Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 9, No. 2, June 2021, pp.1115-1123

A proposed encryption technique of different texts using circular link lists

Wisam Abed Shukur [1], Ahmed Badrulddin [2], Mohammed Kamal Nsaif [3]
[1] University of Baghdad, College of Education for Pure Sciences/Ibn Al-Haitham, Computer Science Dept., Iraq
[2] University of Baghdad, Baghdad University Presidency, Law Affairs Dept. Iraq
[3] University of Baghdad, College of Education for Pure Sciences/Ibn Al-Haitham, Computer Science Dept., Iraq

ABSTRACT

A different texts encryption technique is presented in this paper. The sensitive information is encrypted in different manner via using circular link lists as data structure that contains different encryption algorithms such as: LU and LEE, Rabin, Okamoto-Uchiyama, McEliece and Paillier algorithms. Using circular link lists as data structure aims for making the information ciphering most secure. The main idea of using circular link lists is making each character of sensitive information will encrypt by different cipher method in each iteration of encryption process. The above encryption algorithms are scheduled in circular link lists and selected via execution process respectively. The sensitive information that used in this work are consist of English and Arabic texts. So, the special characters and symbols are considered. The merge text from different languages such as English and Arabic with its special characters and symbols is encrypted effectively. When a different text encryption technique is implemented, the experimental results illustrate the high level of security, the ability to cipher merge texts and efficiency. The security, integrity and complexity are satisfied in this work.

Keywords: Cryptosystem, Public-Key, Circular Link Lists

Corresponding Author:

Wisam Abed Shukur
University of Baghdad, College of Education for Pure Sciences/Ibn Al-Haitham
Computer Science Dept., Iraq.
Email: wisam_shukur@yahoo.com, wisam.a.s@ihcoedu.uobaghdad.edu.iq

1. Introduction

In the last decade, many of protection applications are produced because development of networking and communicating infrastructures [1]. However, all parties consider the cryptography is alone suitable efficient method to protect information via insecure transmission channels. Converting process of information that considered as understood quantity into a way which allows the unauthorized parties cannot understand its content is called cryptography [2]. To obtain strong or good encryption algorithm, must applying a proposed different manner or complex mathematics [3]. The strong point of the proposed different texts cryptography method is using proposed manner to schedule and regulate set of cipher methods that is circular link list data structure. This manner gives ciphering a character with different used methods that stored via circular link list initially. The process of these different cipher methods is controlled by four parameters: control key, flag, pointers and counters [4]. The background theoretical of used encryption algorithms is illustrated in the following section shortly.

2. LU and LEE, Rabin, Okamoto-Uchiyama, McEliece and Paillier algorithms

The LU and LEE who proposed this method of encryption to overtake all drawbacks of RSA. therefore, it gives more advantages than RSA practically. The speed of LU and LEE is fast than RSA because its processes of encryption and decryption are much simpler since their mathematics foundations such as arrays. It requires key generation initially. In this process, choose p and q as prime, then find n from product p and q. a11, a12, a21, a22 are selected and must be satisfy $a11*a22 - a12*a21! = 0$, to calculate integer b1 and b2, applying Euclid's algorithm with condition $b1*p - b2*q = 1$. after that we find C1, C2 by applying $C1 = ((a21 - a11)* b1 * p + a11) \bmod$ and $C2 = ((a22 - a12)* b1 * p + a12) \bmod n$ to obtain public key that consists of (p, q, b1, b2, a11, a12, a21, a22). To

cipher the information, must be divided into pair number m1&m2 satisfying 0 < m1 < S1 and 0 < m2 < S2 then we apply the C = C1 *m1 + C2* m2 mod n to obtain encrypted text. While decryption process is executed by applying the following relations: M1=(C'a22-C"a12)/(a11a22-a12a21) and M2=(C"a11-C'a21)/ (a11a22-a12a21), and C '=C Mod P, C" =C Mod Q [5].

