A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security

Article *in* International Journal of Scientific and Research Publications (IJSRP) · March 2019

DOI: 10.29322/IJSRP.9.03.2019.p8779

1 author:

Mohammed Abdulhameed Al-Shabi
Taibah University
27 PUBLICATIONS **151** CITATIONS

SEE PROFILE

A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security

M. A. Al-Shabi*

***Department of Management Information System, College of Business Administration,**
Taibah University, Saudi Arabia, mshaby@taibahu.edu.sa
DOI: 10.29322/IJSRP.X.X.2018.pXXXX
http://dx.doi.org/10.29322/IJSRP.X.X.2018.pXXXX

Abstract- This paper discusses 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 speed (implementation) and security (special keys) determine whether an encryption algorithm is good. What is more, computational resources, such memory (RAM) size, are an integral consideration since they affect algorithm efficiency, hence the need to ensure optimal resource allocation, etc. Particularly, encryption is the process of transforming plain text into ciphered-text, which cannot be understood or altered easily by undesirable people.
This encrypted result is encoded and has immunity against attacks and unauthorized access and manipulation. Encryption algorithms often use private keys that are used to revert the encrypted data to its original meaningful format. Such an algorithm, such as Blowfish, RC5, or RC4, is basically a set of mathematical procedures that make it hard for malicious attackers to understand or use the original data. In symmetric key algorithms, a single key is used to encrypt and decrypt text. On the contrary, the asymmetric key algorithm uses two discrete keys, where both the sender and receiver have access to one of them. These security measures and systems eliminate possible internal and external threats to ensure integrity, correctness, confidentiality, and safety of data and infrastructures are controlled.

Index Terms- Encryption, Cryptography Concept, Information Security, Symmetric Key Algorithms, Asymmetric Key Algorithms

I. INTRODUCTION

The last researchers finding, and investigation have been written previously, the purpose of symmetric and asymmetric encryption algorithms is to safeguard information. They achieve this objective by transforming data into new formats that can hardly be broken or decrypted by unauthorized entities [1], [2], [3], [4] and [5]. Symmetric encryptions, such as DES, RC2, RC4, Blowfish, RC5, RC6, or AES, are the and oldest and easiest forms of encryption where only one unique secret key is used to cipher and decipher information. The sender and receiver share the key, which is a major drawback since an attacker can eavesdrop the key exchange channel and use it to decrypt the data. A safe channel is needed between the sender and the receiver to commute the secret key. In [6], [7] conversely, asymmetric encryption, such as DSA, RSA, and ECC, uses two keys –public and private– to cipher pain text. Any entity with the public key can use it to send a message but the private key is kept secret and is used to decrypt the message, an approach that enhances security. Altogether, they all involve manipulation of plain text to generate ciphertext and vice versa. The following diagram outlines the various algorithms in cryptography.

