ISSN: 0067-2904

Proposal Hybrid CBC Encryption System to Protect E-mail Messages

Soukaena Hassan Hashem
Computer Sciences Department, University of Technology, Baghdad, Iraq

Abstract

Email is one of the most commonly utilized communication methods. The confidentiality, the integrity and the authenticity are always substantial in communication of the e-mail, mostly in the business utilize. However, these security goals can be ensured only when the cryptography is utilized. Cryptography is a procedure of changing unique data into a configuration with the end goal that it is just perused by the coveted beneficiary. It is utilized to shield data from other individuals for security purposes. Cryptography algorithms can be classified as symmetric and asymmetric methods. Symmetric methods can be classified as stream cipher and block cipher. There are different operation modes provided by the block cipher, these are Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB) and Electronic Code Block (ECB). CBC used to complex the cryptographic systems, by using Initialization Vector (IV), Xoring, and encryption with specified key over chain of blocks, but CBC is vulnerable to chosen plaintext attack because the IV is static and vulnerable to chosen ciphertext attack because the encryption method with the key are static. This paper introduce a proposed E-mail messages encryption systems , the proposal based on modified CBC mode operation hybrid with some of techniques exploited in the encryption such as RADG, DNA, RNA and a suggested permutation methods. The proposed modifications applied on the CBC are generate IV randomly, generate key randomly, and propose encryption method, these modifications proposed to avoid the attacks that CBC is vulnerable to.

Keywords: cryptography, CBC, RADG, DNA.

مقترح تهجين نظام التشفير الكتلي المتسلسل لحمايه رسائل البريد الالكتروني

سكينه حسن هاشم
قسم علوم الحاسوب ، الجامعه التكنولوجيه، بغداد، العراق

الخلاصة

البريد الإلكتروني هو واحد من أكثر وسائل الاتصال استخداما. السرية والتكامل والتخويل تكون اهداف امان ضرورية في مجال الاتصال عبر البريد الإلكتروني ، خاصة في مجال الأعمال التجارية. ومع ذلك ، لا يمكن ضمان أهداف الأمان هذه إلا بمساعدة استخدام التشفير. التشفير يمكن تعريفه بانه هو تحويل المعلومات من نص صريح الى نص مشفر غير مفهوم يمكن فك شفرته فقط من قبل الاشخاص المخولين اللذين يمتلكون المفاتيح السريه. عادة يتم استخدام التشفير لحماية البيانات من الغير مخولين لغرض توفير الامنية. خوارزميات التشفير يتم تصنيفها الى نوعين الخوارزميات المتناظرة والخوارزميات غير متناظرة. الخوارزميات المتناظرة يمكن تصنيفها الى نوعين التشفير الكتلي والتشفير الانسيابي. التشفير الكتلي يوفر حالات مختلفة لانظمة التشفير مثل (ECB) , (CFB), (OFB), (CBC) . يعتبر CBC من اقوى الانواع التي يتم استخدامها لتوفير انظمة التشفير من خلال استخدام Initialization Vector (IV) وعمليه Xoring

*Email: soukaenehassan@yahoo.com

مع التشفير باستخدام مفتاح محدد. لكن المشاكل الاساسية التي تواجه CBC هي الهجوم من نوع Chosen plaintext attack بسبب ثبوتية ال IV والمشكلة الاخرى هي الهجوم من نوع Chosen ciphertext attackبسبب ثبوتية مفتاح التشفير. في هذا البحث اقترح نظام تشفير رسائل الايميل باستخدام ال CBC المحدث والمهجن مع بعض التقنيات المستثمره في التشفير مثل RADG و DNA وRNA وطرق بعثره مقترحه. ان التعديل المقترح لطريق CBC هو توليد ال IV عشوائيًا وتوليد المفتاح عشوائياً واقتراح طريقة تشفير ساعد في تجنب المشاكل الاساسية التي يعاني منها CBC.

1. Introduction

Utilize the Electronic mail (e-mail) is common in all the new information society. People utilize their personal computers, workstations and cell phones in order to send and read e-mails. While e-mail provides great comfort for sharing the information, it makes many research challenges. One of the vital issues is the security because of the weak network core. The protected email framework must give the accompanying two security properties which are: 1) Confidentiality: Only the intended recipient can read message sent. 2) Authentication: The intended recipient can determine the source of a particular message. 3) Integrity: ensure the message should not be modified through communication channel. Cryptographic techniques can be applied to in order to achieve the above two security goals [1]. Encryption can be defined as a mechanism which can be used in order to help the ensuring of the security by making the data inaccessible to everyone except the authorized recipient [2]. In cryptography, block ciphers are the most basic components in numerous symmetric-key encryption frameworks. The CBC, presents one of the most famous modes of the operations which use a block cipher in order to provide the confidentiality or the authenticity [3]. Figure-1 shows the CBC mode of operation.

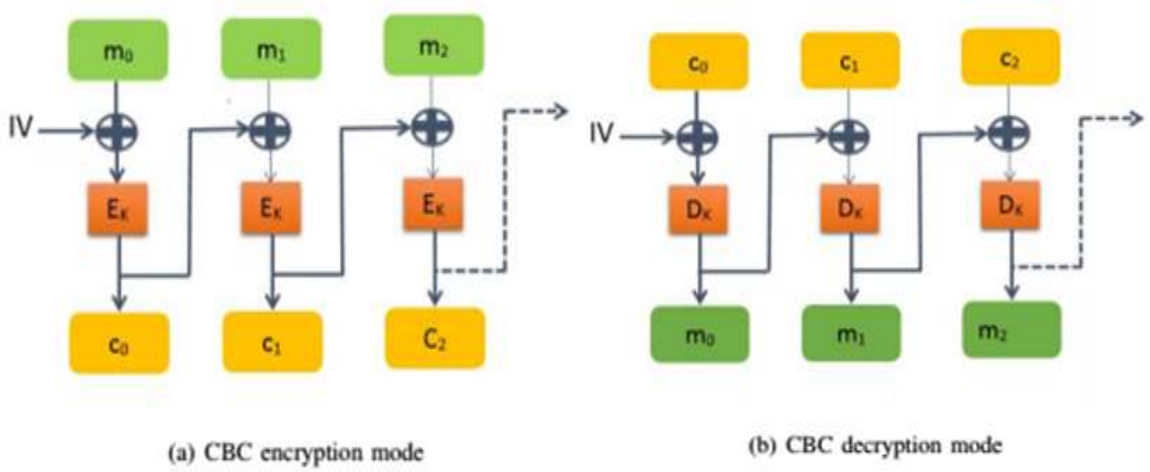


Figure 1-CBC mode of operation [3].