Rabin cipher is like RSA essentially but choice of e is an optimal. its security is more closely with factoring process than RSA. it is important making a rule for choosing the accept solution in decryption process. if N = p*q then p and q are primes distinct amd squaring is a four-to-one map. as with RSA, the m value in encryption process is a symmetric key actually. to simplify taking of square roots, the choice of p, q ≡ 3 (mod 4). the Rabin method is used with other moduli efficiently. Since it includes the squaring operation and it assumes the security, the square roots computing modulo N is related. This means in turn is equivalent to factoring process. The main different feature of Rabin comparing with RSA is hardness of breaking. the public and private keys are used in Rabin cipher as all asymmetric cryptosystems works. The public key is used for encryption process and published, while the private key is possessed by the recipient. the public and private keys are generated by generating pair primes p and q as large random with same size roughly. To obtain n value, multiply p with q. the public key is n and private key is (p,q). in encryption process, the message or information is represented by integer form **m** with R [0, 1…n-1] and we find c value that represents cipher text by applying following relation: C = m^2 Mod n, Sending c value to recipient via communication channel [6]. While in decryption process, to obtain plain text from c must using private key to result m1, m2, m3 and m4 by applying the following relations:

m1 =C^ ((p+1)/4 Mod p, m2 = (p-C^ ((p+1)/4)) Mod p
m3 =C^ ((q+1)/4) Mod q, m4 = (q-C^ ((q+1)/4)) Mod q

To find a, b values, by applying the following relations:

a=q* (q^{-1} Mod p), b=p* (p^{-1} Mod q). finding possible solutions that are four: M1= (am1+bm3) Mod n, M2= (am1+bm4) Mod n, M3= (am2+bm3) Mod n and M4= (am2+bm4) Mod n. Recover m after we choose one of them if it is English text then it is easy to recover but if message random bit stream like such as digital signature or key generation there must add some text before encryption process.so, Gcd (m, n) ≠ 1, the cipher text c doesn't have four square, but rather only one or two.

The OU (Okamoto-Uchiyama) considered as a part of cryptographic. information sending by sender to pass it via a known communication tool between them, main goal is concealing information from unauthorized or a third party. the encryption process is done by sending party and the decryption process is done to result the messages before actions of encryption process by receiving party. With OU, the security is sent with a public communication since using a variable random probabilistic which prevents unauthorized or a third party from determining which ciphered information produced from a special plaintext. the secret or private p, q and (n = p2 q) as not private are generated then distributed via a secured channel as communication tool between them. The OU as shown in following steps [7]:

1. $g^n n = p^2 q$p and q as pair large prime will generate and set
2. g ∈ (Z/nZ)* is Choosing and $g^p \neq 1$ Mod p^2.
3. Assume h= Mod n.
4. The (n,g,h) are considered as not private and (p,q) are considered as not public.

In ciphering process, a message or information m is encrypted, where m is an element in Z/pZ according to below steps:

1. Select r ∈ Z/nZ at random.
2. $L(x) = \frac{x-1}{p} g^m h^r$Cipher text C = mod n.

$m = \frac{L(C^{p-1} mod\ e^2)}{L(g^{p-1} mod\ e^2)} mod\ e$While in deciphering process, if we define
and the decryption process is done by applying the following relation:

The McEliece cryptosystem considered as one of the most promising algorithms that uses public-key technique. It differs from other public-key cryptosystem because exploiting discrete logarithms or integer factorization processes, the private key of McEliece adopts the matrix generator of a binary Goppa code and exploits a dense change that happen by set of actions such as transformation and permutation matrix for disguising the private key into the public. the McEliece cryptosystem has main advantage that its encryption and decryption procedures are fast. it requires lower number of operations like RSA significantly. While its

disadvantages are two basically, low rate of encryption process and large size of key. The main reason of both is the binary Goppa codes that based on generally. Basically, the main model of McEliece cryptosystem is illustrated in figure1 below [8].