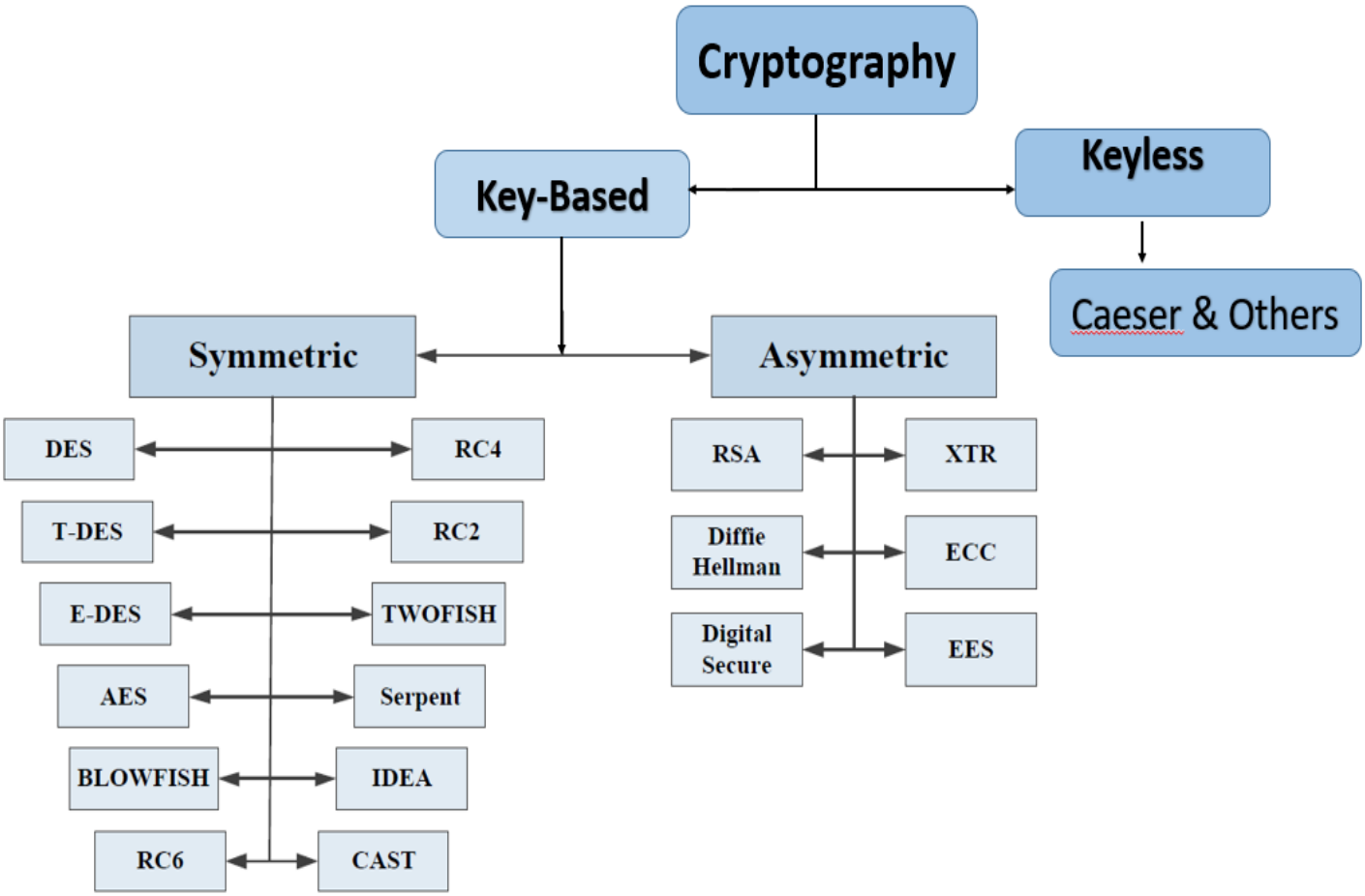


Figure 1. Classification of Cryptography

II. LITERATURE SURVEY

A. Encryption and Decryption

The many concepts of cryptography revolve around computer security and OSI security architecture. Computer security incorporates the CIA model, that is, Confidentiality (authorized access), Integrity (data correctness and accuracy), and Availability (ready access for authorized entities) [5]. The OSI security architecture focuses on services and security attacks, mechanisms used to predict and prevent an attack, and the preparations to recover in case of disasters. In this light, Encryption is altering the database into plain text (useful readable information) to ciphertext (unusable information) and allowing an authorized party to use computational algorithm(s) (key) to revert it into the original form (decryption) [8], [6]. In other words, the ordinary information is hidden to avert passive (collecting victim information for malicious purposes) and active (alteration or manipulation of victim information) attacks.

B. Cryptography Goals

Generally, the main goal that cryptography intends to achieve is to secure information and ensure efficient usage and manipulation. This aim can be broken down into issues relating to confidentiality, authentication, data integrity, non- repudiation, access control, and availability. The following table details the descriptions of each one of them;

TABLE I: Cryptography Goals

Goal	Description
Authentication	The verification of an entity's identification to can prove their identity to another who does not have personal knowledge of their identity
Confidentiality	Ensuring the meaning of a message is encoded for security and that sensitive information can only be available to authorized users [9].
Data Integrity	Ensure that the exact information received is the same as the information sent. It is basically an assurance of data accuracy, consistency, and correctness.
Access Controls	Special permissions granted to different users in order to access different features [10].
Non- Repudiation	Assurance that a person or entity cannot refuse or fail to be accountable for their actions.
Availability	The ease of accessing data, information, or resources.

A. *Data Encryption Standard (DES)*

DES is the earliest 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) [11]. DES is a symmetric cryptography method that uses one key in both ciphering and deciphering. Initially, it was based on an earlier design of Hoirst Feistel called LUCIFER [12]. Currently, the algorithm uses the Feistel block cipher that requires one to specify the round function, key schedule, and any other needed processing, as shown in the figure below. Practically, the plain text (structured into 64-bit blocks) and the secret key (56-bit) are the two inputs taken for encryption. The output –64-bit cipher-text– include a number of substitutions and permutations that increases the difficulty of deciphering. As a result, it is widely adopted. Amidst its strengths, DES is limited by several shortcomings. One advantage is the use of 56-bit keys that makes it difficult to use brute force to decrypt the data. Another advantage is the nature of the algorithm; cryptanalyst can perform cryptanalysis by exploiting characteristics of the algorithm with no major weakness. However, various experts have found some weaknesses in the cipher. For instance, the same output can be generated by inputting two chosen inputs to an S box. Further, it has an unclear and confusing initial and final permutation. Still, it remains the preferred option for many.

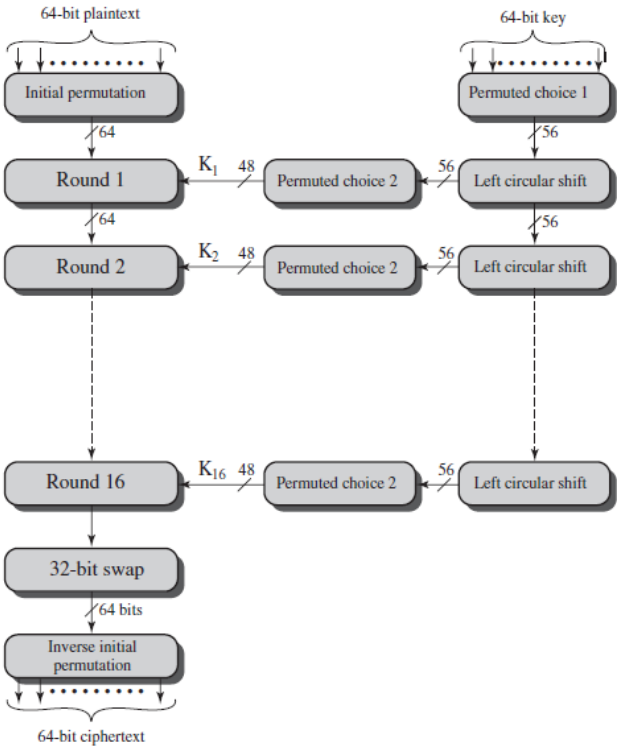


Figure 2. DES Encryption Algorithm

B. Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) referred as Triple Data Encryption Algorithm (TDEA) that was firstly proposed by IBM in 1998 and standardized in ANSI X9.17 and ISO 8732 [11]. This encryption algorithm is meant to address the errors encountered with its predecessor –the DES– without necessarily having to recreate a new algorithm. It is in two variations, the 3-key triple DES (K1, K2 and K3) and the 2- key triple DES (K1 and K3); they all use the 56-bit keys [13]. Practically, it is a symmetrical block cipher that imposes DES cipher algorithm thrice on each block of data, as shown in the figure below. However, it is reportedly slower when compared with other cipher methods [14] . This aspect together with its smaller key size are the major disadvantages.

