A Highly Secure Secret Key Encryption Methodology Using Dual Permutation

Ratul Chowdhury¹, Samir Ghosh¹, Anirban Das², Prof. Samir Kumar Bandyopadhyay³

Assistant Professor, Department of Computer Science and Engineering, Future Institute of Engineering and Management, Kolkata, India¹
UG student, Jogesh Chandra Chowdhuri College, Kolkata, India²
Professor Department of Computer Science and Engineering, University of Calcutta, Kolkata, India³

Accepted 2017-07-15; Published 2017-07-26

Abstract:
This paper describes a novel secret key cryptography algorithm where a dual encryption methodology has been incorporated. The first level is a block level encryption, where the original text message is divided into several fixed size blocks. An initial permutation has been applied on that n number of block sets and by using a secret key, a particular sequence of blockshas been chosen. The second level is a bit level encryption, where the same permutation has been applied within each block and a particular bit sequence within a block has been chosen. XOR and bit shifting are some intermediate operation has been applied for security purpose. A secret key is being prepared by storing the block level as well as the bit level random values. The block size of this proposed method is 16bits. The main key advantage of the proposed method is that by using this bit level and block level encryption the security is increased of the algorithm in a higher semantic level.

Keyword: Block level Permutation, XOR operation; bit shifting, Bit level permutation, Secret key.

Introduction:
Information security has become the main key concern for communication over public network. Cryptography and steganography are two pillars of information security [1]. Cryptography is the art of storing and transmitting data in a particular form so that only those for whom it is intended can understand and process it. In steganography, the messages are hidden within a media in such a way that none can understand the very existence of the message i.e. it cannot be perceived by human. The media can be audio, video or image[2]. Due to the upsurge in the demand for secure transactions over the network, constant evaluation and continuous research into the field of information Security particularly in the fields of cryptography is vital. Cryptographic algorithm is broadly classified into two types, symmetric key cryptography and asymmetric key cryptography [3]. Symmetric algorithms are secret key algorithm that uses the same key for encryption and decryption purpose or whose encryption and...
decryption keys can be generated from each other. Symmetric key algorithms therefore require that the key should be kept secret. Asymmetric key algorithm also called public key algorithm uses different keys for encryption and decryption purpose. In this scheme the sender and the receiver of the message, each have their own private key that works with the public key shared between them. Some popular symmetric and asymmetric key cryptography algorithms are given in [4-5].

Cryptography algorithm is proposed with dual encryption concept.

**Review Works:**

The Data Encryption Standard (DES) is popular encryption technique. The DES is block cipher technique in which it uses the same secret key for encryption and decryption purpose. The Block size and Key size of DES is 64-bits and 56-bits respectively. It consists of 16 identical stages, Initial Permutation (IP) and Final Permutation (FP) [3]. The DES consists of following steps:

1. In the first stage a 64-bit plaintext is given as input to the IP and IP is performed on plaintext and to obtain the Permuted Input it rearranges the bits.
2. The second step includes of 16-rounds of the same function, and it consists of permutation and substitution methods.
3. The output contains 64-bits and it is a function of input plaintext and key.
4. By swapping the output of left and right side, the pre-output is produced.
5. Finally the pre-output is gone through FP i.e. opposite of IP to create 64-bit cipher text.

Second popular symmetric key algorithm is AES. The AES stands for Advanced Encryption Standard and it is based on design method called as a substitution permutation network. The AES-128, AES-192, and AES-256 block ciphers are included in it. Every cipher encodes and decodes information in the block of 128-bits, using cryptographic keys of 128-bits, 192-bits, and 256-bits respectively. For 10 rounds, 12 rounds and 14 rounds 128-bits, 192-bits and 256-bits keys are used respectively [3-4].

The AES Encryption, Decryption process has following 4-stages:

1. Substitute byte: To carry out a byte-by-byte substitution of the block it uses an S-box.
3. Mix column: A substitution that makes use of arithmetic over GF(28).
4. Add round key: A simple bitwise XOR of the current block with a portion of expanded key.

