JOURNAL OF MADENT ALELEM COLLEGE VOL 7 NO 2 YEAR 2015

Design and Implementation of A New Hybrid Encryption Algorithm

Ghada Salim Mohamed

Debt.Programing Eng

University Collage Of Madenat Al -Elem

gha_2090@yahoo.com

Abstract

Several approaches and techniques have been proposed to make communication via the Internet secure; one of these approaches is cryptography. In this paper the proposed algorithm based on merge of two encryption algorithms(public key algorithms), also used (XOR logic operation), (NOT logic operation) and permutation operation .The proposed hybrid algorithm consist of many level of cryptography so it has complexity with speed of implementation more than original algorithms.

Key words: Internet, cryptography, logic operation

تصميم وتنفيذ خوارزمية تشفير هجينة جديدة

غادة سالم محمد

كلية مدينة العلم الجامعة

الخلاصة

العديد من التقنيات والطرق اقترحت لجعل الاتصالات عبر الانترنت أمينة . واحدة من هذه الطرق هي التشفير. في هذا البحث تم اقتراح طريقة للتشفير تعتمد على دمج طريقتين من طرق التشفير باستخدام المفتاح المعلن بالإضافة إلى مستويات عديدة من التشفير تعتمد على استخدام (XOR Logic Operation, Not Logic Operation, Permutation Operation. بالتالي فان النظام المقترح يمتلك تعقيد مع سرعة في التنفيذ اكبر من الخوارزميات الأصلية.

1.Introduction

Computers are now found in every layer society, and information is being communicated and processed automatically on a large scale [1]. So that, daily communications of all kinds over the internet have become incredibly popular. Since the rise of the internet, one of the most important factors of information technology and communication has been the security of information. Thus many applications are Internet-based and in some cases, it is desired that the communication be made secret. In essence, the internet is an open channel and security problems such as interception, modification and others are very real.

Several approaches have been proposed to make communication via the internet secure [2]. One of these approaches is Cryptography, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key [3].

Cryptography is the science of writing in secret code [2] and is an ancient art of ensuring that messages (writing) are kept secure (hidden) from those recipients to whom the messages are not addressed [3].

2.Cryptographic Goals

Cryptography is also used to provide solutions for many problems such as:

1.Confidentiality (privacy).

2.Data integrity.

3.Authentication.

4. Non-repudiation.[4]

3.Types of Cryptography

There are several ways of classifying cryptographic algorithms. There are, in general, two types of cryptographic schemes:

a) **Secret Key Cryptography (SKC).**

b) **Public Key Cryptography (PKC).**

3.1 .Secret Key Cryptography (SKC)

It uses a single key for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption [2].

3.2 .Public Key Cryptography (PKC)

Public-key cryptography is considered the most significant new development in cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975. Generic Public-key cryptography (PKC) employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key [4]. One of the keys (public key) is used to encrypt the plaintext and may be advertised as widely as the owner wants. The other key (private key) is used to decrypt the cipher text and is never revealed to another party. The sender encrypts some information using the receiver public key; the receiver decrypts the cipher text using his private key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information [5].

4. Public-Key cryptography algorithms

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include: RSA, Rabin, ElGamal, Paillier, Elliptic Curve Cryptography (ECC),Cramer-Shoup and many other public key cryptography algorithms [5].

4.1 .Rivest, Shamir and Adleman(RSA) Public Key Cryptography

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization any other public key cryptography algorithms [5].

4.1.1. RSA keys generation.[3]

The first step in RSA encryption is to generate a key pair. Two keys are generated of which one is used as the public key and the other is used as the private key. The keys are generated with the help of two large prime

numbers. The keys are generated as follows:

Algorithm (1):RSA Initialization.

Input: Two large prime numbers(p,q)

Output: A public keys (n, e), and a private keys (n,d).

1. **Begin.**
2. Generate two large random primes**p** and **q**.
3. Compute n which is equal to product of those two prime numbers,

n= p.q

4. Compute **φ(n) = (p-1)(q-1).**
5. Choose an integer **e, 1 < e <φ(n),** such that **gcd(e, φ(n)) = 1**.
6. Compute the secret exponent **d, 1 < d <φ(n),** such that

e.d ≡ 1 (mod φ(n)).

7. The public key is (n, e) and the private key is (n, d). The values of p,

q, and φ(n) should also be kept secret.

8.End.

- **n** is known as the modulus.
- **e** is known as the public exponent or encryption exponent.
- **d** is known as the secret exponent or decryption exponent.