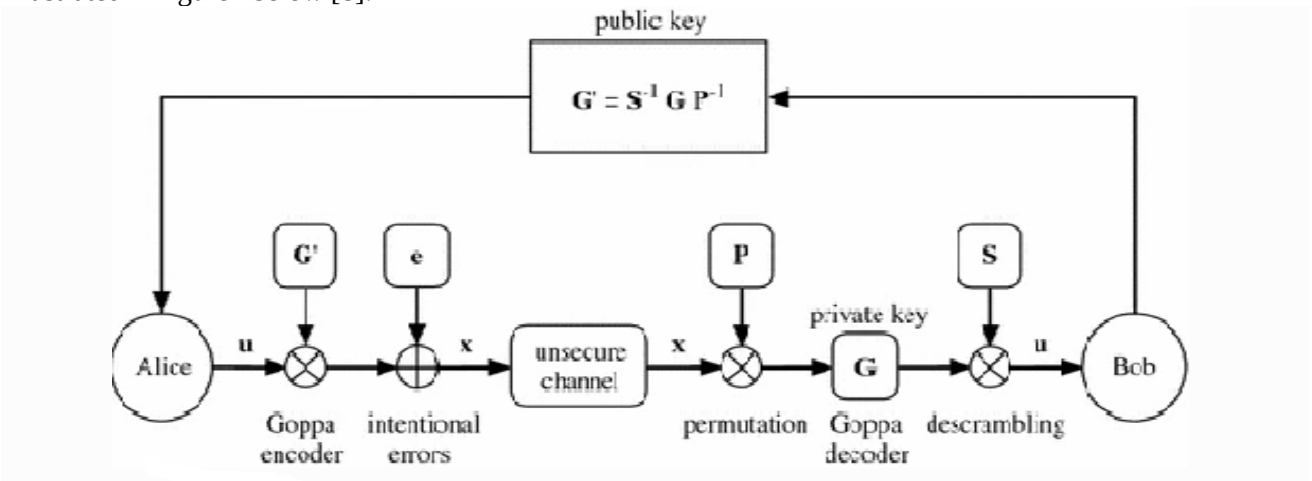

Figure 1. McEliece cryptosystem model

The private and public keys in McEliece Cryptosystem are generated according to following steps[9]:

1. k, n, and t are fixed integers that considered as parameters of system.
2. The steps 3 – 7 are performed by each entity A.
3. The G is generation and k *n is chosen. The linear code as binary (n, k) that correct errors denoted by ***t***, an efficient algorithm of decoding is known.
4. a random k*k is selected as non-singular matrix S.
5. P is permutation matrix and a random n* n is selected.
6. When G‘= SGP, the k*n matrix is computed.
7. (G ‘, t) are public and (S, G, P) are private.

In ciphering process, many actions must be done by the sender as illustrated in the following steps:

1. The (G‘, t) are obtained as authentic keys.
2. the message is represented by binary string m with length k.
3. 3. An error vector z that random binary is chosen with n length that at most *t* 1’s.
4. c = m*G’ + z is computed.
5. the cipher text c is sent to A.

While in deciphering process, to recover original information or plain text from cipher text according to following steps:

1. c‘= c*P^{-1} is compute and P^{-1} is an inverse of P matrix.
2. to decode c‘to m‘, the generated code by G is use decoding algorithm.
3. m = m ‘*S^{-1} is computed.

Paillier cryptosystem produces a new scheme of probabilistic encryption by calculating computations of Z∗ n2 group, where RSA modulus is denoted by n. it has features that more attractive. this process makes one execution with many bits with an expansion factor that considered as constant, an efficient decryption process is obtained [10].

with generation process, the public and secret keys are generated via applying many steps as shown in the following steps:

1. the pair p and q randomly chosen that large and
   that considered as independent for each to satisfy gcd (p*q,(p − 1)(q − 1)) = 1. (for both prime equivalent size).
2. $n = p\ q$ and h = lcm(e − 1, q − 1) are computed.
3. Select g as random integer that: $g_n \in Z^* 2$.
4. the *n* must divides *g* order by checking the existence of following modular multiplicative inverse: μ = (L(g^{λ}

$\bmod n^2))^{-1} \bmod n$, function L is defined: $L(u) = u^{-1}$.