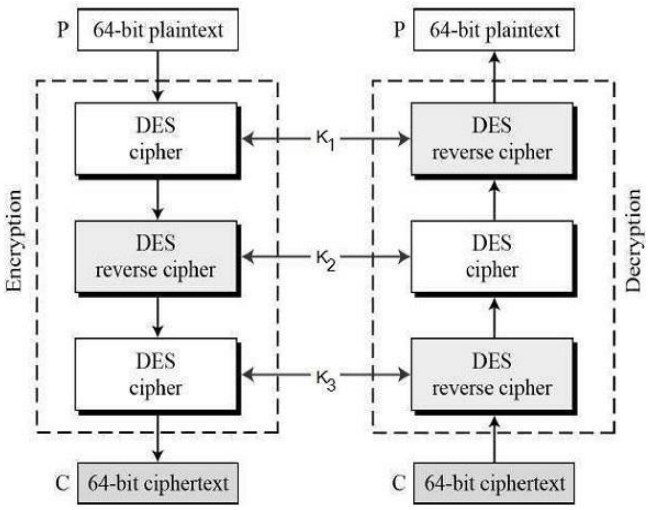
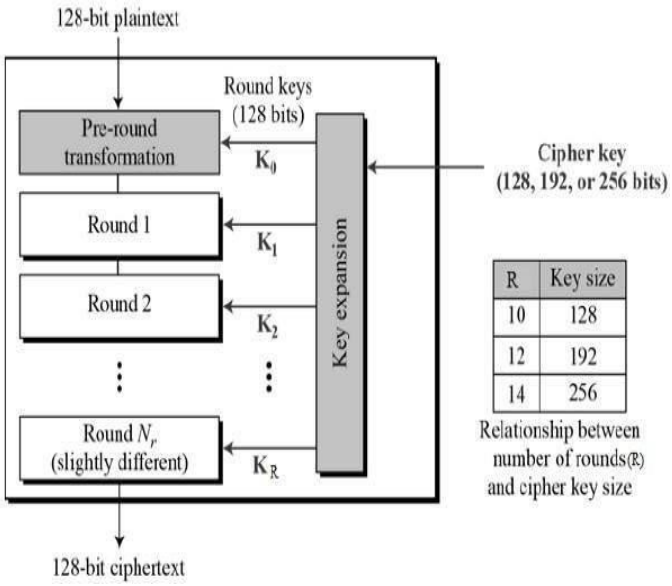


Figure 3. 3DES Encryption Algorithm

C. Advanced Encryption Standard (AES)

The NIST announced a call for the candidates of a cipher to implement a new encryption standard in 1997 because of the need for high security and efficiency, it's time to replace the existing DES and 3DES encryption algorithm with new AES [11]. Owing to a higher encryption speed and enhanced security, AES is a popular choice for many. In fact, its length-variated keys replace the small-sized 3DES keys. Additionally, it is many times faster. Depending on the key length, AES can be classified as AES-1 (128-bits key-length), AES-192 (192-bits key-length), or AES-256 (256-bits key-length). For 128bit keys, the AES system goes for ten rounds, for 192-bit keys it goes 12 rounds, and for 256-bit keys it goes for 14 rounds, as shown below. Plain text is transformed severally: substitute byte transformation, shift rows transformations, mix columns transformations, and add round key transformations. Its flexibility in key length is an advantage during software implementation in C programming and Java language, and in both hardware and software [15]. However, it consumes more resources, and it requires more processing power because of the bigger block size, this together with the simple mathematical structure are its main disadvantages.



R	Key size
10	128
12	192
14	256

Figure 4. AES Encryption Algorithm

D. Blowfish

Blowfish is a symmetric cipher with a variable key length. The key length for Blowfish varies from 32 bits to 448 bits and is faster than DES. In operation, it splits messages into 64-bit blocks and individually encrypts them. These blocks are further divided into data and key expansion [16], [17]. These and other factors make it one of the fastest algorithms currently in use. Additionally, despite the many cryptanalyses, blowfish is yet to be broken. Its advantages include independent S boxes, complex key schedule, as well as high speed and efficiency. It has a disadvantage when it comes to time consumption. Further, the key must be transferred (sometimes insecurely) to different users and as they increase, key management is likely to be a problem [18] . Still, it stands out from other symmetric ciphers.

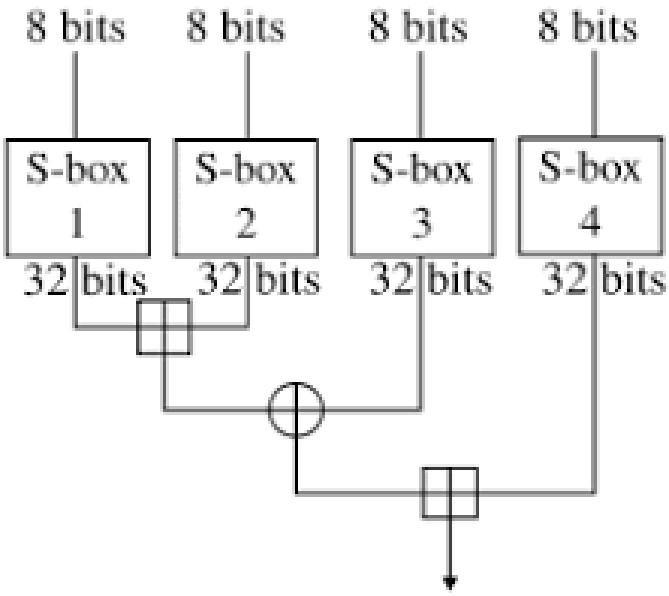


Figure 5. Blowfish Encryption Algorithm

E. Hybrid Cubes Encryption Algorithm (HiSea)

is the symmetric non-binary block cipher because the encryption and decryption key, plaintext, ciphertext and internal operation in the encryption or decryption process that is based on the integer numbers. HiSea encryption algorithm is developed by Sapiee Jamel in 2011 [11], [19]. These algorithms are created by the combination and permutation of integers. The advantages of public key are combined with an element of symmetric algorithm to create an enhanced cipher method [3]. However, one disadvantage of hybrid encryption algorithm is the problem of securely transporting keys, hence the need to exchange them through people, which is still a challenge. Still, this algorithm is advantageous since it has proved to be resistant to attacks and does not make the ciphertext longer as compared to the others. In this regard, it is a secure option as long as both the public and private keys are kept secure.