4.1.2 . RSAEncryption

Encryption is done using the public key component e and the modulus n.

To whomever we need to send the message, we encrypt the messagewith their public key **(e, n).**Encryption is done by taking an exponentiation of the message m withthe public key e and then taking a modulus of it.

Algorithm (2):RSAEncryption

Input: The plaintext to encrypt, the public key (n, e).

Output: The encrypted cipher text.

1. **Begin.**
2. Obtain the recipient's public key**(n,e)**
3. Represent the plaintext message as a positive integer **m < n**
4. Compute the cipher text **c = m^e mod n**.
5. Send the cipher text c to the recipient.
6. **End.**

4.1.3 RSADecryption

Decryption is done using the Private key. The person who is receiving the encrypted message uses his own private key to decrypt the message. Decryption is similar to the encryption except that the keys used are different.

Algorithm (3): (RSA Decryption)

Input: The received encrypted cipher text and the private key.

Output: The original plaintext.

1. **Begin.**
2. Recipient uses his private key **(n, d)** to compute $\mathbf{m = c^{d} \bmod n}$.
3. Extract the plaintext from the integer representative **m**.
4. **End.**

- The RSA algorithm has been implemented in many applications and it is currently one of the most popularly used encryption algorithm [3].

4.2 .Paillier Public Key Cryptography

The Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography, invented by Pascal Paillier in 1999 [6].This probabilistic scheme has generated a good amount of interest, the main interest seems to be centered around the homomorphic property allows this scheme to do simple addition operations on several encrypted values and obtain the encrypted sum. The encrypted sum can later be decrypted without ever knowing the values that made up the sum**.**

The problem of computing n-the residue classes is believed to be computationally difficult. This is known as the Composite Residuosity (CR) assumption upon which this cryptosystem is based , Because of this useful characteristic, the scheme has been suggested for use in the design of voting protocols, threshold cryptosystems, watermarking, secret sharing schemes, private information retrieval, and server-aided polynomial evaluation[7].

4.2.1 .Algorithm (1): Paillier Initialization[6].

Input: Two large prime numbers(**p,q**)

Output: A public keys (**n, g**), and a private keys (**p, q, μ, λ**).

1. **Begin**
2. Select two large prime numbers, p and q about the same size.

3.Compute the modulus n the product of two primes **n =(p*q)** and**λ = LCM (p - 1, q - 1)** (**λ** is Carmichael's function)

(**LCM** is a Least Common Multiplicative)

4. Select random integer**g** where **g** ∈ $Z^*_{n^2}$where g's order being a non zero multiple of n (Since **g = (1 + n)** works and is easily calculated, this is the best choice). This can done efficiently by checking **gcd (L (g mod n^2),n)**=1

5.Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: **μ=L (g∈mod n^2) $^{-1}$mod n** where **function L** is defined as **(Lagrange function) L(u)=u-1\ n for u =1 mod n**

6.Publish the public key **(n, g)** and keep the private key (**p,q, μ, λ**)secret **7.End.**

4.2.2 .Algorithm (2) :(Paillier Encryption)[6].

Input: The plaintext to encrypt, the public key (**n,g**).

Output: The encrypted cipher text.

1. **Begin**
2. Plaintext is m where **m < n**.
3. Find a random r**, r∈ Z^*_n**
4. Compute cipher text **c = g^m .r^n mod n^2.**
5. **End**

4.2.3 .Algorithm (3): (Paillier Decryption) [7]

Input: The received encrypted cipher text and the private key.

Output: The original plaintext.

- **Begin**
- The cipher text **c < n^2**.
- Calculate**α**, where **α.n≡ 1 mod∅(*n*).**
- Retrieve plaintext by compute **m = L(c · r^{-n} mod n^2).**
- **End**

4.2.4 .Paillier Implementation Requirements

There are some of algorithms and definitions [8,9] are used in execution of the Paillier cryptography method that are shown below:

1. Algorithms of (the greatest command divisor (gcd(a,b))):

this algorithm take **a** and **n** positive integer, not equal zero and give as output the largest divisor d such that **d | a** and **d | b**

2. Algorithms of (Inverse (a, n)):

This algorithm take **a** and **n** integer number, and return x such that:

a.xmod **n** =1, where **0 < a < n**.

