MINAR International Journal of Applied Sciences and Technology

Article type : **Research Article**

Date Received : **15/09/2020**
Date Accepted : **13/10/2020**
Date published : **01/12/2020**
: **www.minarjournal.com**
http://dx.doi.org/10.47832/2717-8234.4-2.1

SURVEY: EFFICIENT HYBRID ALGOR ITHMS OF CRYPTOGRAPHY

Mays M. HOOBI[1]

Abstract

Day after day, the digital data sizes undergo rapid increases over Internet, it is significant; the data shouldn't be accessed by the unauthorized users. The attackers attempt at accessing those sensitive part of the data. There is a necessity for the prevention of the unauthorized access of the data and guarantee the secure data exchange. A variety of the cryptographic approaches have been used for the conversion of the secret data of the users into secure ciphertext formats. The cryptographic methods have been based on, private and public keys. The researchers have worked on the efficient and secure transmission of data and presented a variety of the cryptographic approaches. For the efficient and secure transmission of the data over networks, there is a necessity of using hybrid approaches of encryption. In this article, various encryption methods are reviewed such as Rijndael, Number Theory Research Unit, Data Encryption Standard, 3 Data Encryption Standard, Elliptic Curve Cryptography, Rivest–Shamir–Adleman, Optimal Asymmetric Encryption Padding, Diffie-Hellman, HiSea, Improved Caesar, Digital Signature, and Advance Encryption Standard.

Keywords: Brute Force Attack, Cryptography, Digital Data, Hybrid Encryption, Search Space.

[1] Baghdad University, Iraq, mays.m@sc.uobaghdad.edu.iq, https://orcid.org/ 0000-0001-6100-6383

1. Introduction

Information technology infiltrated more aspects of the society throughout the past decades. The increase in the numbers of the interactions amongst the end users, organizations like the banks, and governments are conducted in an electronic way [1]. The cryptographic approaches are utilized for securing the digital data. There are two cryptography types: private key cryptography- which utilizes only one key, which is referred to as the symmetric key, and the public key cryptography, which utilizes 2 key crypto systems every one of the parties has one secret key and one public key. The aims of using cryptography methods are confidentially, authentication, integrity, and non-repudiation. Encryption can be defined as the procedure of the conversion of the plaintext to a cryptic text, for the purpose of securing it against data theft [2]. This article tries to show the most popular and utilized hybrid algorithms in the field of data encryption.

2.Cryptographic Methods

This section explains several based encryption methods are used in number of important researches; these methods are listed as below: -

2.1- Rijndael Algorithm

The Rijndael is one of the iterated block ciphers with a variable length of the blocks and a variable key length. The lengths of the key and the block may be independently set as 128, 192 or 256 bits. The intermediate result of the cipher has been referred to as the “State”,it is a rectangular array that has 4 rows and several columns which are equal to the length of the block, divided by 32. The ciphering key is similarly a rectangular array that has 4 rows as well as several columns that are equal to the length of the key, divided by 32 as is illustrated in Table1 [3].

Table-1: AES Rounds with Key Length

Version of the AES	Key Lengths (Nk words)	Block Sizes (Nb words)	Numbers of Rounds Nr
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

There are 4 main functions that are performed in every one of the AES rounds, which are :

a) SubByte.
b) ShiftRow.
c) MixedColumn.
d) Add Round Key.

Figure (1) illustrates the structure of Rijndael Algorithm [4]

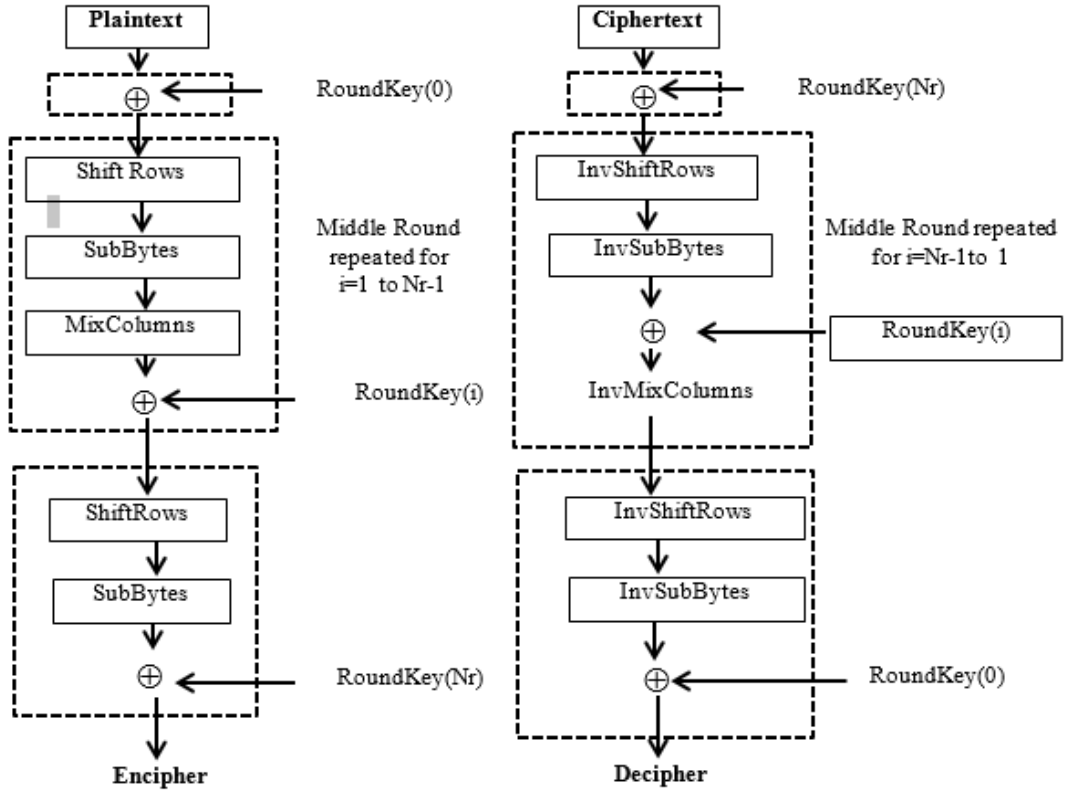

Figure -1: The Structure of Rijindael Algorithm

2.2- Number Theory Research Unit (NTRU) Method

NTRU was developed in 1996 and it is a rather new crypto-system. The cryptographic NTRU strength lies in the fact that it carries out various operations for the private key, with considerably lower level of time consumption compared with other methods. This algorithm has been based upon embedding the messages in the polynomial ring, R, consisting of the truncated polynomials of N-1 degree, which haves integer coefficients reduced mod specific parameters. The ring notation has been specified by the equation(1) :

$$R = Z[X]/(X^{N-1}) \ldots\ldots\ldots\ldots (1)$$

Z is a group of the integers and N is 1 more than polynomial degree. NTRU PKCS has been specified by several keys and parameters (par) as can be seen from the table (2) [5].