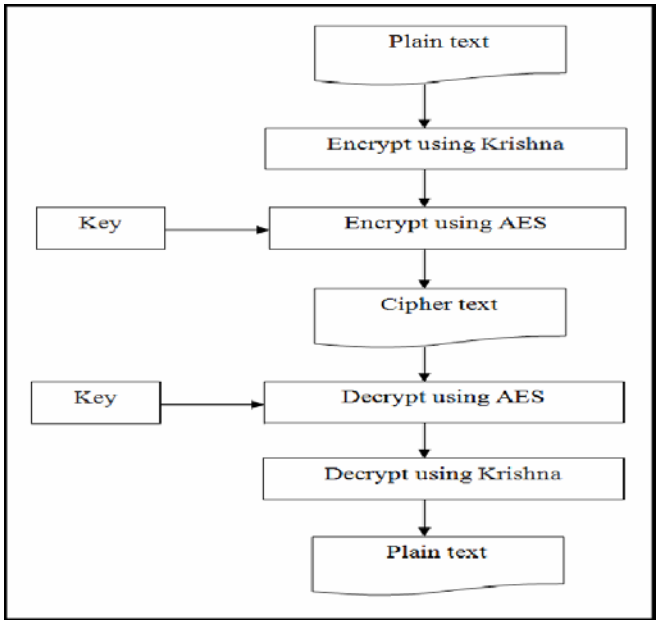


Figure 6. (HiSea) Encryption Algorithm

F. Rivest Cipher 4 (RC4)

is a symmetric key and a stream cipher. It utilizes WPA and WEP to enable wireless communication. It is preferred because of ease of implementation and its fast speed. It uses key streams that are combined with plain text in order to output ciphertext during the process of encryption. In terms of memory requirements, it uses byte manipulation and hence only needs 256 bytes of memory for the array. Generally, it consumes less memory space, which improves its efficiency. It was largely secure until a cryptanalysis attack exposed its vulnerabilities [20]. As a result, improvements were made other variations such as RC4A, VMPC, and RC4+ were introduced. An algorithm key can only be used once. However, cryptanalysis has shown that one in every 256 keys is likely to be weak. Amidst the drawbacks, it is considered a good cryptography algorithm.

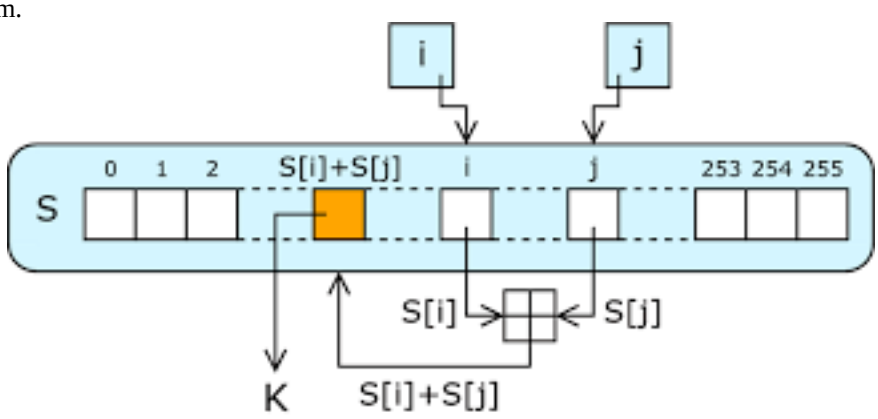


Figure 7. Encryption in (RC4)

G. Tiny Encryption Algorithm *(TEA)*

Tiny Encryption Algorithm (TEA has fewer lines of code making it very easy to design and implement. The system uses two 32-bit unsigned integer/code blocks can be generated from a 64-bit block and 128-bit-length keys (k [0] - k [3]) to generate results in form of w [0] and w [1]. Sets of magic numbers/constants are used to avert attacks that are based on the regularity of rounds [21]. A notable weakness is the fact that it has the problem of equivalent keys (at least three), hence making it a weak cryptographic hash function in certain situations.

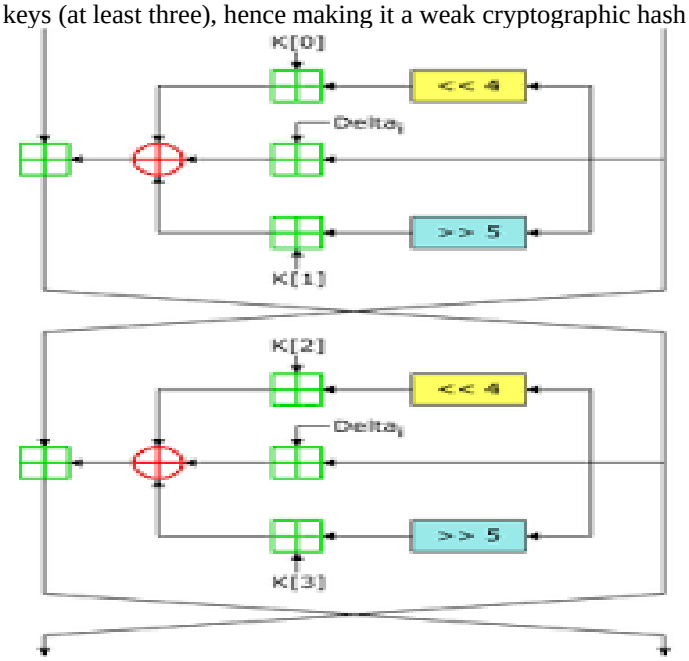


Figure 8. TEA Block Cipher

H. CAST

As the name suggests, CAST was developed using the CAST design method. Further, it shares features with other cipher methods that are based on Feistel structure. This algorithm has been helpful in removing repetition and it boasts of having strong keys. However, it is not very secure and is prone to attacks such as timing attack. Additionally, it is considered to be fast enough when compared with others in the same class [12]. Nonetheless, it is suitable in other areas where its vulnerabilities do not limit its effectiveness.