Both of these DES and AES algorithms has fixed length plain text and key size respectively.

The third method is Blowfish [13]. It is also a symmetric key cryptography technique. Its block size is 64-bit, but the key length is variable. Its variable key size ranges from 32-bits to 448-bits. It is one of the fastest techniques which have developed up to date. This algorithm is simple and placed in the public domain due to which it can be used freely by anyone. Blowfish algorithm contains two parts Key Expansion and Data Encryption. The key of the Blowfish algorithm is 448 bits, so it requires 2448 mixes to look at all keys. Finally by using this secret key the cipher text has been prepared.

The forth method is RSA algorithm [14]. It is an asymmetric key cryptography algorithm. This algorithm uses two keys (public and private), first to encrypt second to decrypt. The public key used for encryption of messages and decrypted by using the private key. The following steps are performed to obtain the keys for RSA algorithm:

1. Select two large prime numbers p and q.
2. Calculate n=p*q; where n is modulus for both keys.
3. Select e (public key) such that it is not a factor of (p-1) (q-1).
4. Calculate d (private key) such that: d*e mod (p-1) (q-1) =1.
5. For encryption, calculate the ciphertext C from plaintext M as C= Me mod n.
6. For decryption, calculate the plaintext M from the ciphertext C as M= Cd mod n.

Modern mathematical cryptography draws on many areas of mathematics, including especially number theory, abstract algebra (groups, rings, and fields), probability, permutation and...
Concepts from different aspects are now a day’s incorporate with cryptography for security purpose. Some researchers proposed encoding and decoding a message in the implementation of Elliptic Curve Cryptography [6]. It is a public key cryptography using Koblitz’s method. In their work, each character in a message is encoded by its ASCII code then the ASCII value is encoded to a point on the curve. Each point is encrypted to two cipher text points[6].

Quantum Cryptography is a technology ensuring secured communication that is used as a means of data transaction among network systems. Other researchers proposed a three-way key conveyance convention based on Quantum Key Distribution. They created a new three way model where a reliable outsider is used to secure the correspondence channel using an unknown discreet key[7].

Neural network and cryptography together can be used for strong network security. The Neural network forms the key for encryption and decryption. The key is in the form of weights of neural network which is difficult to break[8]. Some researchers proposed a multilayer quantum neural network used by back propagation algorithm to construct a cryptography system[9].

DNA cryptography is a branch of cryptography derived from DNA computing and based on difficult biological processes. With the emergence of DNA computing a promising field of cryptography came into picture, called DNA Cryptography. Large information storage and massive parallelism properties of DNA molecules encourages its use for cryptographic purpose. [10].

Visual cryptography on the other hand is an image encryption technique, which hides the image based secret. The main advantage of visual cryptography is that it does not require any complex computation for decryption of secret it basically performed by human visual system. In another proposed method, where they extracted R,G and B component from a color image, and by applying a gray share generation algorithm on R components they have created n number of Rshares and finally they combined B, G and R components to make color shares [11].

The proposed method in this paper a symmetric key cryptography algorithm. AES and DES methods has two serious shortcomings, the size of the plain text and cipher text has fixed so there is no flexibility and secondly the computation time is very high. This method consists of 4 stages, Block level permutation, Character shifting, XOR operation and Bit level permutation. Each level of the algorithm is dependent on the secret key and has its own complexity level. The main advantages of this method are that the plain text size and key size is not fixed and the estimated time is less than other method.

**Proposed Method:**

The proposed method is a symmetric key algorithm, that is, the same key is used for both encryption and decryption purpose. The key idea behind this algorithm is based on the permutation function. From any random sequence, the proposed algorithm can find the original sequence and vice versa. The general structure of the proposed algorithm is shown in figure 1.

![Figure 1: Detailed encryption process](Image)

Next part is to describe the block level division of the plain text by space elimination. Suppose the plain text message is divided into number of
blocks say n. Each block consist of 16 characters. An initial block level permutationalgorithm get_position is applied into n number of blocks and according to the value of the secret key a particular sequence from n! Combinations is chosen for next level shown in figure 2. The first level encryption has been performed by using this initial permutation function.