CBC block encryption mode offers a very common method of the encryption which is utilized in many implementations, regardless of the reality that the encryption in this mode can only be executed utilizing a single thread. Encryption block sequence is a block encryption mode which is utilized in order to provide the confidentiality, but does not integrate messages in the encryption. The operating basis in this mode is XOR adding to each block of the plaintext suffix to the previously received encrypted text. Each block depends on the subsequent encrypted text. Finally, the first clear text block is added to the XOR to IV. IV size is the same size as the plaintext blocks [4]. In order to make decryption to the encrypted text blocks, XOR output data from the decryption algorithm must be added to the earlier encrypted text blocks. The recipient knows all the blocks of the encrypted text only after receiving the encrypted message, and thus can decrypt the message utilizing many threads at once. If a portion of a simple text message (for example, due to some previous transmission error) is corrupted, all subsequent encrypted text blocks will be destroyed and the encrypted text received from that plain text can never be decrypted. Instead of that, on the off chance that one ciphertext bit is destroyed, only two received plaintext blocks will be destroyed. Finally, a message which is needed to

be encrypted utilizing the CBC mode should be outspread until being as long as a twofold of single blocks length [4].

Deoxyribonucleic Acid (DNA) cryptography represents a new and promising direction in cryptography research. DNA can be employed in cryptography for storing and carrying the information, in addition to computation. DNA is proved to be very powerful in cryptography, cryptanalysis and steganography problems. Hence, DNA can be utilized in cryptography to achieve an improvement in security and speed to the other cryptography methods [5]. DNA encoding can be defined as a technique to identify 4 different DNA bases A, C, T and G with 0 and 1. Instant messages can be effectively encoded utilizing this framework. Assume somebody needs to send the number "97" utilizing DNA encoding. It can change over "97" into a double frame by breaking 9 to 4 bits in twofold shape 1001 and 7 changing over to 0111. Both paired structures 9 and 7 are joined. The subsequent twofold number will be 10010111. Beginning from the left section, two successive parallel numbers are taken and changed over to the comparing DNA nucleotide bases by following the chart appeared in Table (1). In this way, the number "97" will be encoded as "CTTG". The encrypted message "CTTG" will now be sent over a channel to the recipient. The recipient then decodes them in order to extract the original message [6].

Table 1-Conversion scheme for binary form to DNA nucleotide [6]

Binary form	DNA nucleotide
00	A
01	T
10	C
11	G

RNA consists of four rules (abbreviations A, U, G and C), hence spreading its message with a genuinely basic code. As of late, inquire about has demonstrated an uncommon effect of RNA adjustments in all means of the development procedure. In excess of one hundred changes of RNA were related to parts in both hindrance and encouraging the official of proteins, DNA and other RNA particles [7]. New Keyless Security System Reaction Automata Direct Chart (RADG), which is based on the direct graph of the automatic situations and the interaction. RADG is rooted in the fact that it does not require any key to perform cryptographic operations; making it a practical blueprint for large wireless systems [8]. Figure-2 shows the transition design of RADG.

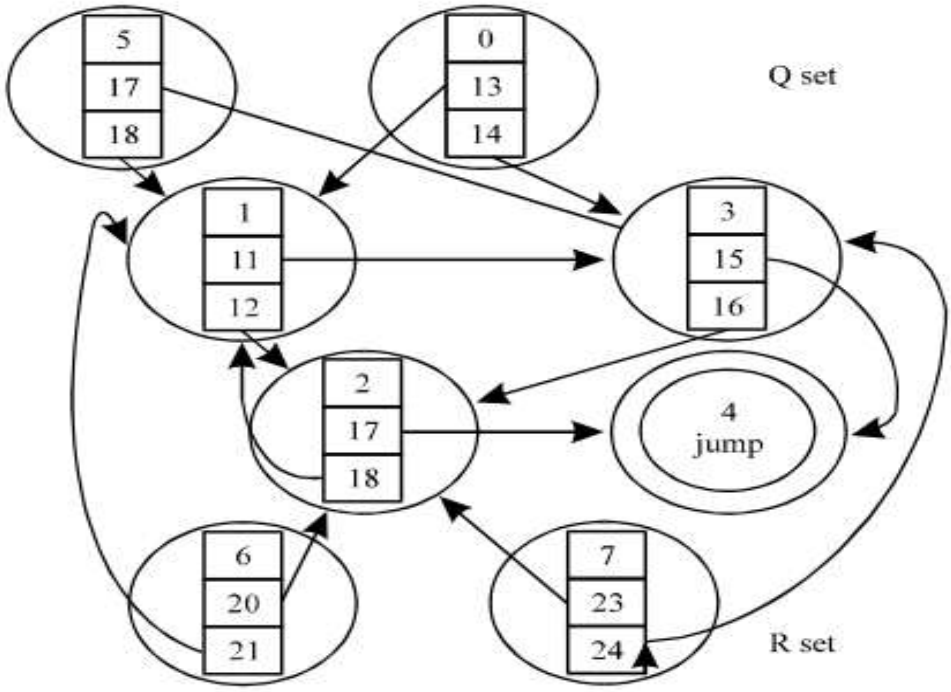


Figure 2-Transition Design of RADG [8].