5. The (n , g) are keys as public, while (λ , μ) are keys as private.

In ciphering process, the encryption is done via applying many steps by the sender as shown in the following steps:

1. m is a message that will encrypt if $N \in Z_n$
2. r is random and selected if $r \in Z^*_n$
3. obtaining cipher text: $c = g^m * r^n \bmod n^2$

While in deciphering process, to recover original information from cipher text according to following steps:

1. Cipher text $c \in Z^{*2}$
2. Compute message: $m = \overset{n}{L}(c^{\lambda} \bmod n^2) * \mu \bmod n$.

3. Related work

Using data structures with cipher methods to produce proposed cryptographic method is considered as newest method. This type of framework is beginning take place in papers of researchers. In [11], the multiple algorithms of encryption via cloud computing environment based on circular queue as data structure to increase security of ciphering process via adding complexity. In [12], there are many cipher algorithms that works together as hybrid manner used to encrypt information based on circular queue as data structure with control key to regulate the process avoiding redundancy.

4. Proposed method

The hybrid text such as English or Arabic or both if merge is encrypted by using different public key cryptosystem methods that works together with different manner. Using these cipher methods with circular link list data structure for scheduling them is strengthen the proposed cipher method. The obtained outputs of this proposed cipher method is more complexity than other cipher methods if applied separately. Using circular link list data structure for scheduling different public key cryptosystem methods prevents the frequency of cipher process. So, it prevents success guessing for original information. The proposed method consists of initialization stage, data structure creation stage, setting stage, pre-encryption stage, encryption stage, post-encryption, transmission stage, reception stage, pre-decryption and stage of decryption. The block diagram of proposed cipher technique is shown by figure 2. All these stages are explained with figures in this section.

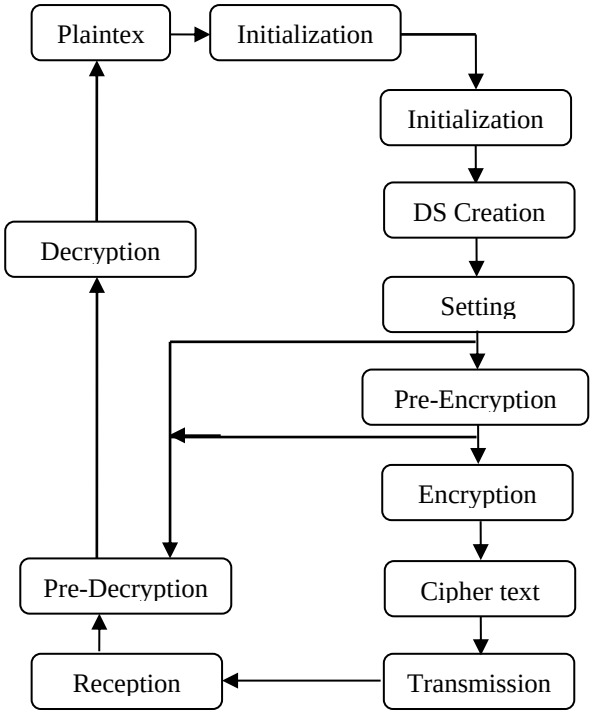

Figure 2. Block diagram of the proposed method

4.1 Initialization stage

Here, loading file of critical information or plaintext then determining nature or type of loaded information, which language is used for writing it (Arabic or English or both) and reformatting the loaded information according to cryptosystem methods used in this work based on type of input for cryptosystem methods used such as an integer or binary. The last process in this stage is preparing the loaded information by removing special characters and separators if they not required for encryption task.