3. Algorithms of (Fast modular exponentiation):

this algorithm take **x, e** and **n** integer number, and compute the modular exponentiation : $\mathbf{c= x^{e}}$**.**

4. Calculate the modulus (that take **b** and **n** positive integer, not equal zero and give **a** as congruent of **b** modulo **n** where(**b, n, a**) are integer numbers where **0 < a < n.**

5. Other ways that used to increase the performance:

a) Precompute the value $\mathbf{r^n}$ only once in initialization for each message passed.

b) Set **g = (1 + n).** This is the simplest value and there seems to be no benefit of calculating something more complicated.

c) Precompute $\mathbf{n^2}$**,** which is necessary in computing modules $\mathbf{n^2}$**.**

5.Proposed Hybrid-Encryption System

Action Steps of the proposed system could be clarified as follows:

5 .1 The proposed algorithm encryption process

Input: Plain text, Keys.

Output: The cipher text(String of binary bits).

1. **Begin.**
2. Divided the plain text (PT) into blocks (bi) each one consist of 8 characters, process one block each time.
3. Convert the characters of block to decimal form by using ASCII code .

4. Encryption the decimal number by using **The Proposed Hybrid Public Key Method(Algorithm(A),(Algorithm(B)).**
5. Divide the result cipher number by 256 , store the result of division in D1,and store the remainder of division in D2
6. Convert D1 to string of bits(S1),Convert D2 to string of bits(S2).
   (we can use **n** instead of 256 ,the difference will be in number of bits that used to represent result cipher number form ,**The length of binary string of bits=2* Number of bits used to represent n in binary form**)
7. Perform (S1 XOR S2)that give S3
8. Concatenate S1 and S3 in one string (S4)
9. Perform NOT (S4) that give string (S5).
10. Reverse the order of bits of S5
11. Perform ((new S5) XOR (String of bits S6(S6=the secret key **d** in binary form)).
12. Store the bits of string into 2D array (4X4) and Permutation the elements of the array depend on specific 2D array (4x4) that shown in **Figure(2).**
13. Convert the permuted array element into one string of 16 bits.
14. Perform the same above steps on the next character until all the character of block are complete, then take the next block and process it in the same manner until all the blocks of plain text are process .
15. **End**