2. Related Work

In 2017, Hudnall M., Vrbsky S., Parrish A. [9], they provide levers of "trust marks" (which are primarily developed in order to support one effective registration in a unified environment) to support secure e-mail messages between multiple systems where confidentiality and integrity requirements are particularly strict. Such a system can be used in order to increase the ability of users in different organizations to communicate without fear of revealing sensitive information intentionally or unintentionally. Although there are many barriers to adoption, this system may ultimately reduce reliance on separate communication networks and confidential communications systems.

In 2018, Hoomod H. K, Radi A. [10], they propose the security of the e-mail system which utilizes the modified AES algorithm and utilize the main biological chaos consisting of the biometric system and the chaos system (Lo and Lorenz). This amendment is utilized in order to make the proposed system more sensitive and random. The implementation time for both the encryption and the decryption of the proposed system is much lower than the original AES, in addition to being suitable with each mail server.

In 2015, Green M.D. , Miers I. [11], they investigate new mechanisms in order to achieve secure encryption forward in storage and forwarding systems such as the e-mail and the SMS. In a secure forward encryption system, the utilizer periodically updates his/her secret key so that the previous messages still confidential if their key is compromised. A fundamental commitment of the work is to give another type of encryption that is called puncturable encryption. Utilizing a repeatable encryption scheme, recipients may frequently update their decryption keys to disable the decryption for the selected messages, the recipients, or the time periods. Most importantly, this update does not need the recipients to make connection or distribution of new core materials to the senders.

In 2017, Nourai M., Levkowitz H. [12], they present and describe a new and comprehensive model of new technologies in order to protect the e-mail messages. The overall structure of this innovative model is simpler and effortless to utilize than the one currently utilized. They utilize a simplified trust model, which can be utilized in order to relieve the utilizers from having to perform many complex steps to achieve e-mail security. Utilizing the new technologies which are introduced in this work can protect users' email of the unauthorized access and protect their privacy. In addition, simplified infrastructure provides the ability to the developers in order to understand the structure in a way that is effortless to eliminate from interoperability.

3. Proposed E-mail Messages Encryption System

Emails are not secured because they are moving online. Messages may be intercepted, and read by the unauthorized or the unintentional persons. Email can also be amending stealthily - even falsely - creating the impression that a person has made a statement she/he has not done. Ordinary internet mail simply does not provide techniques in order to ensure the integrity, the privacy or the authorship. Email can be secured by restricting its movement on trusted computers and secure connections, but these controls are not possible in a large-scale environment with distributed management. As a result, the only way to protect the Internet mail is through the utilizing of encryption. The proposed encryption system is utilized the modified CBC operation mode to make the encryption more secure; since the original CBC version is vulnerable to two types of attacks which are: Chosen Plaintext Attack and Chosen Ciphertext Attack. Figure-3 and Algorithm (1) illustrate the proposed email encryption system.

a) Email Messages Encryption

b) Email Messages Decryption

Figure 3-The proposed System

Algorithm (1): Proposed Encryption System

Input: Email Message, Encrypted Email message

Output: Encrypted Email message, Email message.

Begin

Step1: Encryption

1.1 Read the Email message.
1.2 Convert the message characters to binary form.
1.3 Divide the binary codes of the secret message to n blocks.
1.4 Read the two seeds.
1.5 Generating the IV using the seeds (see algorithm (2)).
1.6 XORED between the IV and the first block and store the result in R1.
1.7 Read the secret two keys.
1.8 Generating the key using proposed key generation method (algorithm (3)).
1.9 Read the secret keys which will be used in the sub encryption method.
1.10 For I=1 to n

Begin

- If I =1 then

1. Encrypt R1 using the generated key (Algorithm (4)).
2. Get I ciphertext.
3. Store the result in R2.

- Else

1. Read I block.
2. XORED between the R2 and I block and store the result in Z.
3. Encrypt Z using the generated key (Algorithm (4)).
4. Get I ciphertext.
5. Store the result of the encryption in Z.

End

1.11 Send the result (n ciphertexts).

Step2: Decryption

2.1 Receive the n ciphertexts in binary form.
2.2 Read the two seeds.
2.3 Generating the IV using the seeds (see algorithm (2)).
2.4 XORED between the IV and the first block and store the result in R1.
2.5 Read the secret two keys.
2.6 Generating the key using proposed key generation method (algorithm (3)).
2.7 Read the secret keys which will be used in the sub encryption method
2.8 For I=1 to n

Begin

- If I =1 then

1. Decrypt R1 using the generated key (Algorithm (5)).
2. Get I plaintext block.

3. Store the result in R2.
- Else

1. Read I block.
2. XORED between the R2 and I block and store the result in Z.
3. Decrypt Z using the generated key (Algorithm (5)).
4. Get I plaintext block.
5. Store the result of the decryption in Z.

End

2.9 Convert the plaintext blocks binary form to characters.
2.10 Read the secret message characters.

Step3: End.

The main idea of the CBC is the encryption and providing randomness to the encryption. In the proposed encryption system CBC is used with special modification to it. These modifications can be classified as:

1) IV generation based two seeds which can be considered as private keys.
2) Key generation based DNA, RADG and RNA.
3) Proposed sub encryption method can be considered as the core of the CBC architecture.

3.1 Proposed IV and keys generation methods

In this section the proposed IV and keys generation methods will be illustrate in details.

3.1.1 Proposed IV generation method

Initialization Vector (IV) is one of the main parts of the CBC mode operation and plays an important role to provide difficulty in the predication of the plaintext. In the basic structure of the CBC the IV is static which make it vulnerable to chosen plaintext attack, but in the proposed encryption system a proposed method to generate IV and make it's generation dynamic in order to avoid the mentioned attack. Algorithm (2) shows the steps of IV proposed generation method.