4.2 DS creation stage

A circular link list as structure of data is created. The required size of created circular link list is five since the number of cipher methods that used in the proposed method is five as we seen above. the created circular link list includes five nodes and each node of them consists of two parts, the first part contains data detail and the second part contains pointing or addressing detail. So, it includes more than one pointer for moving between nodes of created circular link list. The first node is specified by using external pointer. The circular link list data structure is shown in figure 3.

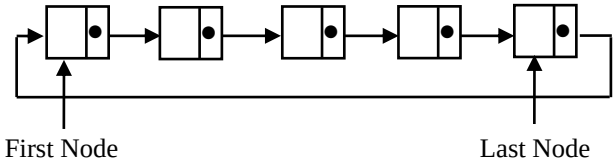

Figure 3. Circular link list data structure

4.3 Setting stage

In this stage, reading all nodes of the created circular link list with an integer value. The first node contains 11 value that refers to LU and LEE cipher method, the second node contains 22 value that refers to Rabin cipher method, The third node contains 33 value that refers to Okamoto-Uchiyama (OU) cipher method. The fourth node contains 44 value that refers to McEliece cipher method and the fifth node contains 55 value that refers to Paillier cipher method. All these cipher methods with its values are stored in setting file that shown in table 1 below:

Table 1. Setting file

No.	Abbreviation	Method ID	Method Name
1	LL	11	LU and LEE
2	RR	22	Rabin
3	OU	33	Okamoto-Uchiyama (OU)
4	ME	44	McEliece
5	PP	55	Paillier

4.4 Pre-encryption stage

In this stage, reading each information part of the created circular link list to specify which cipher method will used for encryption information based on setting file. The initialized sensitive information is loaded and reformatted according to specified cipher method by setting file. The last task in this stage is generating of keys related to specified cipher method by setting file. The initialized sensitive information, the specified cipher method by setting file will use and private and public keys are ready.

4.5 Encryption stage

Applying encryption algorithm requires loading and reading outputs of previous stage. The initialized sensitive information, the specified cipher method by setting file and encryption keys(private and public) will read then apply encryption algorithm and store result text in new file. The encryption algorithm is consist of many steps that shown in algorithm 1 below and figure 4 shows the procedures of encryption.

Algorithm 1: Process of encryption

Input: m_i, x_i.
Output: c_i.
Begin
Load initialized sensitive information as m_i file;
While m_i is not empty file
Reading m_i;
while m_i is not space or special character
Load and read setting file;
Read created circular link list based on setting file
Generate all required keys;
Apply specified ciphering style by created link list that is circular with m_i using x_i ;
C_i is saved as obtained result in new file;
END
END.