Table-2 : NTRU Parameter and Keys

Par	Explanations
N	The polynomials in truncated ring of polynomials have N-1 degree
P	Small modulus: The message coefficients are reduced to modulo p
Q	Large modulus: The truncated polynomials' coefficients are going to be reduced modulo q
F	A polynomial that is secret key
H	A polynomial which is public key
G	A polynomial which is utilized for the generation of the public key h from f

Par	Explanations
K	A security parameter that is utilized for controlling the resistance to specific attack types, which include the plain-text awareness.
R	The random “blinding polynomial.
dg	The polynomial g has dg coefficients = 1, dg coefficients = -1, and the remaining = 0.
df	The polynomial f has df coefficients = 1, (df-1) coefficients = -1, and the remaining = 0.
dr	polynomial r has dr coefficients =1, dr coefficients = -1, and the remaining = 0.

Sender wishes to create a pair of public/private keys for NTRU thus should apply steps illustrated in table (3).

Table-3: NTRU Key Generation

Step No.	Details
1	Choose two random polynomials f&g in the defined ring R. The polynomial is relative to random polynomial modulo q.
2	Compute the inverse of f modulo q as well as the inverse of f modulo p. The inverse values are represented respectively as fq & fp. $f \times fq = 1 \pmod q$ $f \times fp = 1 \pmod p$
3	select f such that its inverse values fq and fp exists.
4	Compute the product, $h = p.fq \times g \pmod q$
5	Sender secret key is the pair of polynomials f & fp. Bob's public key is polynomial h.

Receiver wishes to send a message to the sender with the use of the sender public key h. For more illustration about NTRU encryption, show table (4).

Table-4: NTRU Encryption

Step No.	Details
1	receiver converts his message as polynomial m in which the coefficients are selected mod p, in the range of –p/2 to p/2 (m represents a small polynomial modulo q)
2	receiver performs a random selection of a random polynomial r, utilized for obscuring the message.
3	receiver performs the calculation of the polynomial $e = pr \times h + m \pmod q$
4	polynomial e represents the encrypted message that is sent by the receiver to the sender.

Sender receiving the receiver encrypted message e, and wishes to decrypt it, now must implement NTRU decryption algorithm as illustrated in table (5) [6].

Table-5: NTRU Decryption Algorithm

Step No.	Details
1	Sender utilizes their private polynomial f for computing a = f × e (mod q), choose the coefficients of a in a range of –q/2 to q/2.
2	Sender will then compute polynomial b = a (mod p)
3	Reducing every coefficient of a mod p.
4	Sender utilizes their other private polynomial fp for calculating c = fp × b (mod p)
5	Polynomial c will be the original message m of the receiver

2.3- Data Encryption Standard (DES) Method

This it is a symmetric key encryption method, which means that the same private key will be utilized to encrypt and decrypt the message. DES is a block cipher which operates on fixed length plaintext input message blocks and processes with the use of the key, and performs the transformation of plain-text with the use of a complex set of the processes for the production of the ciphertext (of an equal length). Every block is numbered from the left to the right, making the 8 bits of every one of the bytes. The DES description has been illustrated in figure2.

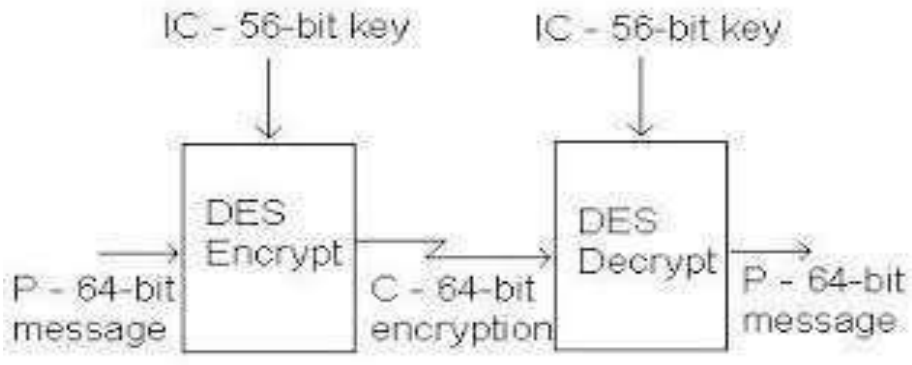

Figure-2: Description of DES Algorithm

It operates on 64bit plaintext for producing 64-bit ciphertext, which is why, 64-bit plaintext data has been provided as input for performing initial permutation (IP) first, then the key dependent permutation and finally the final permutation that is an inverse of the IP, in other words, IP-1 DES carries out 16 operation rounds for producing 64bit output data. DES implementation requires 4 main processes, fundamentally the shifting, XOR, permutation and LUT (Look up table). As can be seen from figure3 [7]. Initially, 64-bit data input is permuted through the application of initial permutation and after that, it is split to 2 equal parts, a left half (L0) and a right half (R0), every one of them is 32-bits long. The R0 in the first round becomes the left half of the following round and right half of the following round is resulted from initially expanding the 32-bits to 48bits through the use of the function of expansion in that is expanded through the repetition of some of the bits then those expanded 48-bits will be XORed with 48-bit key and the results will be fed to 8 substitution boxes (S-boxes) of 6-bits long, converting the 48-bit input into 32-bit result, in other words, 6-bit s-box produces 4-bit output for the purpose of forming eight 4bit boxes and ultimately a permutation is performed on those 32bits. In the following stage that 32-bit permuted output will be XOR-ed with the 1st right 32-bit half for getting the following 32-bit right half. The bit of the parity DES utilizes a 56 bit long key that is considered to be short, which is why, the DES algorithm has been considered as a weak algorithm. Actually, the DES key length is 64 bits long, however, only 56 bits are taken under consideration whereas the remaining of 8 bits are utilized as parity bits (in order to calculate the checksum). Function F in key dependent permutation has been considered as the most significant DES function [8].