Algorithm (2): IV Generation method

Input: Two secret seeds

Output: IV

Begin
Step1: Read seed1, seed2.
Step2: Swapping every seed characters with corresponding characters (table (2)).
Step3: Convert the swapping result to binary representation.
Step4: XOR between the first seed and the second seed.
End

Table 2-Characters corresponding swapping

Seq.	Character	Corresponding Swap character	Seq.	Character	Corresponding swap character	Seq.	Character	Corresponding swap character
1	a	;	17	q	5	33	6	p
2	b	‘	18	r	4	34	7	o
3	c	“	19	s	3	35	8	n
4	d	]	20	t	2	36	9	m
5	e	[	21	u	1	37	:	l
6	f	}	22	v	0	38	.	k
7	g	{	23	w	z	39	?	j
8	h	)	24	x	y	40	(	i
9	i	(	25	y	x	41	)	h
10	j	?	26	z	w	42	{	g
11	k	.	27	0	v	43	}	f
12	l	:	28	1	u	44	[	e
13	m	9	29	2	t	45	]	d
14	n	8	30	3	s	46	“	c
15	o	7	31	4	r	47	‘	b
16	p	6	32	5	q	48	;	a

3.1.2 The proposed Key Generation Method

The proposed key generation method consists of three parts which are: DNA coding, using RADG encryption method as pointer, and RNA coding. First the secret seed will be encoded using DNA codes (which provide 256 probabilities); second the RADG will be used as pointers to RNA coding table (which provides 64 probabilities). After that the RNA coding will be used to encode the secret codes as RNA codes. Then the RNA codes will be converted to binary form. The following algorithm illustrates the proposed system. The below algorithm illustrates the details of the proposed method.

Algorithm (3): Proposed Key Generation

Input: binary secret seed, sub secret key1, sub secret key2.

Output: Generated key.

Begin
Step1: Reading of the binary secret seed.
Step2: Convert the secret seed to DNA coding (table (3)).
Step3: Convert the DNA coding to binary form (table (4)).
Step4: Swap step3 bits using RADG to decimal values (Figure-4).
Step5: Read secret key1 which will be used in mathematical equation to choose the RNA codes.
Step6: Choose RNA codes.
Step7: Read the secret key2.
Step8: Apply rearrangement to every RNA codes.
Step9: Convert the RNA codes to binary form Table-5.
Step10: Read the key which will be used in the proposed sub encryption method.
End

Table 3-Binary to DNA bases

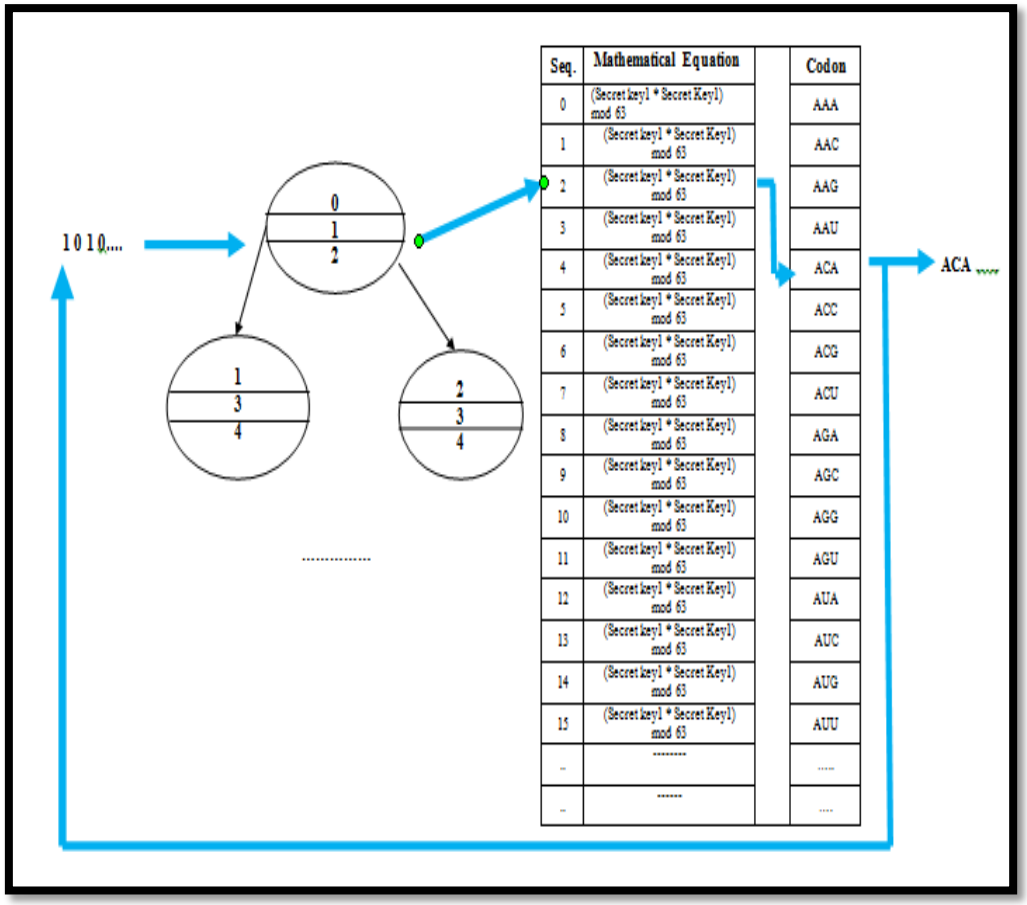
Binary code	Corresponding DNA bases
11	**A**
10	**C**
01	**T**
00	**G**

Table 4-DNA to Binary bases

DNA bases	Corresponding Binary code
A	**00**
C	**01**
T	**10**
G	**11**

Table 5-RNA bases with binary corresponding

RNA bases	Corresponding Binary code
A	**11**
U	**10**
G	**01**
C	**00**



Seq.	Mathematical Equation	Codon
0	(Secret key1 * Secret Key1) mod 63	AAA
1	(Secret key1 * Secret Key1) mod 63	AAC
2	(Secret key1 * Secret Key1) mod 63	AAG
3	(Secret key1 * Secret Key1) mod 63	AAU
4	(Secret key1 * Secret Key1) mod 63	ACA
5	(Secret key1 * Secret Key1) mod 63	ACC
6	(Secret key1 * Secret Key1) mod 63	ACG
7	(Secret key1 * Secret Key1) mod 63	ACU
8	(Secret key1 * Secret Key1) mod 63	AGA
9	(Secret key1 * Secret Key1) mod 63	AGC
10	(Secret key1 * Secret Key1) mod 63	AGG
11	(Secret key1 * Secret Key1) mod 63	AGU
12	(Secret key1 * Secret Key1) mod 63	AUA
13	(Secret key1 * Secret Key1) mod 63	AUC
14	(Secret key1 * Secret Key1) mod 63	AUG
15	(Secret key1 * Secret Key1) mod 63	AUU
..	--------	.....
..	------	....