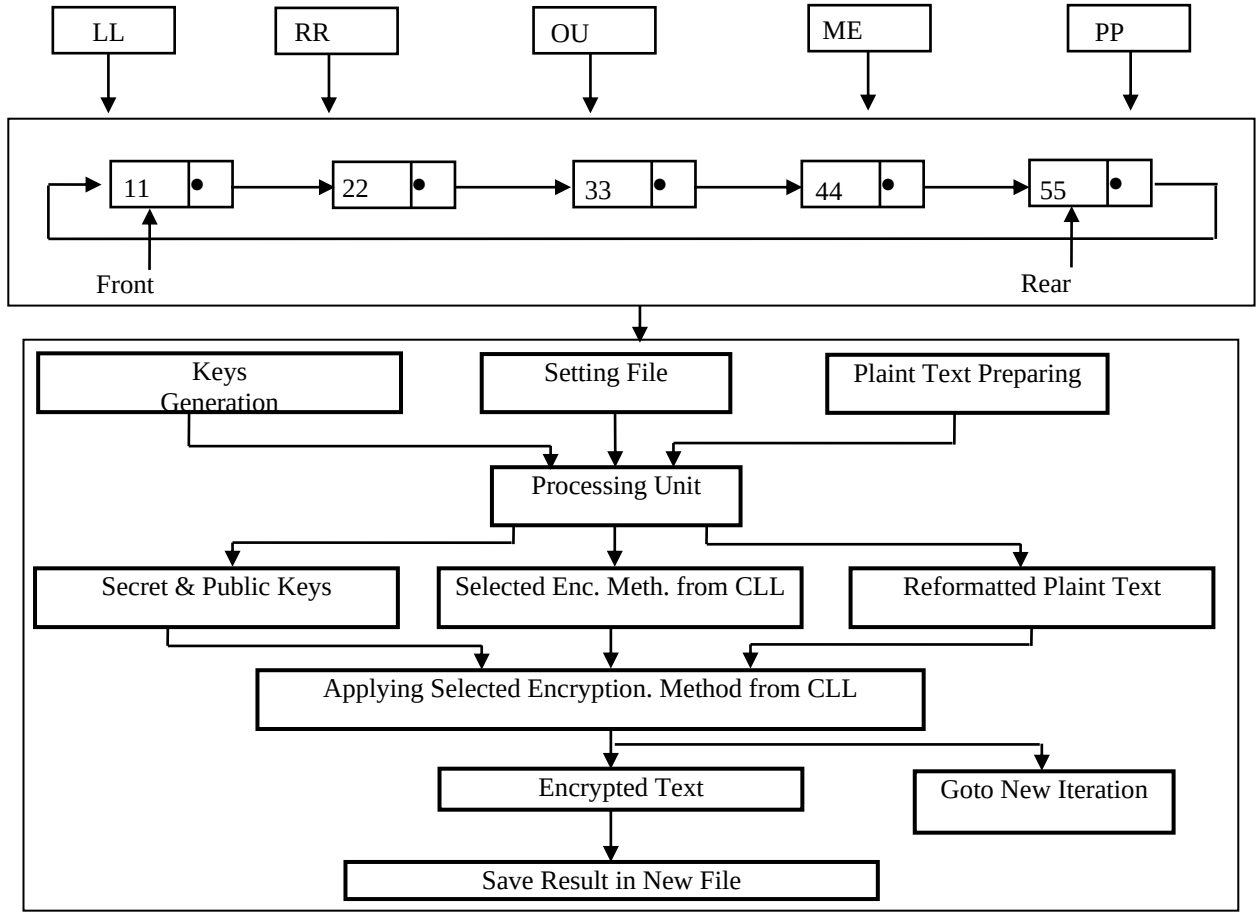

Figure 4. Procedures of encryption process

4.6 Transmission stage

The obtained encrypted information from encryption stage is transmitted via insecure communication channel to the receiver. The communication channel is based on internet. To send encrypted information, there are many applications and techniques that requires internet. The used communication channel must be considered many factors such as size of transmitted file and noises via transmission channel.

4.7 Reception stage

There are two main tasks of this stage, the first task is receiving transmitted information by receiver and storing it. The second task is preparing ciphered text for decryption process. The receiver sends acknowledgement to sender for ensuing receiving ciphered text that transmitted from him.

4.8 Pre-decryption stage

The receiver reads information parts for each node of created circular link list to know scheduling of cryptosystem algorithms. The setting file is loaded to achieve matching process between method id and method name to select it for decryption process. The last task in this stage is preparing keys used in decryption operation.

4.9 Decryption stage

Applying decryption algorithm requires loading and reading outputs of pre decryption stage. The prepared encrypted information, the specified decipher method according to setting file and decryption keys(private and public) will read then apply decryption algorithm and store original information as result text in new file. The decryption algorithm is consisting of many steps that shown in algorithm 2 and figure 5 shows decryption operation.

Algorithm 2: Process of Decryption.

As Input: c_i, x_i.
As Output: m_i
Begin
Loading transmitted information c_i file;
if c_i is not empty file
Reading c_i;
while c_i is not number or space then
Load and reading setting file;
Read created circular link list based on setting file
Generate all required keys;
Apply specified deciphering technique by created link list that circular with c_i by x_i;
p_i is saved as obtained result with newer file;
END
END.