2.4- Triple Data Encryption Standard (3DES) Method

The 3DES algorithm is of another form that has been considered rather secure, due to the long size of the key. This algorithm involves a 3 X 64 = 192bits long key, it is 3 times the single DES key length. The 3DES includes of 3 DES keys as can be seen from figure3, e.g. k1, k2 & k3 every one of them is 64 bits long. In the 3DES encryption, the data undergoes encryption with the 1st key (k1), after that, its output undergoes decryption with the 2nd key (k2) and finally, the result is encrypted once more with the 3rd key (k3). It should be remembered that only 56 bits of every one of the keys (k1, K2 & k3) are considered not 64 bits. Which means that 8 bits of each one of the keys are not considered as key bits and utilized as bits of parity, based upon those 3 keys' values [7].

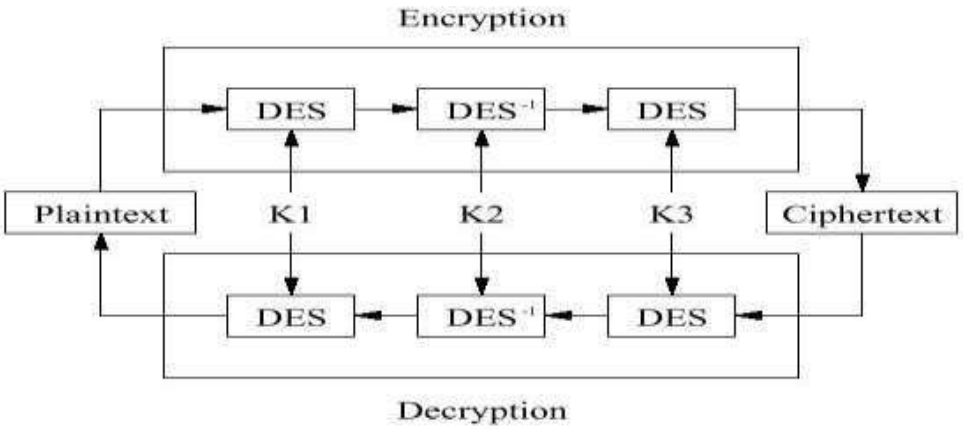

Figure-3: 3DES Keys

2.5- Elliptic Curve Cryptography (ECC) Method

Neal Koblitz and Victor Miller discovered Elliptic Curve Cryptography (ECC) in 1985. RSA and other primitive algorithms are similar to ECC schemes in which they used public key mechanism. In compared with the other pub-key cryptosystems, ECC offers comparable protection with smaller key sizes, less power consumption, faster computing and savings in bandwidth and memory. Thus, encryption algorithms which relying on discrete logarithms can be put in place effectively use elliptical curves.

However; the ECC function over points on an elliptic curve in contrast to the standard public key algorithms that run over the integer fields. In addition, as with many importance for the public cryptosystems, the CEC's level of safety depends on the key sizes used as well [9].

the ECC is relying on the ECDLP's problem. ECDLP specifies that in the case where there is an elliptical curve E identified through a finite field Fp and the two points P, then guessing the value of the integer k from Q2E(p)is atricky task. The cryptography of the elliptic curve involves three activities separately: generation of key, encryption and decryption. These operations are critical to create a legitimate cryptosystem. The message in ECC is firstly mapped on the curve using a valid point Pm. After that the Pm point of message is encrypted, so that we get a pair of Cm cipher points.This Cm will then be decrypted to restore the original Pm message point.An additional point is also needed for the purpose of key generation operation;this point is called the root of the generator (G). G is always in the same order as the ell iptic curve group Ep (a, b) in which p is a large prime integer, a and b are the elliptic curve param eters[10].

A large integer nB (nB < p) is retained as a secret key while the point PB = nB G is made as a pu blic. Besides to the publicly declared point, G and the elliptic curve details Ep (a, b) must also be made public. In case of there is no public information are defined

,

Thesender shall pick a positive integer k randomly such as k < p. The public key PB is then used

To produce the cipher text Cm consisting of two points {k G} and {Pm+ (k PB)}
The sender then sends C1 and C2 cipher points pair (both with the same Cm) to the recipient. The receiver multiplies the pair's first point by his own secret or private key when he receives the cipher point pair Cm and subtracts result as shown in equations below from the 2nd point [11].

2nd point nB 1st point

$= C2 - nB * C1$ ..... (2)
$= \big(Pm + (k * PB)\big) * (nB * (k * G))$ ..... (3)
$= \big(Pm + (k(nB * G))\big) * (nB * (k * G))$ ..... (4)
$= Pm$ ..... (5)

Pm is the original (x,y) point on the curve that was encrypted by the sender.

The smaller key size and faster computing power make ECC too significant to be overlooked even in transition from conventional to the quantum cryptography. The issue with the ECC is that it only deals with the coordinates of (x, y), while usually the sent messages are numbers, symbols and alphabets. In the ECC, as discussed earlier, a point Pm on a curve is encrypted into a pair of the points Cm (C1, C2) on the curve. However, the area of concern is the generation of the point Pm from the plain-text message M. The method of generating point Pm from plain-text M is referred to as the "mapping". The mapping not only should be limited to mapping of message, however, it should as well be ensuring that it can get back the original message M from Pm after the receiver decrypts Cm [12]. This process has been called as the "reverse mapping". The entire procedure has been depicted in figure (4).