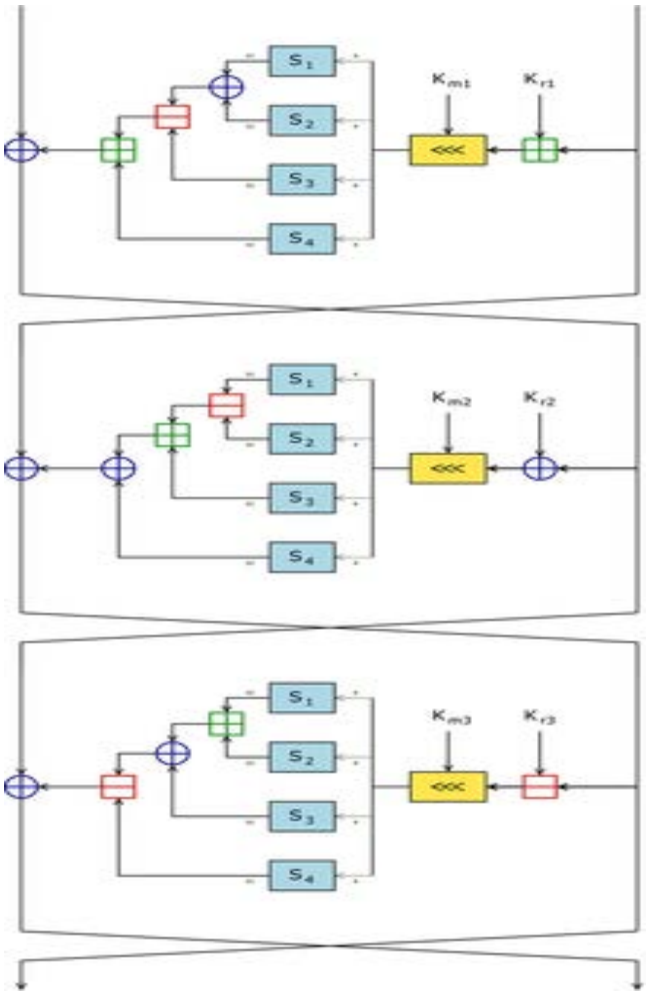


Figure 9. CAST Block Cipher

I. Twofish

Twofish algorithm was designed to replace the DES Encryption algorithm. This move can be explained by its main advantages where it is considered highly flexible in its ability to tradeoff the key setup and encryption speed [22] . In fact, it accepts any key length of up to 256 bits and performs differently depending on the key schedules. Further, it does not contain any factor that can make it inefficient on a 16-bits microprocessor or on the proposed 64-bits microprocessor [23]. However, when compared to the AES algorithm, it is slower. Nonetheless, it is a safe method that can withstand brute force.

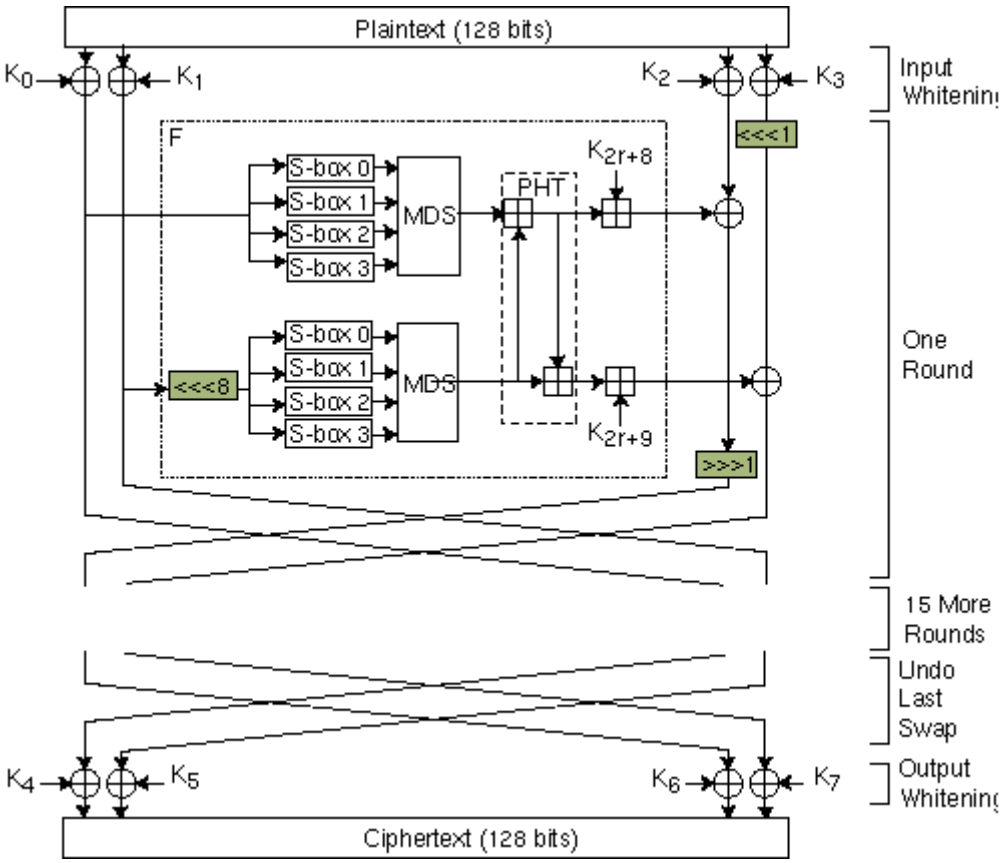


Figure 10. Twofish Block Cipher

J. Serpent

The serpent cipher method is a key block algorithm that uses 128-bits and 256-bits key block sizes. Practically, it is a 32- round system that operates on four 32-bit words, hence the 128-bits block size. The merit of this algorithm arises from the fact that it is easy to implement, it is fast and more secure than 3DES. Despite the few weak points, the algorithm has been useful in hardware encryption [23].