Figure 4-Step4, Step5, Step6 illustration**.**

Example:

Secret Key2 =312 RNA codon=ACA

Apply Rearrangement using Secret Key2

1 2 3

RNA Codon = A C A using Secret Key2 which is (312) the Codon arrangement will be AAC.

Figure 5-Example of Step (7, 8) steps.

3.1.3 Proposed sub encryption method

The proposed method consists of three parts which are: binary bits processing and applying rotation to it using sub specific key which determine the no of rotation, reading the secret matrix and applying rotation to it using specific two sub secret keys. The first sub key is used to determine the number of row rotation. The sub second key is used to determine the number of column rotation. The third part is the reading of original generated secret key and processes it by converting it to binary codes, then to 2D array and after that performing row rotation and column rotation to this matrix using two sub specific keys. Algorithm (4) shows the proposed method.

Algorithm (4):- the proposed sub method (Encryption)

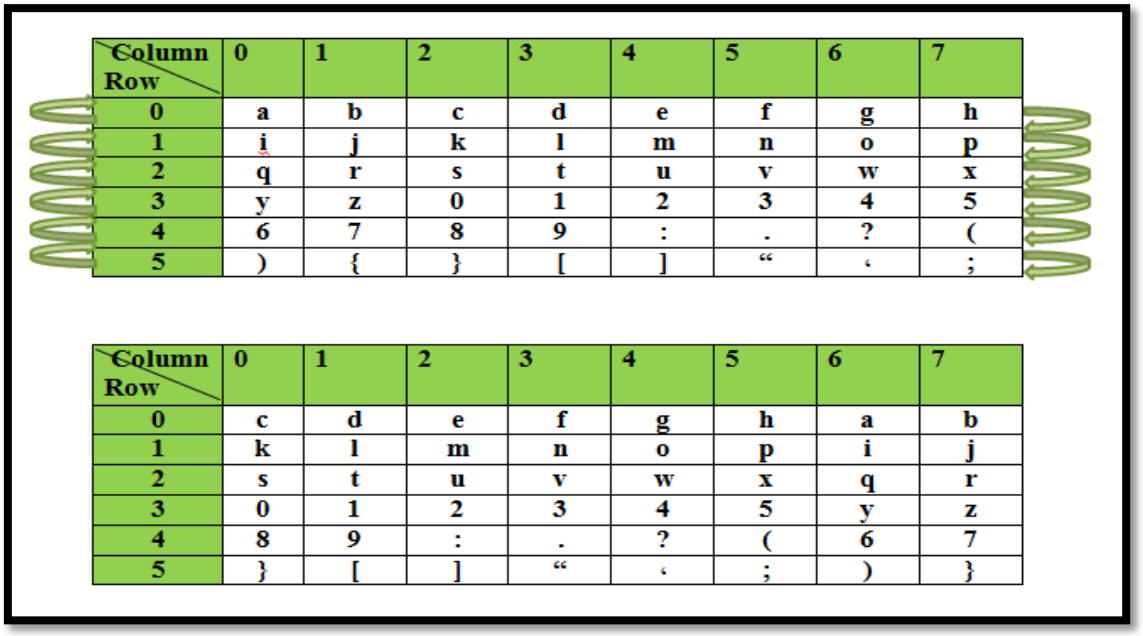
Input: - binary bits, generated key, sub secret keys.

Output: - binary bits after processing.

Begin
Step1: Read the binary bits.
Step2: Convert to virtual characters.
Step3: Read the sub secret keys (number of row rotation, number of column rotation).
Step4: Read the secret matrix of characters (Figure-6)).
Step5: Apply row rotation to the characters matrix using the sub secret key which determines the no of rotation (Figure-7)).
Step6: Apply column rotation to the characters matrix using the sub secret key which determines the no of rotation (Figure-8)).
Step7: Convert the virtual characters to numbers using the matrix after the rotation (Figure-9)).
Step8: Convert these numbers to binary representation.
Step9: Read the sub secret key which determines the number of the rotation to the binary representation in step8.
Step10: Apply rotation to step8 result.
Step11: Read the main generated key binary code (which is generated using the proposed generation method)(Figure-10).
Step12: Convert these binary codes to 2D array in order to apply row and column rotation.
Step13: Read the sub secret keys (no of row rotation, no of column rotation).
Step14: Apply row rotation to the matrix of the generated key binary codes using no of rotation (Figure-11).
Step15: Apply column rotation to the matrix of the generated key binary codes using no of rotation (Figure-12).
Step16: Convert this generated key matrix after rotation to 1D vector.
Step17: Apply XOR between Step10 and Step16.
Step18: Read the XOR result.
End