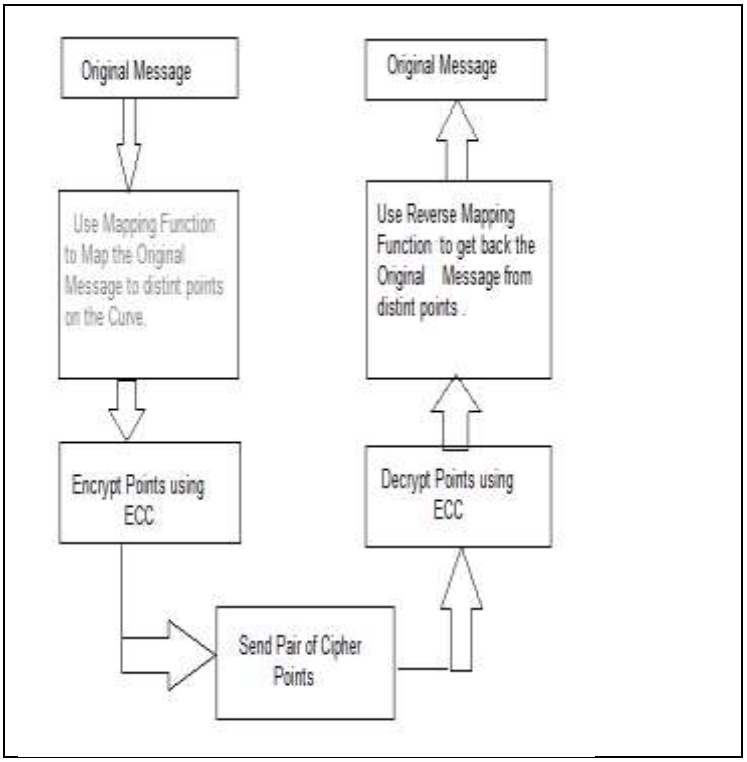

Figure-4 : Diagram of the Mapping and Reverse Mapping in the ECC

2.6- Rivest–Shamir–Adleman (RSA) Method
The security of algorithm is depending on hardness of factoring a large number of composites and a composite number for a specified odd integer e computing eth roots modulo. Public key of RSA consists of integer pair (n, e). The modulus n is a large number of composites while the public exponent ‘e’ is normally a small prime. The modularity is the result of multiplying 2 primes.

Using the main advantage of RSA, variable size key and encryption block to improve security [13]. To illustrate RSA encryption and decryption show figures (5-7) in addition to table (6)[14].

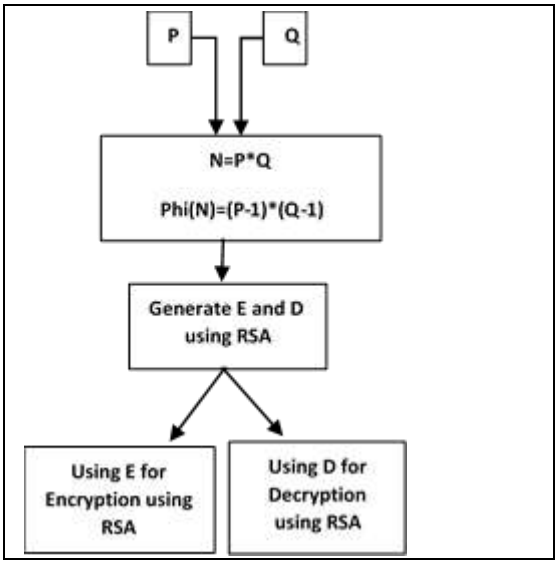

Figure -5: RSA Algorithm

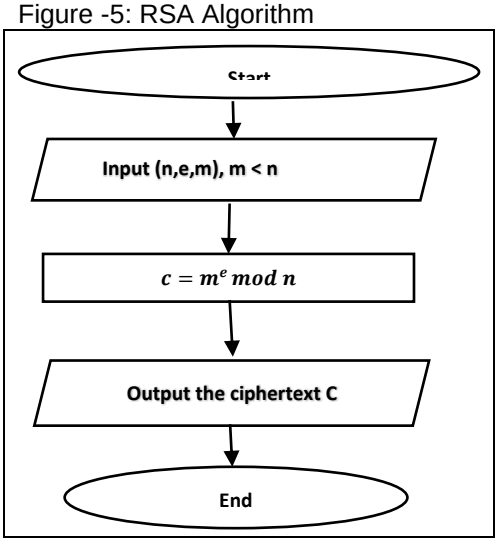

Figure -6: RSA Encryption

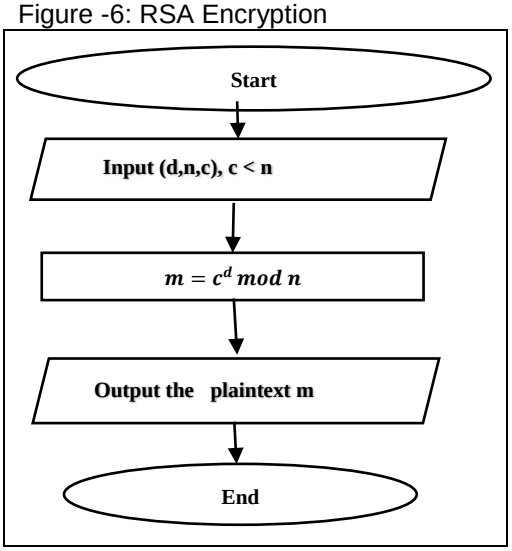

Figure-7 : RSA Decryption

Table-6: RSA Parameters

Symbol	Mean
N	Modulus
E	Public Exponent
M	Message
C	Ciphertext
D	Private Key

2.7- Optimal Asymmetric Encryption Padding (OAEP) Method

OAEP is a message encoding process, this process is done by encoding a message with OAEP. The encoded OAEP message is a concatenation of a string of "masked data" with a "masked random number'.' Masked data is formed in the simplest form of OAEP through taking result of th4e XOR of the plain-text M and the hash G of random string r. While the masked random number is XOR of r with hash H of masked data. An OAEP has several variants which has a component called "plaintext-awareness".' This means an opponent has to know the original plaintext to construct a valid encoded OAEP message. To achieve this, first, the plaintext message M is padded (e.g. with zeroes string) then the masked data is calculated [7-14].