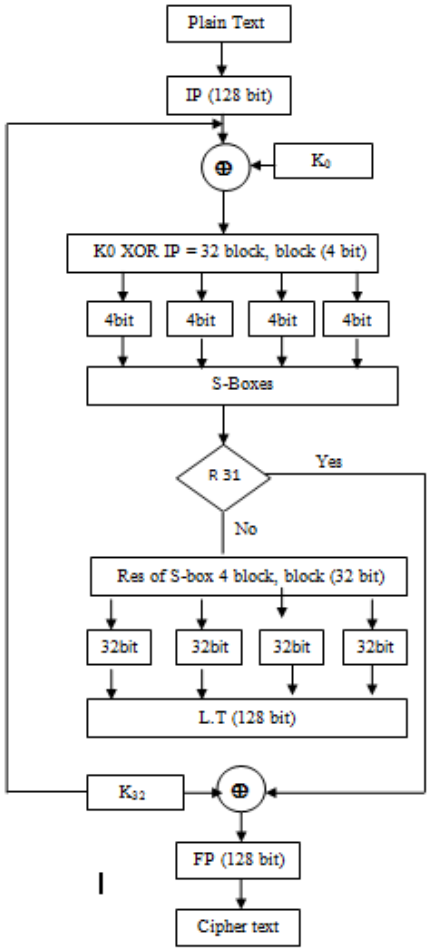


Figure 11. Serpent Block Cipher

K. RC2

RC2 is a block encoding algorithm that was introduced all the way back in the year 1987. RC2 is also known as ARC2. The acronym RC is understood as Rivest Cipher or Ron's Code. It is meant to replace the DES. RC2 he key provided by the user may be of size from one byte up to 128 bytes. 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 [24].

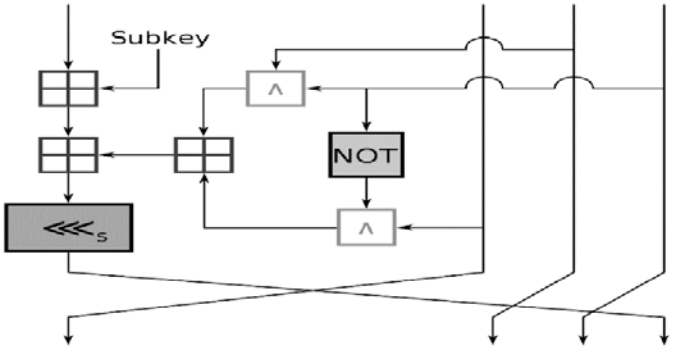


Figure 12. RC2 Block Cipher

III. ASYMMETRIC KEY CRYPTOGRAPHY

A. Rivest-Shamir and Adleman (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 [24]. operate by using a variable key and encryption block. It uses block size data where plain text and cipher text are integrated between 0 and 1. The main advantage of RSA is that it has enhanced security as compared to other algorithms. In fact, it is among the safest algorithm [25], [26]. However, it is limited by low encryption speed, complexity in keys creation, and susceptibility to attacks due to the low speed [27]. Three steps are involved: generation of public/private key pair, encrypting the plain text (data) into ciphertext (data), and decrypting the data to generate the original text. The following diagram explains the steps followed;

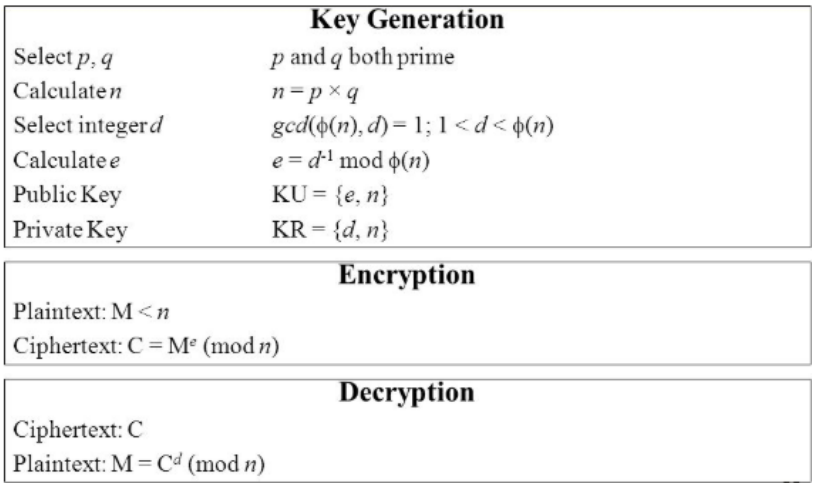


Figure 13. RSA Encryption Algorithm

B.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 [24]. This algorithm is used to create a shared secret between two parties through a secured physical channel. Each of the parties comes up with a secret key that is only known to them. The arrangement enables a secure exchange [28]. Among the advantages is the fact that it is secure, the algorithm used is complex enough, and the secret key is never transmitted over a channel. However, on the downside, the algorithm is prone to attacks, it is expensive, and is not suitable in most encryption situations since it lacks authentication.