Figure 6-Secret matrix

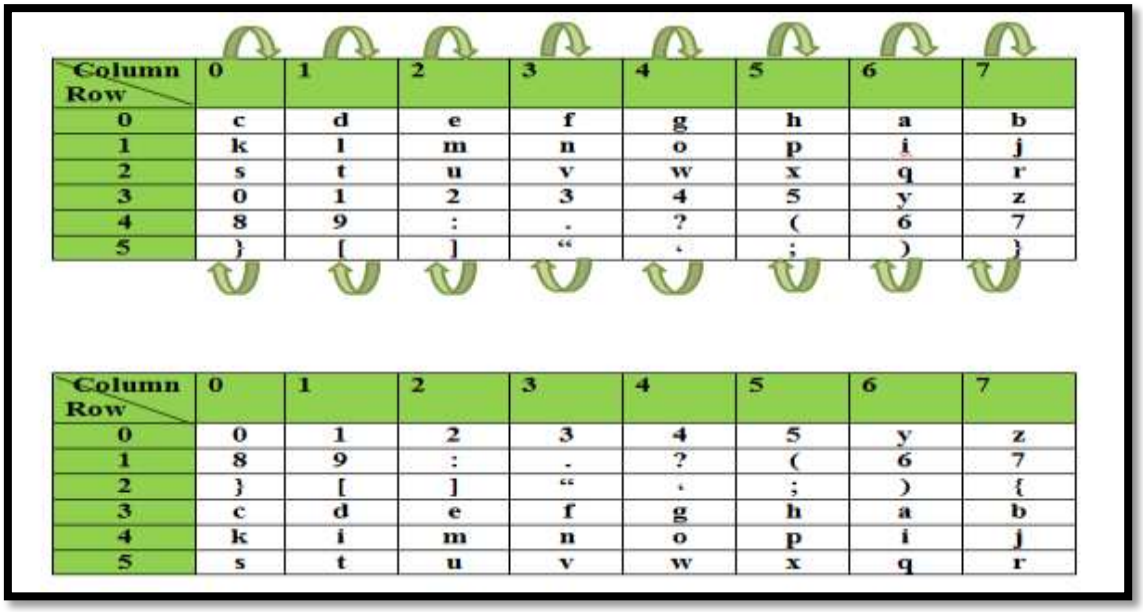
Column / Row	0	1	2	3	4	5	6	7
0	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
1	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
2	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**
3	**y**	**z**	**0**	**1**	**2**	**3**	**4**	**5**
4	**6**	**7**	**8**	**9**	**:**	**.**	**?**	**(**
5	**)**	**{**	**}**	**[**	**]**	**“**	**‘**	**;**



Column / Row	0	1	2	3	4	5	6	7
0	a	b	c	d	e	f	g	h
1	i	j	k	l	m	n	o	p
2	q	r	s	t	u	v	w	x
3	y	z	0	1	2	3	4	5
4	6	7	8	9	:	.	?	(
5	)	{	}	[	]	“	‘	;

Column / Row	0	1	2	3	4	5	6	7
0	c	d	e	f	g	h	a	b
1	k	l	m	n	o	p	i	j
2	s	t	u	v	w	x	q	r
3	0	1	2	3	4	5	y	z
4	8	9	:	.	?	(	6	7
5	}	[	]	“	‘	;	)	}

Figure 7-Row Rotation (secret key which specify no of rotations=2)



Column / Row	0	1	2	3	4	5	6	7
0	c	d	e	f	g	h	a	b
1	k	l	m	n	o	p	i	j
2	s	t	u	v	w	x	q	r
3	0	1	2	3	4	5	y	z
4	8	9	:	.	?	(	6	7
5	}	[	]	“	‘	;	)	}

Column / Row	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	y	z
1	8	9	:	.	?	(	6	7
2	}	[	]	“	‘	;	)	{
3	c	d	e	f	g	h	a	b
4	k	i	m	n	o	p	i	j
5	s	t	u	v	w	x	q	r

Figure 8-Column Rotation (secret key which specify no of rotations =3)

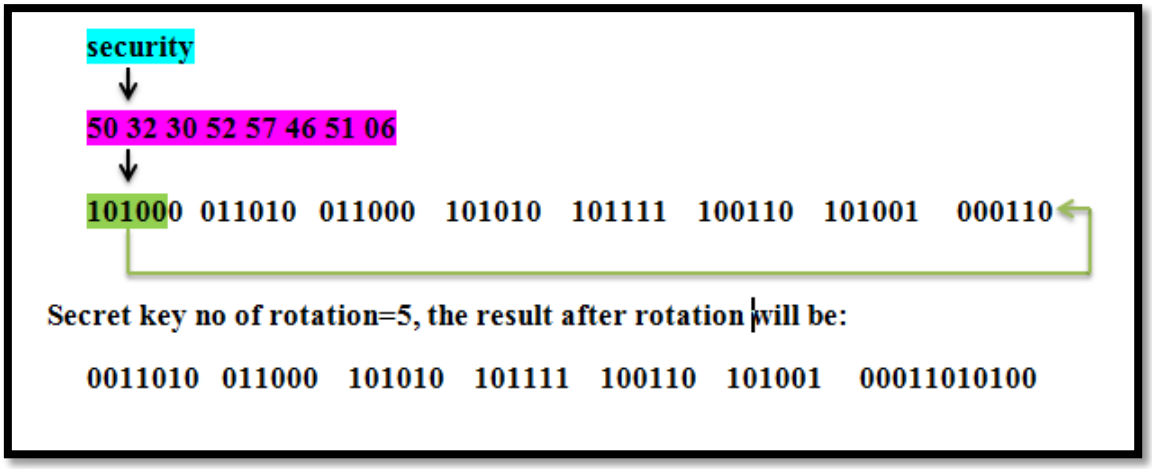


Figure 9-Example of Step7, Step8, Step9 and Step10

Generated key binary code:

0101 1100 0011 0100 0011 1010 0111 1100 1000 0010 1100 1011 1111 1011 0000 0010 00

Matrix of the generated key:

Column / Row	0	1	2	3	4	5	6	7
0	0	1	0	1	1	1	0	0
1	0	0	1	1	0	1	0	0
2	0	0	1	1	1	0	1	0
3	0	1	1	1	1	1	0	0
4	1	0	0	0	0	0	1	0
5	1	1	0	0	1	0	1	1
6	1	1	1	1	1	0	1	1
7	0	0	0	0	0	0	1/0	0/0

Figure 10-Example of Step11 and Step12

Column / Row	0	1	2	3	4	5	6	7
0	0	1	0	1	1	1	0	0
1	0	0	1	1	0	1	0	0
2	0	0	1	1	1	0	1	0
3	0	1	1	1	1	1	0	0
4	1	0	0	0	0	0	1	0
5	1	1	0	0	1	0	1	1
6	1	1	1	1	1	0	1	1
7	0	0	0	0	0	0	1/0	0/0