2.8- Diffie-Hellman Algorithm (D-H)

W. Diffie and M. Hellman identified what Diffie-Hellman (D-H) algorithm is now known as. D-H key exchange is a systematic approach for the exchange of cryptographic keys, this algorithm generates the sender's and receiver's secret key. The D-H key exchanging method enables two parties without previous knowledge of one another in order to create a mutual secret key together with insecure channel of communication. After that, the key will be utilized for the encryption of the communications messages with the use of a symmetric key encryption [16]. For more illustration about D-H show table (7), figure (8).

Table-7: D-H Algorithm

Step No.	Step Calculation
1	Select two numbers 'R' and 'G'. 'R' is a prime number and 'G' is called as base
2	Select a secret number 'A' and another secret number 'B'
3	Calculate public number X = G^A mod R And Y = G^B mod R
4	Exchange their public numbers
5	Computes First session key as K1, K1= Y^A mod R
6	Computes second session key as K2, K2 = X^B mod R
7	Here K1 = K2 = K

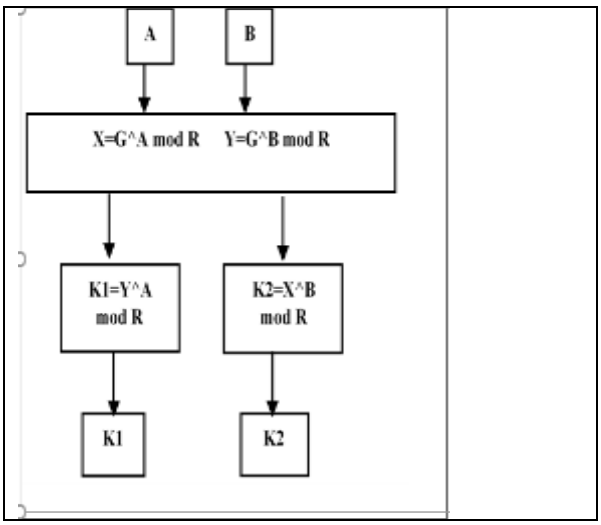

Figure-8: D-H Algorithm

2.9- Hisea Method

HiSea is an encoding for antisymmetric block, using an integer for the encryption and decryption of plain text. For the encryption process, message is a 64-byte ASCII, where the Hybrid Cube (HC) depends on multiplication the layer Magic Cubes (MC) matrix [13].

The HC matrix of the 4x4 command is defined as Hi, j , i {1, 2, 879} and j {1, 2, 3, 4} as follows:

Hij = MCi,j MCi, j, where the MCi, j is a jth layer of ith magic cubes. Assume we have coordinates x = {1, 2, 3, 4} where we multiply with the matrix of the MC 1 layer to produce HC 1 and then we generate HC 2 by multiplying the coordinates of the MC 2 layer withX = {1, 2, 3, 4}

In a similar way, we finish the remainder of a layers before a new HC cube has been built based upon MC layers, the sophistication may be expanded by combining many HC layers of input to build complex coding and decoding algorithms. Figure (9) show the HiSea's overall design, where keys, plain text,and encrypted text are structured in matrix 4 order in encryption method. HiSea encryption text, that is defined by protection and wide space and also has complex keys to guess or measure or time-consuming for attacker, this is added to enhance the encryption difficulty [17]. Diagram (1) illustrates the steps of HiSea Algorithm.

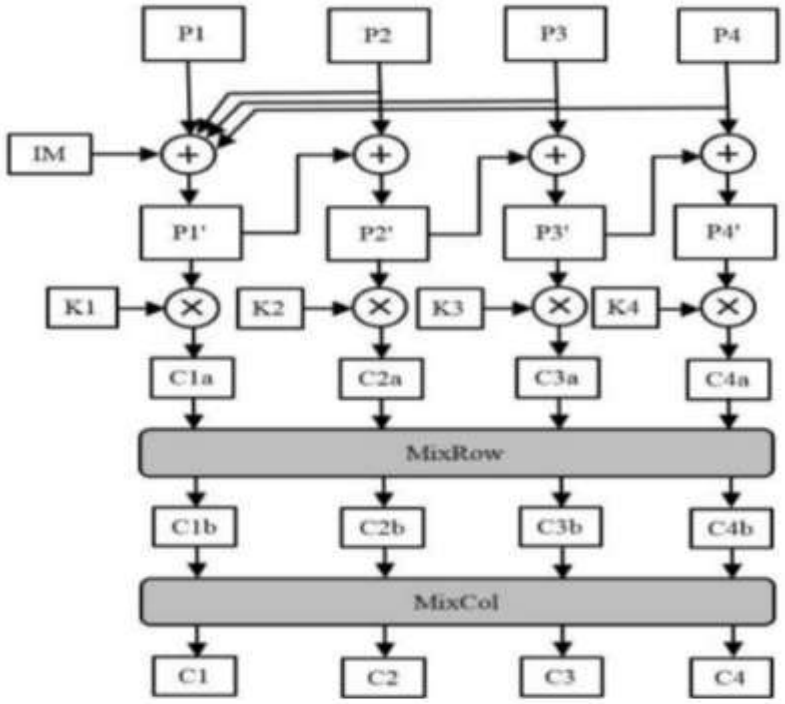

Diagram (1): Diagram of HiSea Algorithm

2.10- Improved Caesar Method

Cryptographic algorithms are utilizing Caesar cipher that was also referred to as shift cipher, is considered as one of the major utilized cipher-text techniques. Also, it is specified as a substitution cipher, in which each one of the characters in plaintext will be substituted by a letter which was some number of positions down in alphabet as shown in figure (9)[18].

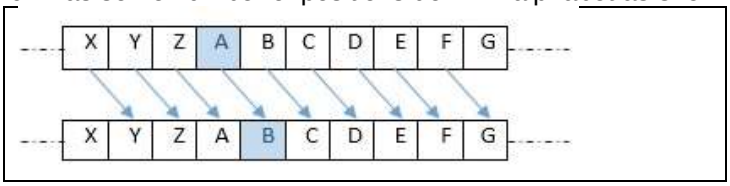

Figure -9: Traditional Caesar Cipher with Shift +1

Improved Caesar has the ability to handle case sensitive plain-text, the plaintext will be transformed to numbers, and after that during conducting a few computation operations on acquired numbers, the possibilities to get the same number for the corresponding letter was uncommon, while the Improved Caesar is specified for being case sensitive, thus, a lot of plaintext combination cases might be covered. All such properties are providing high-security to data which is transmitted by utilizing insecure channels which connect the receiver and sender. For the purpose of increasing the Caesar cipher, a few of the major mathematical calculations were achieved on cipher-text for increasing its strength. In addition, the decryption and encryption of plain-text were achieved by utilizing positional values and face values of corresponding characters as key. Table (8) and table (9) are clarifying the meaning regarding position values and face values, in which the face values were specified as the values allocated to the specific letter and fixed for corresponding one including, A-1, B-2….Z-26, a-27, b-28….z-52. Whereas the position values were allocated on the basis of the position regarding the matching letter in plaintext [19].