**Figure 2: Block level permutations**

**Algorithm gets position:**
Input: An initial sequence per_start and a sequence number per_no.
Output: Permuted sequence.
Data structure: An array pos[L…U] where L and U are the lower and upper bounds of array index.
Steps:
1. Find the length of the initial sequence in variable length.
2. i:=0
3. while ( i<=length-1) do
4. rem=per_no mod factorial(length-1-i)
5. per_no=per_no/factorial(length-1-i)
6. If(per_no≠0 and rem=0)then
7. pos[i]=length-1-i
8. else
9. pos[i]=per_no
10. EndIf
11. per_no=rem
12. i=i+1
13. EndWhile
14. Print pos
15. Stop
Function factorial(Str_len)
1. If (Str_len=0 or Str_len=1)
2. Return 1
3. Else
4. Return (Str_len * factorial (Str_len-1))
5. EndIf
6. End Fuction

The procedure for secret key generation is now described. A random number generator function produces a random number that varies minimum 6 bits to maximum n!. After permutation if the number of block sequence is less than 6 bits, then a mapping has been done to find the sequence number within that range. This random number is the secret key for this proposed algorithm. Each step of the algorithm is dependent upon the secret key.

Now exact block level encryption has been performed. The first operation is bit shifting. The bit shifting has been performed according to the bit value of the key. Let us assume the key value is ‘541329’ and consecutive 6 characters of a 16 bit block are ‘D,B,A,C,H,E’.

According to this method, D,B,A,C,H,E will be shifted 5,4,1,3,2, and 9 times and the new character sequences will be I,F,B,F,J,N. After completing one round, the same key value has been used in a circular basis for the rest of the character within a block. The character shifting has been described in figure 3.

**Figure 3: Character shifting**

To perform the EXOR operation, each character within a block is further divided into subblocks, which consists of the corresponding 8 bits binary equivalent of that character. According to the value of the key, the XOR operation has been applied in each sub block and finally reconverts the binary equivalent into character. Let us assume the secret key is ‘541329’. For the first 16 sub blocks, the value of the 5th sub block remains unchanged. Nowby using the value of the
5th sub block, the XOR operation for the rest of the block will be executed. For the next 16 sub blocks according to the value of the key, unchanging the 4th sub block, the EXOR operation will be performed with the value of the 4th sub block. After performing the EXOR operation the corresponding binary equivalent is reconverted into character. The same procedure will be repeated for the rest n number of blocks in a circular basis.

In the last phase of the encryption process, the final bit level encryption has been performed. We have applied the same permutation algorithm get_position in each block and by using the secret key, a particular sequence from 16! Combinations are chosen. For block 1, the LCM of the first 4 character of the secret key is to be calculated. According to the value of the LCM, a particular sequence is chosen form 16! Combinations. For block 2, the whole system is shifted one step forward i.e we have to perform the LCM of the consecutive four characters excluding the first character. The same procedure has been performed for the rest number of blocks. If the digits of the key get finished, the system will continue in a cyclic order.

In receiving side the same algorithm has been used in reverse order. The actual block diagram for decryption is shown in figure 4.

As soon as the cipher text is accepted by the receiver, the block level division is performed and each block is transferred to get position algorithm. The input of the reverse permute function is the permuted sequence and the sequence number. For block number 1, the sequence number has been derived by computing the LCM of the first four digits of the key. The output of the get_position is the actual sequence. For block number 2, the sequence number is the LCM of the next four character of the key. The same procedure has been performed for the rest of the blocks in a cyclic order.

In this phase, the XOR operation and bit shifting in each 16 character block has been applied. To perform the XOR operation, each character within a block is further divided into its 8 bit binary equivalent. Now the XOR operation has been applied to each 16 sub blocks. Let us assume the secret key is ‘541329’. Now for the first 16 sub block, according to the first digit of the key, the 5th sub block is unchanged. An EXOR operation has been applied to the rest of 15 sub blocks with 5th sub block and we will reconvert each sub block into character. The same procedure has been applied for the rest n-1 blocks.