Column / Row	0	1	2	3	4	5	6	7
0	1	0	1	1	1	0	0	0
1	0	1	1	0	1	0	0	0
2	0	1	1	1	0	1	0	0
3	1	1	1	1	1	0	0	0
4	0	0	0	0	0	1	0	1
5	1	0	0	1	0	1	1	1
6	1	1	1	1	0	1	1	1
7	0	0	0	0	0	1/0	0/0	0

Figure 11-Generated key matrix with row rotation (no. of row rotation =1)

Column / Row	0	1	2	3	4	5	6	7
0	1	0	1	1	1	0	0	0
1	0	1	1	0	1	0	0	0
2	0	1	1	1	0	1	0	0
3	1	1	1	1	1	0	0	0
4	0	0	0	0	0	1	0	1
5	1	0	0	1	0	1	1	1
6	1	1	1	1	0	1	1	1
7	0	0	0	0	0	1/0	0/0	0

Column / Row	0	1	2	3	4	5	6	7
0	0	1	1	0	1	0	0	0
1	0	1	1	1	0	1	0	0
2	1	1	1	1	1	0	0	0
3	0	0	0	0	0	1	0	1
4	1	0	0	1	0	1	1	1
5	1	1	1	1	0	1	1	1
6	0	0	0	0	0	1/0	0/0	0
7	1	0	1	1	1	0	0	0

Figure 12-Generated key matrix with column rotation (no. of column rotation =1)

Algorithm (5): the proposed sub method (Decryption)

Input: binary bits generated key, sub secret keys.

Output: binary bits after processing.

Begin
Step1: Read the received binary bits.
Step2: Read the generated key binary code, see Figure-10.
Step3: Convert Step2 binary code to 2D array, see Figure-10.
Step4: Read the number of Row rotation and the number of Column rotation.
Step5: Apply inverse row rotation, see Figures-(11, 12).
Step6: Apply inverse column rotation, see Figures-(11, 12).
Step7: Convert to 1D vector.
Step8: XOR between the received binary code and Step7.
Step9: Read the number of Rotation to retrieve the secret binary codes, see Figure-13.
Step10: Apply inverse rotation to this code, see Figure-13).
Step11: Retrieve the decimal numbers from this binary code, see Figure-13.
Step12: Read the number of Row and number of Column rotation.
Step13: Read the secret matrix.
Step14: Apply inverse Rotation to the matrix rows.
Step15: Apply inverse Rotation to the matrix columns.
Step16: Retrieve the characters that are corresponding to the decimal numbers (step11) using the rotated matrix.
Step17: Retrieve the secret text characters to binary bits.
End

4. Implementation and Experimental Results

The main feature of the CBC encryption is the randomness of the encryption and in the proposed system. This randomness is increased since in addition to the randomness of the CBC encryption. The secret keys will be used in the proposed sub encryption method that are generated. This key is random based the NIST randomness measures. Also, the generated ciphertexts which the proposed system produced by the random keys are randomly based on the NIST randomness measures. Table (6) shows the randomness measures for the generated key (5 tests) and for the ciphertext (5 tests). Figure-14 and (15) are charts of these tests.

Table 6-The randomness measures of the generated key (5 keys)

Seq.	Generated Key bits/ Ciphertext bits	Frequency Test Value	Block Test Value	Runs Test Value
1	0101 1100 0011 0100 0011 1010 0111 1100 1000 0010 1100 1011 1111 1011 0000 0010 00	0.62	0.13	0.33
	1100 1001 0000 1111 1101 1010 1010 0010 0010 0001 0110 1000	0.38	0.74	0.48
2	1001 1100 1110 0000 1101 1101 1111 1000 0001 1010 1100 0000 1110 1010 1011 0111 01	0.62	0.43	0.64
	0110 0011 1111 0011 0000 0101 1010 1010 1001 1011 0111 1001	0.56	0.54	0.54
3	1100 1001 1101 0000 1101 1000 1110 1111 1100 1110 0000 1010 0111 1011 1010 0100	0.46	0.26	0.66

	11			
	1100 1111 0101 1010 1001 1010 1100 0000 1111 1010 0001 0111	0.56	0.42	0.73
4	0000 1100 1001 1100 1101 1000 1100 1010 1110 1001 1011 0111 1111 1110 1010 0100 10	0.46	0.3	0.57
	0011 1001 1100 1111 1010 0011 1011 0100 1110 1011 1010 1111	0.08	0.42	0.64
5	1010 0001 1101 1001 1100 1100 1001 1111 1110 1011 1001 0001 1100 1000 1011 0101 11	0.32	0.59	0.9
	1111 1010 1100 0101 1000 0011 1010 0100 1011 1100 0001 0101	1	0.67	0.77