Table -8 : Face Values for Each Alphabet

Character	A	B	C	-	-	-	X	Y	Z	a	b	c	-	-	-	x	y	z
Face Value	1	2	3	-	-	-	24	25	26	27	28	29	-	-	-	50	51	52

Table -9 : Position Values for “CrYPtOgrAPhy”

Plaintext	C	r	Y	P	t	O	g	r	A	P	h	y
Position Value	1	2	3	4	5	6	7	8	9	10	11	12

Tables (10) and (11) explained the steps of improved Caesar algorithm for encryption and decryption consequently [18][19].

Table-10 : Encryption of Improved Caesar Algorithm

Step No.	Included
1	Transformation of the plaintext with the use of the basic Caesar cipher method
2	Using ciphertext which has been obtained from step1 and perform: • Assigning the values of the Face and the position to every one of the individual letters in ciphertext. • Summing up the distinctive values of the face of all letters in the cipher-text. • Subtracting the individual value of the face of every one of the ciphertext letters from the summation which has been obtained above. • subtracting the values of the position of every one of the metching letters of ciphertext which have been obtained from step2.
3	The resulted ciphertext will be sent to receiver in addition to the summation of the values of the face

Table-11 : Decryption of Improved Caesar Algorithm

Step No.	Included
11	Perform the following processes on the obtained cipher-text: • Adding the values of the position of every one of the corresponding letters to ciphertext as received from sender. • Subtraction of every one of the corresponding values which have been obtained from the step (1-a) from summation which has been obtained in addition to the cipher-text, for the purpose of getting the value of the face.

	• Transformation of obtained facial values to the corresponding alphabets.
2	Applying the fundamental Caesar cipher decryption for obtaining the plaintext

2.11- Digital Signature (DSA) Method

A digital signature means signing information in electronic form instead of writing the signature or seal through a string generated by public-key encryption technology, to identify the signer's identity and recognition on the information contained in data. Such a digitally signed data or transform allows the recipient of the data unit for confirming the integrity and source of the data unit. Through using DSA ensure the integrity, non-repudiation, and confidentiality of information in the transmission. The complete digital signature algorithm consists of two parts: the message-digest algorithm and encryption and decryption algorithms, secure Hash algorithm SHA-1 is the most commonly used in digest algorithm. This algorithm can achieve data integrity and authentication very good and has good resistance to aggressive. DSA using public-key cryptosystem to verify data integrity and data sender's identity for recipients with the use of a public key [20][21].

2.12 Advanced Encryption Standard (AES) Method

AES can be defined as a symmetric cryptographic algorithm where the length of the key and the data block of AES may vary based on requirement. The name of the AES is derived from the length of the key, like AES-128, -192 and -256. AES has been of a higher security compared to its predecessor algorithms, it is utilized for obtaining a high security level, however, it is utilized as well for achieving high efficiency and speed. The AES has been designed in a simple way, the protection from all of the known attacks, AES performs 10, 12 or 14 rounds, based upon the length of the key, such that for 128-bit key it carries out ten rounds, for 192-bit key it carried out 12 rounds and for 256-bit key it carries out 14 rounds. The processes of AES encryption/ decryption have been illustrated in diagram (2) [22]

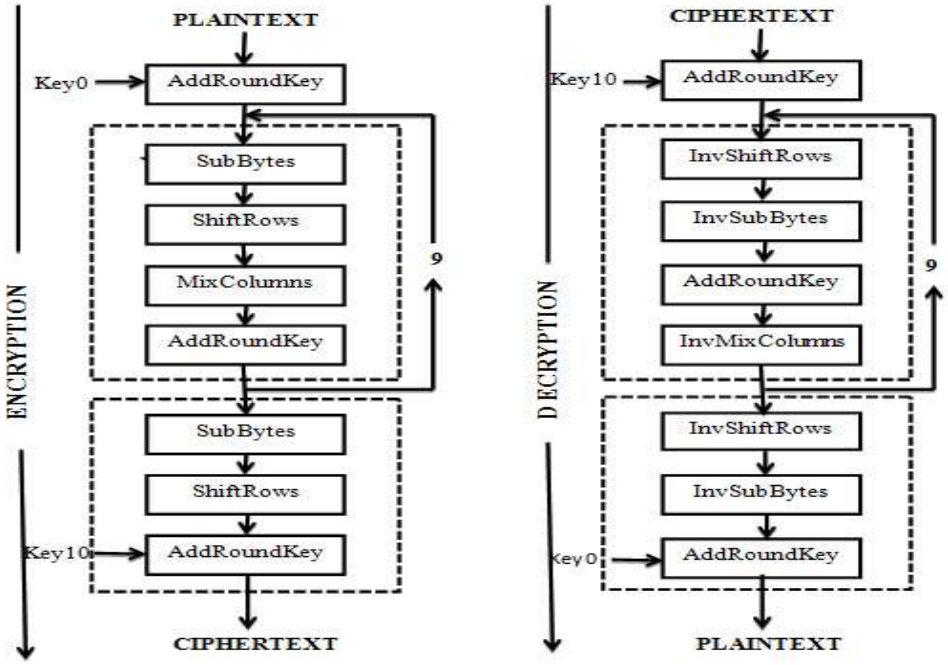

Diagram- 2: Diagram of the AES process of encryption and decryption

Each round of AES algorithm consists of the following four steps [23]:

a) SubBytes Transformation.
b) ShiftRows Transformation.
c) MixColumns Transformation.

d) AddRoundKey Transformation.