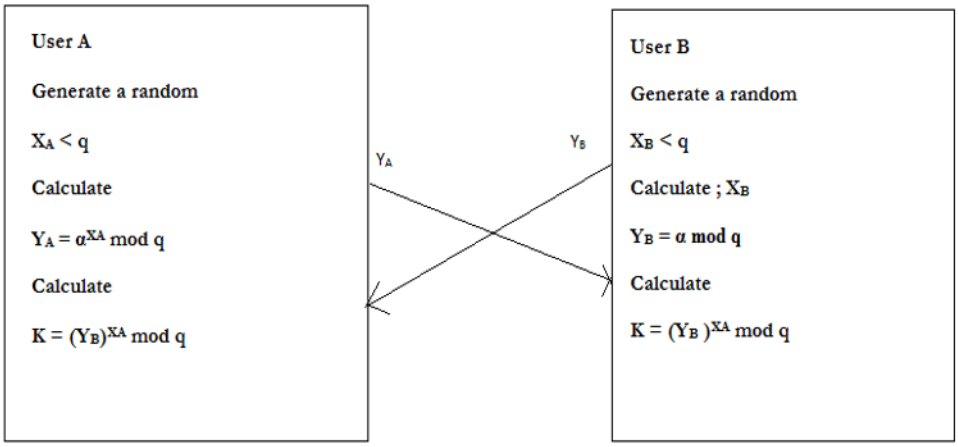


Figure 14. Diffie-Hellman Encryption Algorithm

C. Elliptic Curve Cryptography (ECC)

ECC 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 based on the algebraic structure of elliptic curves over finite in limited domains. It is effective enough to ensure security with a 164-bit key [24]. 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 [29]. 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.

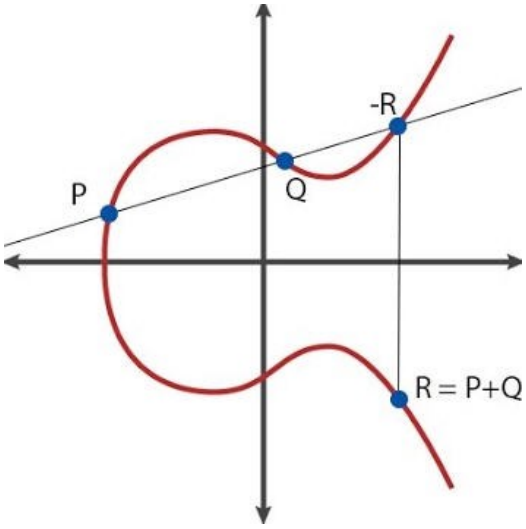


Figure 15. Basic Elliptic Curve Cryptography

IV. FESTIAL STRUCTURE AND BILATERAL PERMUTATION

A. Substitution-Permutation (SPN))

This is a connection of linked logical operators used in block cipher algorithms. It performs encryption and decryption with the aid of S boxes and P boxes. Ciphers of substitution replace plaintext with the ciphertext. The input keys are divided into multiple small boxes which are applied in an S-box that substitutes and the P-box. The key positions are mixed. The data is broken into small bits which are bilateral. The result is the ability to build strong block ciphers.

B. Feistel Structure (FN)

This is a structure from which other block ciphers are derived. During encryption, many processing rounds are performed on plain text, with each round involving substitution steps followed by permutation steps. In the Feistel structure, the plain text is sub-divided into two equal halves (left and right). The DES algorithm is an ideal example. Notably, the data is not broken into any state hence it is unchangeable.

V. RESULT AND COMPARATIVE ANALYSIS

A comparative analysis on various metrics shows the weaknesses and strengths of both symmetric and asymmetric algorithms. In the following figure, a performance evaluation considers factors such as battery consumption, time consumption, block size, round, structure, types of attack, and hardware/software implementation. Depending on the intended use, one is able to identify the algorithm that is suitable on certain implementation environments.

TABLE II: Comparative Analysis

Symmetric Cryptography								
Algorithm	**Published &Developed by**	**Battery Consumption**	**Time Consumption**	**Block Size**	**Round**	**Structure**	**Attack**	**HW & SW**
DES	1977 by IBM	Medium	Slow	64 bits	16	Festial	Brute force	both
3DES	1998 by IBM	High	Very Slow	64 bits	48	Festial	Brute force, known or Plaintext	both
AES	2001 by Vincent	High	Fast	128,192,	10-	Substitution	Side channel	both

	Rijman, Joan Daeman			or 256 bits	128,12-192,or 14-256			
Blowfish	1993 by Bruce Schneier	Lowest	Very fast	64 bits	60	Festial	Dictionary	Hardware
HiSea	2011 by Sapiee Jamel	Low	Medium	128 bits	85	Lai-Massey scheme	Narrow Bichques	Software
RC4	1987 by Ron Rivest	High	Fast	2064 bits	256	Festial		Both
RC6	1998 by Ron Rivest et.al	Medium	Fast	128 bits	20	Festial	Brute force	Hardware
RC2	1987 by Ron Rivest	High	Fast	64 bits	16	Festial	Brute force	Software
TEA	1994 by Roger and David	Low	Fast	64 bits	64	Festial	Related Key	Software
CAST	1996 by Carlisle Adams and Stafford Tavares	High	Fast	64 bits	12 0r 16	Festial	Chosen plain text, Timing	both
Twofish	1998 by Bruce Schneier	Low	Slow	128 bits	16	Feistel	Side channel	Hardware
Serpent	1998 by Ross Anderson, et.al	Medium	Fast	128 bits	32	Substitution	XSL attack	Both
Symmetric Cryptography								
Algorithm	Published &Developed by	Battery Consumption	Time Consumption	Block Size	Round	Structure	Attack	HW & SW
RSA	1977 by Ron Rivest et.al	Low	Slowest	Variable	1	Public Key Algorithm	Cycle attack	both
Diffie-Hellman	2002 by Hellman	High	Medium	Variable	1	Festial & Substition	Man in the middle	both
ECC	1985 by Neal Koblitz and Victor Miller	Medium	Fast	Variable	1	Public Key Algorithm	Side channel	both

From the above performance evaluation shows the similarities and differences of various symmetric and asymmetric encryption algorithms. Evidently, in the symmetric category, AES performs much better when compared to RC2, DES, and 3DES, especially on time consumption. On this metric, 3DES is a low performer, mainly because of its triple phase encryption approach. Further, discussions on this category show that the key size influences both battery and time consumption. On the asymmetric category, the Diffie-Hellman algorithm is superior to RSA in terms of encryption speed and susceptibility to attacks. Altogether, the choice of a cipher method should be determined by the specific needs rather than the general perception since vulnerabilities of an algorithm are not weaknesses in all implementation scenarios.