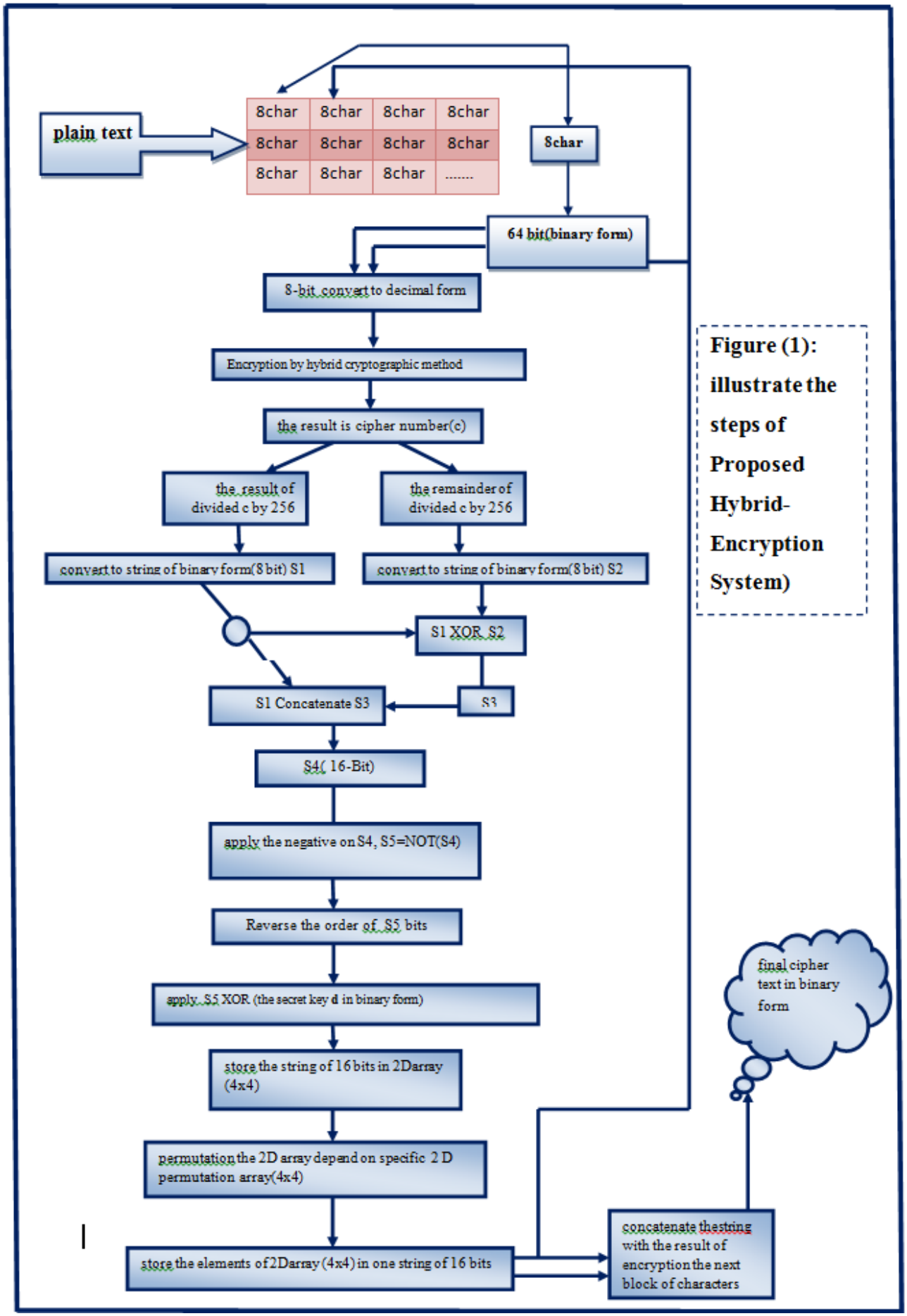

Figure (1): illustrate the steps of Proposed Hybrid-Encryption System)

1) Algorithm(A):Proposed Hybrid Public Key Method (Paillier and RSA)Initialization

In **The proposed hybrid public key method** the first step is to generatea keys, The keys are generated as follows:

1. **Begin**
2. Select two large prime numbers, p and q about the same size.
3. Compute the following :
   1) the modulus n the product of two primes **n =(p*q)**
   2) **λ = LCM (p - 1, q - 1)** (λ is Carmichael's function).
   3) Compute **φ(n) = (p-1)(q-1).**
   4) Select random integer **g** where **g** ∈ $Z^*_{n^2}$where g's order being a non zero multiple of n This can done efficiently by checking **gcd (L (g mod n2),n)**=1
   5) Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: **μ=L (g∈mod n^2) $^{-1}$mod nL(u)=u-1\ n for u =1 mod n(Lagrange function)**
   6) Choose an integerβ**, 1 <**β**<φ(n),** such that **gcd(**β**, φ(n)) = 1**.
   7) Compute the secret exponent **d, 1 < d <φ(n),** such that **β.d ≡ 1 (mod φ(n)).**

4.Publish the public key, (n, g,), and keep the private key(**μ,d,** λ) secret .

5. End.

Algorithm(B):The Proposed Hybrid Method (Paillier and RSA) Encryption

- **Input:** Plain text, Keys.
- **Output:** The cipher text(decimal numbers).
- **Begin**
- The cipher text **C< n^2**.
- Calculate γ, Where γ=**m** $^{\beta}$ mod n.
- Compute **the**cipher text **=g**$^{\gamma}$ · **β**^{n} **mod n^2.**
- Where **C**=**g**$^{m^{\beta} \bmod n}$ ·**β**$^{(p.q)}$ **mod** n^2
- **End**

Algorithm(C):The Proposed Hybrid Method (Paillier And RSA) Decryption

Input: The received encrypted cipher text , private keys**.**

Output: The original plaintext.

- **begin**
- Let C be the cipher text to decrypt, where **C**∈ $Z^*_{n^2}$

- Compute the plaintext message as: M = $\frac{L(C^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$

  or by substitution the value of **($\mu = L(g \in \bmod n^2)^{-1} \bmod n$)** the plaintext message can compute as follow :$M = L(C^{\lambda} \bmod n^2).\mu \bmod n$

- **End**

2)2D Permutation Array (PA)

The specific 2D array (4x4)used to permutation the elements of the array

(3,3)	**(2 , 2)**	**(0 , 0)**	**(1 ,1)**
(1 ,2)	**(0 , 1)**	**(3 , 1)**	**(2 , 1)**
(2 , 4)	**(3, 2)**	**(1, 3)**	**(0 , 2)**
(0 , 3)	**(1 , 0)**	**(3, 0)**	**(2 , 0)**

Figure(2): 2D array permutation (4x4)

(0 , 0)	**(0 ,1)**	**(0 , 2)**	**(0 ,3)**
(1 , 0)	**(1 ,1)**	**(1 ,2)**	**(1, 3)**
(2,0)	**(2 , 1)**	**(2 ,2)**	**(2 ,3)**
(3 ,0)	**(3 , 1)**	**(3,2)**	**(3 ,3)**

Figure(3): 2D array permutation inverse (4x4)

5.2 .The proposed algorithm fordecryption process (Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

Input: String of bit represent cipher text in binary form , keys.