2.13- Improved Hill Cipher (IHC) Method

Hill cipher algorithm, deals with security issues, IHC algorithm, has optimum efficiency, according to the security issues. The concept of the IHC algorithm is the conversion of □ clear-text letters to □ cipher-text letters through a set of the linear transformation operations, this decryption only needs 1 inverse transformation operation, and the key is the actual transformation matrix. The password of the IHC is part of multiple-letter substitution codes and it is referred to as well, as the password of matrix transformation. The cryptography vector is □ as illustrates in the following equations: -

$$C = \begin{matrix} C1 \\ C2 \\ C3 \end{matrix} \quad \text{.....(6)}$$

$$M = \begin{matrix} m1 \\ m2 \\ m3 \end{matrix} \quad \text{.....(7)}$$

$$E(X) = 1/N \sum_{i=1}^{N} Xi \quad \text{.....(8)}$$

$$K = K(i,j) = \begin{matrix} k11 & k12 & k1i \\ k21 & k21 & k2i \\ ki1 & ki2 & kij \end{matrix} \quad \text{.....(9)}$$

In formula, □ represents the cipher-text and □ stands for the clear-text and key □ is an invertible matrix. The formula of the decryption is □ =□−1(mod□). All of the arithmetic operators are carried out under mod of □ = 26 [22].

3.Literature Review

According to the wide advancements of the networks and computer applications, the information security has great deal of attention in the daily areas of the life. The most significant issue is the way of controlling and preventing the unauthorized accesses to the secure information, therefore this review article presents a review of several researches that used hybrid cryptography algorithms for satisfying the information security purpose. At beginning show table (12) that illustrates the researches in this section.

Table- 12: Literature Review Researches

Research No.	Research Title	Author(s)	Year of Publication	Used Algorithms
1	Improved Rijndael Algorithm by Encryption S-Box Using NTRU Algorithm	Halah H. Mahmoud, Mayes M.Hoobi	2015	Rijndael, NTRU
2	Strong 3DES Algorithm with the use of the N-th Degree Truncated Polynomial Ring Unit	Mays M. Hoobi	2017	3DES, NTRU

3	Efficient Hybrid Cryptography Algorithm	Mayes M.Hoobi	2020	DES, ECC
4	Enhanced Multistage RSA Encryption Model	Mays M. Hoobi, Sumaya S. Sulaiman, Inas Ali AbdulMunem	2020	RSA, OAEP, D-H, Hisea,
5	Improved Structure of Data Encryption Standard Algorithm	Mays M. Hoobi	2020	DES, DSA, Improved Caesar,

Authors Halah H. Mahmoud, Mayes M.Hoobi In research no.1 as [4] presented “Improved Rijndael Algorithm by Encryption S-Box Using NTRU Algorithm”. This research presents a proposed Rijndael encryption and decryption process with NTRU algorithm, Rijndael is commonly accepted because of its strong encryption, and complicated processing as well as the fact that it is resistant to the brute force attacks. The suggested modifications have been implemented by encryption and decryption Rijndael S-Box using NTRU algorithm.

Author Mayes M. Hoobi in research no.2 as [6] presented “Strong 3DES Algorithm using N-th Degree Truncated Polynomial Ring Unit”. In order to increase the security degree in all communications, the two parties have to be having a copy of secret key which is, unfortunately, not easy to accomplished. The 3DES approach is weak because of its weak operation of the key generation, which is why, the key has to be re-configured for increasing the security of this algorithm, as well as its effectiveness and strength. The encryption key results in the enhancement of the security of the 3DES algorithm. Their study has suggested a combination of 2 sufficient algorithms of encryption for the satisfaction of the information security purpose through the addition of a new security level to the 3DES with the use of the NTRU. This goal has been accomplished through the addition of 2 new key functions, the 1st is the Enckey(), and the 2md is the Deckey() for encrypting and decrypting the key of the 3DES in order to make this algorithm more stronger.

Author Mayes M.Hoobi in research no.3 as[12] presented “Efficient Hybrid Cryptography Algorithm ”. One of the most significant issues and quite an important part of the cryptographic algorithms is its key. For the higher secure communication level the key has a significant impact, DES algorithm is weak because of its weak key generation, so that the key has to be re-configured for increasing the security of its algorithm as well as the effectiveness and strength. The key of encryption improves securities of the DES algorithm. This research assumed a combination of 2 sufficient algorithms of encryption for achieving the aim of the information security through the addition of a new security level to the DES with the use of the ECC. This goal has been satisfied through the addition of 2 new key functions, the 1st is the Enc_K(), and the 2nd is the Dec_K() for encryption and decryption key of DES algorithm to make this algorithm more confronted with the attacker

Authors Mays M. Hoobi, Sumaya S. Sulaiman, Inas Ali AbdulMunem in research no.4 as [14] presented “ Enhanced Multistage RSA Encryption Model”. Efficient and new editions of cryptography algorithms can help decrease security risks, any type of data has its own confidentiality, so new algorithms must be utilized for the protection of the confidential data toward unauthorized access. After reviewing RSA and attacking it, it would appear that a new model should be improved to mitigate this attacks and improve the security of the RSA algorithm.

In this research increasing the complexity and search space of RSA algorithm against brute force attack in addition to security enhancement was satisfied by applying four cases with using different cryptography algorithms. This four cases included case1: enhanced the security of RSA by using OAEP, case2: combining of the two most important algorithms RSA and D-H, case3: for increasing complexity and obtaining high level of security the two above cases (case1& case2) were concatenated, finally for most complexity and obtained highest security level with increasing search space of RSA case4 was applied. Case4: contained implementation of case3 in addition to apply new level of security by adding another cryptography algorithm called HiSea algorithm.
Author Mays M. Hoobi In research no.5 as [23] presented "Improved Structure of Data Encryption Standard Algorithm". Brute force attacks are the major DES attacks, this is the main reason that warranted the need for using the improved structure of the DES algorithm. This research proposes a new improved structure for DES to make it secure and immune to attacks. The improved structure of DES was accomplished by using standard DES with a new way of two key generations, this means the key generation system generates two keys one is simple and the other one is encrypted by using improved Caesar algorithm. The encryption algorithm in the first 8 round uses simple key1 and from round 9 to round 16, the algorithm uses encrypted key2. By using the improved structure of the DES algorithm