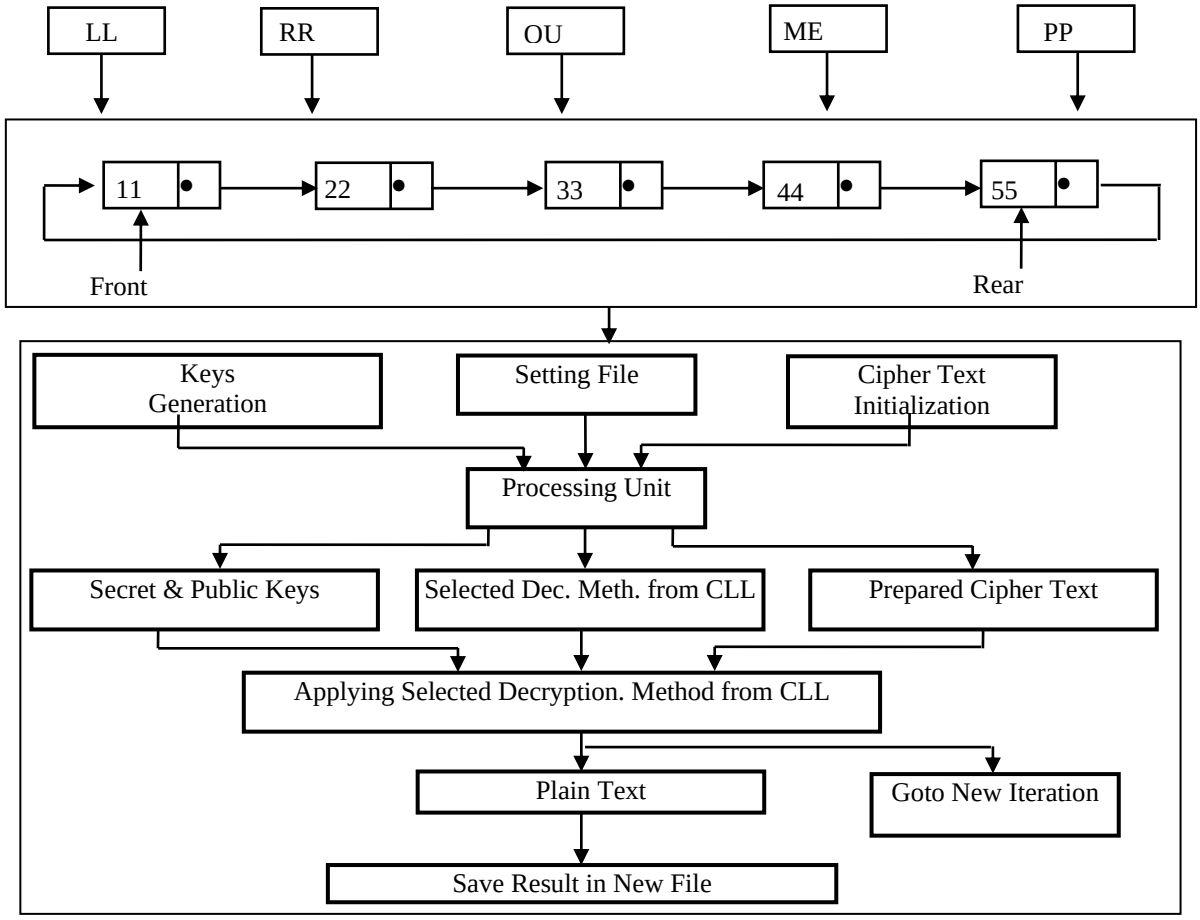

Figure 5. Process of decryption

5. Results

This section deals with practical implementation of the proposed cryptographic method. The type of language that used to write sensitive information is English. The space and special symbols built in plaintext are not ciphered generally. The execution time of used cryptosystem methods is calculated. Table 2 shows the comparison between them according to many factors that considered such as security, running time, efficiency and complexity. The cryptography technique used here is more effectiveness than different other ciphering styles which performed if they performed alone.