Output: M as string of characters

1. **Begin**
2. Divided the input string into blocks each one with 128 bits and process on block (bi)each time .
3. Divided the block (bi) into 8- sub block (bij) each block is 16 bits(j=1-8)
   (i=length of cipher string of bits /128)
4. Store the string of bits of block (bij) into 2Darray (4x4), and Perform inverse permutation (inverse permutation of array can perform by retrieve the original order to the elements of array as shown in **Figure(3)**).

5. Convert the 2Dpermutedarray elements into one string with length 16 bits (S5).
6. Perform ((S5 XORS6) (where S6=the secret key **d** in binary form)).
7. Reverse the order of bits of new S5.
8. Perform NOT (S5) that give string (S4)
9. Divided the s4 into 2 string (1-8 bits store in S1)and (9-16 bits store in S3)
10. perform (S1 XOR X3) that give S2
11. Convert S1 to decimal number D1, convert S2 to decimal number D2
12. Using D1,D2 to retrieve the cipher number (C)
13. Decryption the (**C**) by using**The Proposed hybrid public key method(Algorithm(A),(Algorithm(C)).**
14. Convert the result number to character
15. Perform the above steps on the next 16-bits (bij) until complete all sub block, then process he next block of cipher text

End. (Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

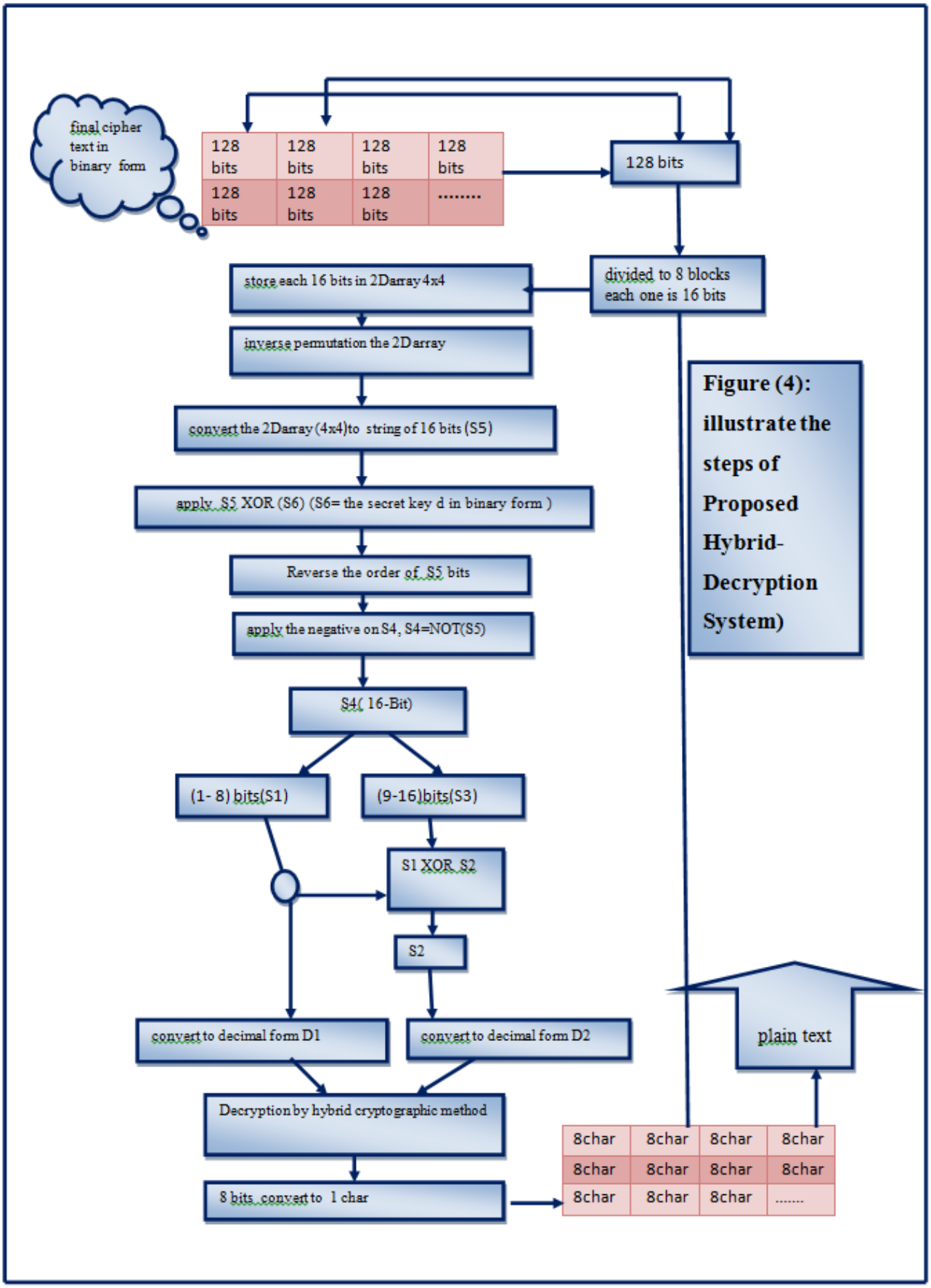

Figure (4): illustrate the steps of Proposed Hybrid-Decryption System)

6. The Results Of The Proposed Encryption Algorithm.

The proposed methods was implemented through Visual Basic.NET 2008 programming language on laptop (Intel(R)core(TM)i7-4500U CPU@1.80 2.40 GH_Z and RAM 6.00 GB)by Using a message with different size , To ensure the efficiency of the proposed methods, a various size of plaintext is assumed such as (7KB, 9KB, 10 KB, 11KB and 15MB). The following results represent the execution time (in second) of the both encryption and decryption operations for the proposed methods as show in table (1).

Table (1)Total Time Of The Proposed Method (In Sec.)

Message size	Operation	Proposed Method
7K	Encryption Decryption	Less than 1sec. Less than 1sec.
9K	Encryption Decryption	1 sec. 1 sec.
10K	Encryption Decryption	1sec. 1sec.
11K	Encryption Decryption	2 sec. 2sec.
15K	Encryption Decryption	3 sec. 3 sec.

- The minimum size of numbers that used in execution of program is n=8 bits , n^2= 16 bits , p =8bits, β=8bits

7. Conclusions