In the next phase, a left bit shifting operation has been performed in each block. According to the value of the key, each character will be shifted to its left. Let us assume the key value is ‘541329’ and the character sequence is ‘I, F, B, F, J, N’. According to the value of the key, the character will be shifted left 5, 4, 1, 3, 2 and 9 times respectively and character sequence becomes ‘D, B, A, C, H, E.’ After completing one round, the same key value has been used in a circular basis for the rest of the character within a block.

In this phase the same get_position algorithm has been applied in block level. Here the input of the algorithm is the encrypted block sequence and the sequence number which is the secret key. The corresponding output of the algorithm is the actual block sequence and by merging each 16 character block, the actual plain text is obtained.

Figure 4: Detailed decryption process
Result analysis:
In the first phase, the security provided by each level has been discussed and in the next phase, a comparison has been done with some existing algorithm. The main key advantages of this algorithm are as follows:

1. It is a lossless encryption algorithm i.e in the decryption end, the same plain text has been received without any loss.
2. The size of the plain text is same after encryption.
3. The plain text can carry any number of characters without any restriction.
4. The security of the proposed algorithm will increase gradually with the increase of the size of the plain text.
5. The time taken by the proposed algorithm is much less as compared to other algorithm.

Each level of the algorithm provides a specific way of security. The first level is block level permutation. If the plain text contains n number of blocks, then to find the original sequence from an arbitrary sequence, it requires to check n! different possible combinations. The second level is bit shifting. Each bit within a block has been circularly shifted according to the value of the key. The value of a particular digit within a key can vary from 0-9. So, each character within a block has a possibility to shift 0 to 9 times. The third level is XOR operation. To perform this step, each block is further divided into 16 different sub blocks where each sub block contains 8 bit binary equivalent of a character in the original block. According to the value of the key, one sub block has been fixed and an XOR operation has been performed with the rest of the sub blocks. So, each sub block has a possibility to perform a XOR operation with the rest of the 15 sub blocks. For 16 sub blocks each has 15 possibilities so there is total 16*15=240 possibility of each block. Finally a bit level permutation has been performed. Since each block contains 16 characters, so there are 16! possible combinations. If there are n number of blocks, then to find the original sequence, the intruder has to check n*16! Possible Combinations. Finally a comparison has been done with traditional RSA algorithm from table 1 we conclude that to encrypt 160 and 320 characters proposed method requires less time as compared to RSA algorithm. It is graphically depicted in figure 5. The conversion from plain text to cipher text for 80 characters is shown in table 2.

<table>
<thead>
<tr>
<th>Time(sec)</th>
<th>160 Character</th>
<th>320 Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our Method</td>
<td>0.012 sec</td>
<td>0.024 sec</td>
</tr>
<tr>
<td>RSA</td>
<td>1.155 sec</td>
<td>2.287 sec</td>
</tr>
</tbody>
</table>

Table 1: Computational time comparison with RSA algorithm

![Time Chart](image)

Figure 5: Graphical comparison with RSA algorithm

<table>
<thead>
<tr>
<th>Number of Character</th>
<th>Original Text</th>
<th>Cipher Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>This is an encryption technique. The quick brown fox jumps over the lazy dog...</td>
<td>Ueh?tr?e:1/8 j H H ZZZZq :P - ^ jh J J HH S WIKEM.BRDNY</td>
</tr>
</tbody>
</table>

Table 2: Plain text to cipher text conversion

Conclusion:
This paper deals with a lot of key concept of discrete mathematics to develop the idea behind cryptography. It is a promising work for the beginners to understand the background of such
branches of mathematics in cryptography. The main powerful feature of this algorithm is that, the algorithm will be cryptographically stronger as the input size increases gradually. Since private Key is the main key feature of any symmetric key cryptography algorithm, so we have developed each level of the algorithm in such a way that it gets dependent on the private key and the tracking complexity of each level is so high that it is practically impossible to track the plain text from the cipher text without using the secret key.

References