Table 2. Evaluation process

Seq.	Factors	Proposed Method	Others (LL, RR, OU, ME and PP)
1	Security	High	Low
2	Complex.	High	Low
3	Running Time	more or equal	Less or equal
4	Efficiency	More	Less
6	Robustness	strength	Weak against chosen cipher text attack

6. Conclusions

there are some conclusions that concluded by implementing a proposed hybrid text cryptography method that listed below:

1. Can encrypts any spaces or special characters with sensitive information.
2. The proposed method deals with different texts that written in English and Arabic languages.
3. Using circular link list increases levels of security and complexity for the proposed method.
4. Each character of sensitive information will cipher with different ciphering styles since scheduling it in circular link list.
5. The power of Paillier, Rabin and Okamoto-Uchiyama is integer factorization while McElice depends its security on bounded decoding and goppa code distinguishability.
6. When double link list is used, the obtained results are less efficiency than proposed method that uses circular link list.
7. The proposed method is more robust than other cipher methods against a chosen cipher text attack.
8. The execution time of the proposed method is equal the execution time of other cipher methods when implemented alone approximately.

References

[1] William S.,**"**Cryptography and Network Security Principles and Practices**"**, 2011.
[2] N. Sharma, Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326, 2017.
[3] Ravi Kumar Choubey, Ahtisham Hashmi, "Cryptographic Techniques in Information Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology IJSRCSEIT, Volume 3, Issue 1, pp. 854-859, 2018.
[4] Wisam A. Shukur, Khalid K. Jabbar, Luheb K.Qurban, " A Proposed Hybird Text Cryptographic Method Using Circular Queue", International Journal of Civil Engineering & Technology (IJCIET), Volume 9, Issue 7, pp. 1123–1132, July 2018.
[5] Haijian Zhou, Ping Luo, Daoshun Wang and Yiqi Dai, "cryptanalysis of general LU and LEE type systems", International Conference on Information Security and Cryptology, DOI: 10.1007/978-3-540-79499-8_32, 2007.
[6] Arpit Kumar Srivastava, Abhinav Mathur, " The Rabin Cryptosystem & analysis in measure of Chinese Reminder Theorem", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013.
[7] Loeky Haryanto, Armin Lawi, Suhastina Suhastina, Putri Qarynah,"On the Okamoto-Uchiyama cryptosystem", Journal of Physics: Conference Series, The 3rd International Conference On Science,2019.

[8] Fabšič T., Hromada V., Stankovski P., Zajac P., Guo Q., Johansson T., "A Reaction Attack on the QC-LDPC McEliece Cryptosystem", Post-Quantum Cryptography PQCrypto, vol.10346, Springer, doi.org/10.1007/978-3-319-59879-6_4, 2017.

[9] D. Engelbert, R. Overbeck and A. Schmidt , " A Summary of McEliece-Type Cryptosystems and their Security", Journal of Mathematical Cryptology Volume 1, Issue 2, 2007.

[10] Alia K. Abdul Hassan, " Reliable Implementation of Paillier Cryptosystem", Iraqi Journal Of Applied Physics IJAP, Vol. 10, No. 4, pp. 27-29, October-December 2014.

[11] Khalid K. Jabbar, Hussin A. Hilal, Rana S. Mohammed, "Text Cryptography Using Multible Encryption Algoritms Based On Circular Queue Via Cloud Computing Environment", Journal of Theoretical & Applied Information Technology, Volume 96, Issue 12, June 2018.

[12] Wisam A. Shukur, Khalid K. Jabbar, Luheb K. Qurban, " A Proposed Hybird Text Cryptographic Method Using Circular Queue", International Journal of Civil Engineering & Technology (IJCIET), Volume 9, Issue 7, pp. 1123–1132, July 2018.