Several conclusions are reached through the working the system steps. The following items represent the important conclusions which are drawn from the proposed system:

1. The experimental results show that the complexity and the execution time of the public-key cryptosystems are trade-off problem, this means when the complexity degree increases the run time increases also but in little amount.

2. the security of the proposed hybrid system it based on (1- composite degree residues,2- factoring large numbers, 3- randomness)that will increase the complexity of proposed system analyzing and make it strong more than the original method and that proves by :

(A) the security Paillier cryptosystem algorithm based on the use of composite degree residues. and it provably secure under adequate intractability assumptions (it provide semantic security against chosen-plaintext attacks).

(B) The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers and the RSA problem

As it know, there are several algorithms used to solve the factorization problem (hard)such as NFS (Number Field Sieve), but when the used number be complex as much as it possible these type of algorithms become inefficient to work, therefore the proposed methods depend on this idea.)

(C) The using of (logic operations (NOT,XOR)will increase some of randomness on the cipher message because the statues of bits will change ,also the permutation operation change the locations of bits in cipher string)

References

1. Stallings W. (1999) Cryptography and Network Security, Principle and Practice ", Addison Wesley.
2. **Gary c.** Kessler. (2007) An Overview of Cryptography URL:http://www.garykessder.net/library/crypto.html.
3. RSA cryptosystem - Wikipedia, the free encyclopedia **URL:http://www.**en.wikipedia.org/wiki/**RSA_cryptosystem**, 2015.
4. **Van Oorschot** M. P., Vanstone S. (1996) Handbook of applied cryptography, CRC Press, 1996.
5. **Adler M.,** Gailly J. (2004) **An Introduction to Cryptography**", PGP Corporation.
6. Paillier. (2015) cryptosystem - Wikipedia, the free encyclopedia **URL:http://www.**en.wikipedia.org/wiki/**Paillier_cryptosystem**.
7. Kert Richardson. (2006) Progress on Probabilistic Encryption Schemes. M.Sc thesis ,the Faculty of the Computer Science Department of the Rochester Institute of Technology.
8. Song.Y. Yan. (2002) Number theory for computing, Springer-Verlag, 2002.
9. Dorothy Elizabeth Rob, ling Denning,"Cryptography and data Security", Purdue University Vav Addison-Wesley Publishing Company Reading, 1982.16.