VI. CONCLUSION

To conclude, this paper presents a survey of the most important cryptography algorithms appearing until now. These cryptographic algorithms are studied and analyzed by the researcher to help in enhancing the performance of the current cryptographic methods. The result shows the techniques that are useful for real-time encryption. 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, the length of the key, structure and usability.

REFERENCES

[1] *A. Gupta and N. Walia, "Cryptography algorithms: A review," International Journal of Engineering Development and Research, vol. 2, no. 2, pp. 1667-1672, 2014.*

[2] *S. Kumari, "A research paper on cryptography encryption and compression," International Journal of Engineering and Computer Science, vol. 6, no. 4, pp. 20915-20919 , 2015.*

[3] *J. T. a. N. Kumar, "DES, AES, and Blowfish: Symmetric key cryptography," International Journal of Emerging Technology and Advanced Engineering, vol. 1, no. 2, pp. 6-12, 2011.*

[4] *S. C. a. S. Sharma, "A comparative study of Rivest Cipher Algorithms," International Journal of Information Computation Technology, vol. 4, no. 17, pp. 1831-1838, 2014.*

[5] *V. M. a. A. Sharma, "A survey on various cryptography techniques," International Journal of Emerging Trends Technology in Computer Science (IJETTCS), vol. 3, no. 6, pp. 307-312 , 2014.*

[6] *A. S. a. A. R. A. Devi, "Performance analysis of Symmetric Key Algorithms: DES, AES"," International Journal of Engineering and Computer Science, vol. 4, no. 6, pp. 12646-12651, 2015.*

[7] *K. S. a. F. S. M. Kaur, "Survey of various encryption techniques for audio data," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 5, pp. 1314-1317, 2014.*

[8] *F. D. a. E. R. F. Idrizi, "Analyzing the speed of combined cryptographic algorithms with secret and public key," International Journal of Engineering Research and Development, vol. 8, no. 3, pp. 45- 51, 2013.*

[9] *W. Stallings, Cryptography and network Security principles and practices, New Jersey: Prentice-Hall, 2005.*

[10] *R. Davis, "The Data Encryption Standard in perspective," in Proceedings of the Conference on Computer Security and the Data Encryption Standard, Gaithersburg, Maryland, 1977.*

[11] *S. J. A. D. Z. P. N. S. a. M. D. M. F. Mushtaq, "A Survey on the Cryptographic Encryption Algorithms," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, p. 7978, 2017..*

[12] *M. M. a. A. Kumar, "Comparison between DES, 3DES, RC2, RC6, Blowfish and AES," in Proceedings of National Conference on New Horizons in IT, NCNHIT, 2013.*

[13] *G. R. a. R. Umarani, "UR5: A novel symmetrical encryption algorithm with fast flexible and high security based on key updating," International Journal of Advanced Research in Computer Science and Software Engineering, pp. 16-22, 2012.*

[14] *,. &. A. B. S. O. A. F. M. Koko, "Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 17, no. 1, pp. 62-69, 2015.*

[15] *G. G. a. R. Chawla, "Review on encryption ciphers of cryptography in network," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 211-213 , 2012.*

[16] *T. N. a. T. Zhang, "A study of DES and Blowfish encryption algorithm," in Tencon 2009-2009 IEEE Region 10 Conference, 2009.*

[17] *J. W. C. &. G. A. Columbus, Blowfish Survey, Department of Computer Science. Columbus: GA Columbus State University, (2012.*

[18] *Y. N. P. G. S. T. S. a. Y. M. M, "Superior security data encryption algorithm (NTRU)," An International Journal of Engineering Sciences, vol. 6, no. 1, pp. 171-180, 2012.*

[19] *M. M. D. I. T. R. Y. a. T. H. S. Jamel, "The hybrid cubes encryption algorithm (HiSea)," Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, vol. 154, p. 191–200, 2011.*

[20] *J. a. P. X. X, "An improved RC4 stream cipher," in International Conference on Computer Application and System Modeling (ICCASM 2010), 2010.*

[21] *S. Shepherd, "The Tiny Encryption Algorithm," Cryptologia, vol. 31, no. 3, pp. 233-245, 2007.*

[22] *S. M. J. B. Robshaw, Key-Dependent S-Boxes and Differential Cryptanalysis, Netherlands: Kluwer Academic Publishers, 2002.*

[23] *F. A. H. N. B. Z. A. Anas Mohd Nazlee, " Serpent encryption algorithm implementation on Compute Unified Device Architecture (CUDA)," in Research and Development (SCOReD), Serding, Malaysia, 2009.*

[24] *S. G. O. G. Abood, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, vol. 8, no. 7, 2018.*

[25] *X. Z. &. X. Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption In Strategic Technology (IFOST)," in 6th International Forum on IEEE, 2011.*

[26] *K. L. &. M. M. U. Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," in In Parallel Distributed and Grid Computing (PDGC), st International Conference on IEEE, 211, 2010.*

[27] *A. N. a. V. R. B. Kumar, "Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images," in International Conference on Communication and Signal Processing (ICCSP), 2017..*

[28] *N. L, "Research on Diffie-Hellman key exchange protocol," in International Conference on Computer Engineering and Technology, 2010.*

[29] *G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications, vol. 67, no. 19, (2013.*