3.Conclusion

The cryptography has an important impact on the secure communications. For the secure communications, a variety of the cryptographic approaches have been utilized. Those approaches have been based upon the symmetric and the asymmetric keys. Every one of the cryptographic methods has its separate advantages and disadvantages. Which is why, it is significant to utilize the accurate encryption approach. After observing the researches in section 3 it has been clear that. Those modifications have results in the enhancement of the complexity degree, increasing in the search space of the key, and making ciphered message hard to crack by attackers. According to results in those studies, the main conclusions may be summarized as increased complexity in the block cipher in an identical range in a finite field GF (28) and an increased search space of the key which increases the likelihood of the brute force attack which is utilized for the cryptanalysis of cipher. The security of any algorithm type depends upon the key secrecy. According to results of the studies, the fundamental conclusions may be summarized as enhanced key functions result in increasing the complexity of a block cipher result in increasing search space of the key which increases the likelihood of the brute force attacks which are utilized for the cryptanalysis of ciphertext. Any algorithm type's security is dependent upon key privacy. According to the results in the present study, the basic conclusions may be summarized as enhanced key functions which result in increasing the complexity in the block cipher increase search space for the key, which result in increasing the likelihood of the brute force attacks which are utilized for the cryptanalysis of cipher as it has been stated in the sections above. The conclusions of the use of multiple cryptographic algorithms in every one of the researches that have been explained in section2 that improved security level by increased the complexity and key search space that lead to protect the security goals against the attackers. After listed these works of this article our opinion is: all hybrid cryptography methods are used was very efficient and improved the security level of traditional algorithms such as DES, NTRU, RSA, D-H,….,etc, so, these works can be improved more and more in future works by concatenation among two or more of listed works to obtain higher complexity hybrid cryptography algorithms.

References:

Mayes.M, Strong Triple Data Encryption Standard Algorithm using Nth Degree Truncated Polynomial Ring Unit, Journal of Science, 2017, Vol. 58, No.3C, pp: 1760-1771

A. Rahman Dalimunthe, H. Mawengkang, S. Suwilo, and A. Nazam, "Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm," J. Phys. Conf. Ser., vol. 1235, p. 012030, 2019.

D. Nofriansyah, Syaref,Maya, Ganefri, Ridwan, Efficiency of 128-bit Encryption and Decryption Process on Elgamal Method Using Elliptic Curve Cryptography (ECC) in TELKOMNIKA (Telecommunication Computing Electronics and Control. 2018, vol. 16, no. 1, pp. 352–360.

Deborah G, Ariel M, Ruji P, Strengthening The Vernam Cipher AlgorithmUsing Multilevel Encryption Techniques, INTERNATIONAL JOURNAL OF SCIENTIFIC &

TECHNOLOGY RESEARCH VOLUME 8, ISSUE 10, OCTOBER 2019 ISSN 2277-8616.

Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

Fausto M, Jenny T, Miranda Alba, Danilo N, RSA EncryptionAlgorithm Optimization to Improve Performance and Security Level of NetworkMessages, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, August 2016.

Greetta.P, Shruti.S, "Improved Caesar Cipher Algorithm Using Multistage Encryption", IJCST Vol. 7, Iss ue 1, Jan - March 2016

Halah H. Mahmoud1*, Mayes M.Hoobi2, Improved Rijndael Algorithm by Encryption S-Box Using NTRU Algorithm, Iraqi Journal of Science, 2015, Vol 56, No.4A, pp: 2982-2993.

Kodali, Sarma. Energy efficient ECC encryption using ECDH. in Emerging Research in Electronics, Computer Science and Technology, Springer, pp. 471–478, 2014.

M. Haj and M. Qatawneh, "Parallel Hill Cipher Encryption Algorithm," International Journal of Computer Applications, vol. 179, no. 19, pp. 16–24, 2018.

Mayes M. Hoobi, Efficient Hybrid Cryptography Algorithm, Journal of Southwest Jiaotong University, Vol 55, No 3 (2020).

Mayes M. Hoobi, Improved Structure of Data Encryption Standard Algorithm, Journal of Southwest Jiaotong University, Vol 55, No 5 (2020).

Mays M. Hoobi1, Sumaya S. Sulaiman2, Inas Ali AbdulMunem, Enhanced Multistage RSA Encryption Model, 2nd international scientific conference of AL-Ayen University, July, 2020.

Preetha M, Nithya M, A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM, International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

Priyadarshini Patil, Prashant Narayankar,Narayan D G, Meena S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Science Direct, Elsevier, International Conference on Information Security & Privacy (ICISP), 11-12 December 2015, Nagpur, INDIA,PP 617-624, 2015.

Priyan, K. and Vishal, P. 2016. Design and Implement Dynamic Key Generation to Enhance DES Algorithm. International Journal for Research in Applied Science & Engineering Technology, 4(7).

Said. High Performance Methods of Elliptic Curve Scalar Multiplication. International Journal of Computer Application. 2014. vol. 108, no. 20.

Shaimaa K, Waleed R, Ahmed O, Zainab K, Subject Review: Comparison between 3DES, AES, &HiSea Algorithms,IJSRSET, Volume 6, Issue 6, 2019.

Sharad Boni,Jaimik Bhatt,Santosh Bhat," Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm", International Journal of Computer Applications (0975 – 8887)Volume 130, No.15, PP 7-11,November-2015.

Tingting Y, Yangyang L, Chengzhe L, Jie D, and Minghua X, The Improved Hill Encryption Algorithm towards the Unmanned Surface Vessel Video Monitoring System Based on Internet of Things Technology, Wireless Communications and Mobile Computing, Volume 2018.

Vilas, V.D. and Dinesh, V.P. and Ashok, S. W. 2014. Performance Evaluation of AES using Hardware and Software Codesign. IJRITCC International Journal on Recent and Innovation Trends in Computing and Communication 2(6).

Waleed Khalid Ahmed, M uamer N Mohammed, Norrozila Sulaiman, An Enhanced Encryption Algorithm for Database Protection Based on Dynamic Key and Reverse String, Journal of Engineering and Applied Sciences 12 (5): 1186-1191, 2017

Zhu, C.; Sun, K. "Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps", IEEE Access 2018, 6, 18759–18770.