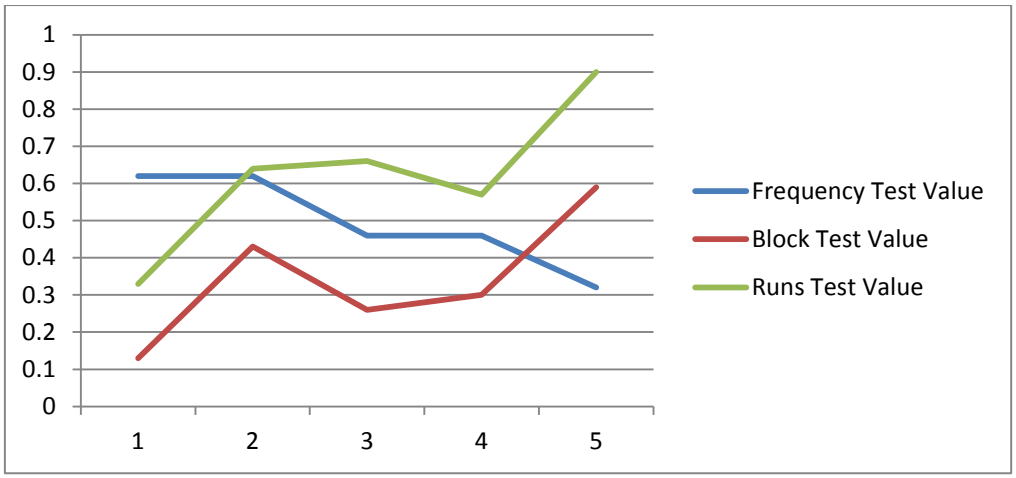


Figure 14-Chart of the randomness measures of generated 5 keys

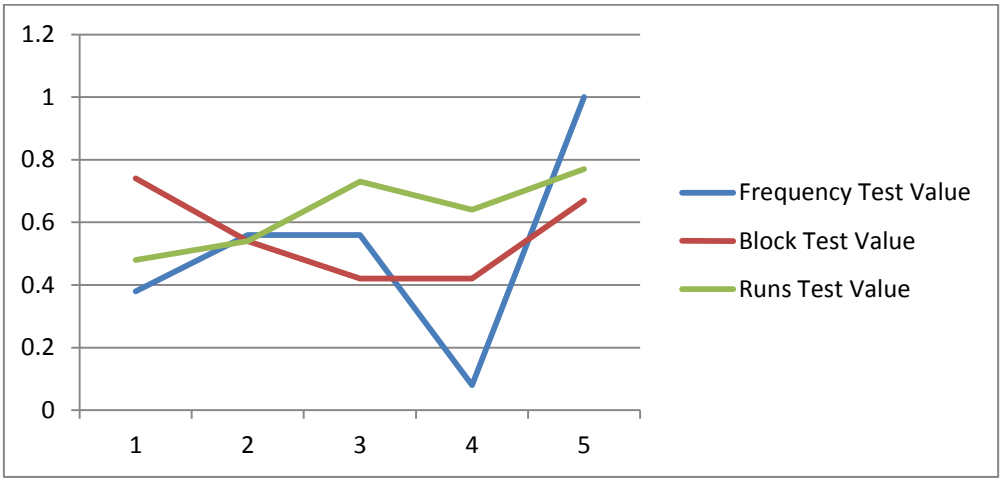


Figure 15-Chart of the randomness measures of ciphertexts encrypted by the 5 keys.

The correlation coefficient of the proposed system in the case of the (generated keys) is (-1) which means that the generated keys are not identical. Also for the ciphertext the correlation coefficient is (-1). This value of the correlation is coefficient proof of the proposed system protection against the

chosen plaintext attack and chosen ciphertext attack and provides the main features of secure Email system which are confidentiality, integration and authentication.

5. Conclusions

Recipient e-mail messages are between the sender's mailbox and the recipient's mailbox on open systems and insecure networks. These messages may be vulnerable to tapping it poses a real risk to the privacy and the integrity of the unauthorized data. E-mail security must include the following properties (confidentiality, authentication, Message integration). Encryption is used to provide these concepts to Email communication.

In this work a proposed encryption system based one of the operation modes which are CBC as general structure of the proposed system. Based on the proposed system analysis and details the following points can be concluded:

1. The proposed system provides confidentiality, authentication, and message integration to email messages.
2. The proposed system provides randomness to the encryption since it is the main feature of CBC because the IV is generated in every time the encryption occurs so the email messages will be protected from the chosen plaintext attacks.
3. The proposed key generation method uses multiple secret keys (secret seed, sub secret key1, sub secret key2) in order to make the key generation random so the email messages will be protected from the chosen ciphertext attacks.
4. The proposed sub encryption method should be used multiple secret keys (generated key, seeds, keys, secret matrix, number. of the row rotation, number of the column rotation, no of binary code rotation).
5. The proposed sub encryption method uses rotation, expansion, and rearrangement processing, so hybrid techniques are validated and this will increases the randomness.

References

1. Li F., Zhong D. and Takagi T. **2016.** ” Efficient Deniably Authenticated Encryption and Its Application to E-mail”, IEEE Transactions on Information Forensics and Security, 2016.
2. Mehta R., Iyer S., Sankhe A. **2017.** ”Semantic E-Mail Addressing Using Digital Signature (SEADS)”, 2017 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS).
3. Abidi A., Tawbi S. and Guyeux C. **2016.** “Summary of Topological Study of Chaotic CBC Mode of Operation”, IEEE International Conference on Computational Science and Engineering.
4. Abidi A., Guyeux C., Demerjian J., Bouall B., Bouall`egue B. and Machhout M. **2018.** ” Lyapunov Exponent Evaluation of the CBC Mode of Operation”, *Chaotic Modeling and Simulation* (CMSIM) **2**: 185–196, 2018.
5. Hameed, S.M., Sa’adoon H. A. and Al-Ani M. **2018.**” Image Encryption Using DNA Encoding and RC4 Algorithm*”, Iraqi Journal of Science*, 2018, **59**(1B): 434-446.
6. Hazra A., Ghosh S. and Jash S. **2018.**” A New DNA Cryptography Based Algorithm Involving the Fusion of Symmetric-Key Techniques”, Springer Nature Singapore Ltd.
7. Heilesen, L. **2018.** ” Encrypted messages in biological processes”, June 21. Department of Molecular Biology and Genetics.
8. Albermany S., Nathim M. and Hussain Z. M. **2017.** ” CRADG: A chaotic RADG security system”, *Journal of Engineering and Applied Sciences*, September 2017.
9. Hudnall M., Vrbsky S. and Parrish A. **2017.** ” Implementing Secure E-Mail on the Open Internet with MailTrust”, Conference: IEEE International Symposium on Technologies for Homeland Security (HST).
10. Hoomod H. K, Radi A.,” New Secure E-mail System Based on Bio-Chaos Key Generation and Modified AES Algorithm”, IOP Conf. Series: *Journal of Physics*: Conference, Series 1003 (2018) 012025.
11. Green, M.D. and Miers I. **2015.**”Forward Secure Asynchronous Messaging from Puncturable Encryption”, IEEE Symposium on Security and Privacy, 2015.
12. Nourai, M. and Levkowitz, H. **2017.** ” Securing Email for the Average Users via a New Architecture”, IEEE Symposium on Security and Privacy.