha, K. S.: A Study of New Trends in Blowfish Algorithm. International Journal of Engineering Research and Application, (2011).

21- Cornwell, J. W., & Columbus, G. A.: Blowfish Survey. Department of Computer Science. Columbus: GA Columbus State University, 1-6, (2012).

22- Abdel-Karim, A.: Performance Analysis of Data Encryption Algorithms, (2006).

23- Nadeem, A., & Javed, M. Y.: A Performance Comparison of Data Encryption Algorithms. In Information and communication technologies, 2005. ICICT 2005. First international conference on IEEE, 84-89, (August 2005).

24- Dhawan, P.: Performance Comparison: Security Design Choices. Microsoft Developer Network, Tech. Rep. (2002).

25- Singh, S. P., & Maini, R.: Comparison of Data Encryption Algorithms. International Journal of Computer Science and Communication, Vol. 2, No. 1, 125-127, (2011).

26- Verma, O. P., Agarwal, R., Dafouti, D., & Tyagi, S.: Notice of Violation of IEEE Publication Principles Peformance Analysis of Data Encryption Algorithms. In Electronics Computer Technology (ICECT), 2011 3rd International Conference on IEEE, Vol. 5, 399-403, (April 2011).

27- Seth, S. M., & Mishra, R.: Comparative Analysis of Encryption Algorithms for Data Communication 1. (2011).

28- Mandal, P. C.: Superiority of Blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 9, 196-201, (2012).

29- Apoorva, Y. K.: Comparative Study of Different Symmetric Key Cryptography Algorithms. International Journal of Application or Innovation in Engineering and Management, Vol. 2, No. 7, 204-6, (2013).

30- Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M.: Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No. 12, 280-286. (2008).

31- Thakur, J., & Kumar, N.: DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation-Based Performance Analysis. International journal of emerging technology and advanced engineering, Vol. 1, No. 2, 6-12, (2011).

32- Hercigonja, Z.: Comparative Analysis of Cryptographic Algorithms. International Journal of Digital Technology & Economy, Vol. 1, No. 2, 127-134, (2016).

33- Alam, M. I., & Khan, M. R.: Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 10, (2013).

34- Saini, B.: Survey on Performance Analysis of Various Cryptographic Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 4, 1-4, (2014).