International Core Journal of Engineering Volume 7 Issue 5, 2021
ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

A Data Symmetric Encryption Algorithm Based on Double Plaintext and Triple-key Rule

Fei Deng[1,a], Zhiying Yang[1,b] and Danyang Song[2,c]

[1]School of Information Engineering, Shanghai Maritime University, Shanghai 201306, China;

[2]School of Engineering, New York University, Brooklyn NY 11201, United States.

[a]purewhitehz@sina.com, [b]zyyang@shmtu.edu.cn, [c]1094221292@qq.com

Abstract

Yongqian Xiang and his team members proposed a symmetric encryption algorithm based on double plaintext, named Bicycle algorithm. The block mode is ECB mode, and the encryption algorithm is based on a binary linear equations. There are some drawbacks in Bicycle algorithm, such as decryption failure due to the accuracy, invalid tamper proof module, unable to deal with the chosen plaintext attack and so on. In order to overcome these defects, we propose a new encryption algorithm called Re:Bicycle algorithm. Feistel network and three key encryption rules are introduced to rearrange the single group encryption structure. A more effective tamper proof function module is designed by using new parameters, and a CBC block mode based on double plaintext is designed to resist the chosen plaintext attack. Experiments show that the Re:Bicycle algorithm is better than the Bicycle algorithm in the overall efficiency.

Keywords

Symmetric Cryptographic Algorithm; Block Cipher; Double Plaintext; Triple Keys.

1. Introduction

As everyone knows that symmetric key encryption is the encryption strategy often used for information encryption. Symmetric key algorithms ensure the security of encrypted message, while asymmetric key algorithms ensure the security of key transmission. The famous symmetric key algorithm standards are DES[1], 3DES[2], AES, etc. 3DES actually adds two rounds of encryption process on the basis of DES, that is, three rounds of symmetric encryption based on DES standard, thus increasing the intensity of encryption. Secondly, DES and AES also belong to the category of block cipher, and block cipher can be divided into several modes, such as ECB, CBC, CFB[3], etc. In 2018, Yongqian Xiang ect. proposed a dual plaintext symmetric encryption algorithm, hereinafter referred to as the Bicycle algorithm[4]. The main idea of this algorithm is to increase the transmission volume of messages and increase the difficulty of exhaustive attacks by encrypting the two sets of plaintext using the corresponding two sets of keys at the same time. However, it is found that there are some defects in this algorithm. Because the essence of the encryption and decryption method is based on the linear function, there will be errors in the actual calculation process, which will affect the success of the decryption, so the algorithm is not feasible.

We proposed an new algorithm based algorithm Bicycle by discarding liner function encryption structure, used Feistel network in three rounds and triple-key rule to encrypt the two blocks of plaintext respectively, which increases the difficulty of decoding and enhances the security on the basis of making the algorithm feasible. The new algorithm is called Re:Bicycle for short.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

2. Motivation of improving algorithm Bicycle

2.1 Defects in algorithm Bicycle

2.1.1 Calculation Error

The encryption principle of Bicycle algorithm is based on a linear equation $\begin{cases} m_1 = k_1 A + B \\ m_2 = k_2 A + B \end{cases}$. m_1 and m_2 be given plaintexts, k_1 and k_2 be two known keys. The values of A and B are obtained through the linear equation, and finally the ciphertext is obtained by splicing these two value. And we know that if we ask for A, our calculation method is $A = \frac{\Delta m}{\Delta k}$. If Δm is not divisible by Δk, then A is an infinite decimal, and the length of the number processed by computer is limited, so it is impossible to process the infinite decimal accurately. If we set the approximate encryption result of computer as A_0 and B_0, then $A \neq A_0$, $B \neq B_0$.

In the decryption process of the receiver, it is assumed that the receiver obtains the key k_1 and A_0 and B_0 in the ciphertext, then the plaintext data obtained by the receiver will be encrypted as $m_1' = k_1 A_0 + B_0$. Because of $A \neq A_0$ and $B \neq B_0$, we could have $m_1' \neq m_1$ and a failed decryption. In addition, it can be concluded that the algorithm can only work normally when Δm can be divisible by Δk. In other word, Δm and Δk are special and divisible values.

2.1.2 Block Mode

The block mode of Bicycle algorithm is based on the ECB. The principle of ECB block mode is that every block of plaintext and ciphertext are one-to-one corresponding, and there is no relationship between blocks. This leads to a problem: if the plaintext blocks are the same, the corresponding ciphertext blocks are the same. So the attacker can see what plaintext combination exists, and use this as a clue to attack the ciphertext.

2.1.3 Preprocessing Step

There are some problems in the plaintext preprocessing step of Bicycle algorithm. In the preprocessing step, a diffusion algorithm is proposed. This algorithm XORs the hashed plaintext and the filled plaintext to hide plaintext. However, in the decryption process, because the preprocessed plaintext is composed of hash value and diffusion value, and the verification process is to use the decomposed diffusion value to carry out inverse diffusion operation, and then carry out inverse filling to get plaintext. Finally, the hash value obtained from plaintext hash is compared with the hash value obtained from previous preprocessed data, that is to say, in the inverse process. In the process of processing, the hash value in the preprocessed data is still used, so the hash value obtained by inverse processing and the hash value decomposed from the preprocessed data must be equal. In this way, no matter how the attacker tampers with the data, the verification algorithm is almost always passable. Therefore, although the diffusion algorithm achieves the purpose of hiding plaintext, it actually cannot play the role of verification and tamper proof.

2.2 Advantages of Algorithm Re:Bicycle

Re: Bicycle algorithm abandons the idea of linear equations encryption and decryption in Bicycle, but encrypts two blocks of plaintexts with three keys and three rounds Feistel structure[6], and designs a CBC mode based on double plaintexts to replace the original ECB mode, so that the packets are no longer independent, but related to each other. On this basis, the initialization vector in CBC mode is used to hide the preprocessed plaintext in the packet, so as to avoid exposing the plaintext in the preprocessing result and to effectively verify the tampering.

3. Symmetric Encryption Algorithm Based on Double Plaintext and Triple-key Rule

Firstly, the parameters used in the algorithm are introduced

m_1, m_2: two plaintexts in one block structure

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

k_1, k_2, k_3: three groups of keys given by the sender

mh_1, mh_2: hash values of two plaintexts obtained by MD5 hash algorithm[5]

mp_1, mp_2: the value obtained by filling two plaintexts with the filling algorithm

init: initialization vector of each block in CBC block mode

mhp_1, mhp_2: the plaintext preprocessing data obtained by splicing the fill value and init with the hash value after XORing

c: Single block ciphertext

The encryption flow structure of Re: Bicycle algorithm is shown in Figure 1.

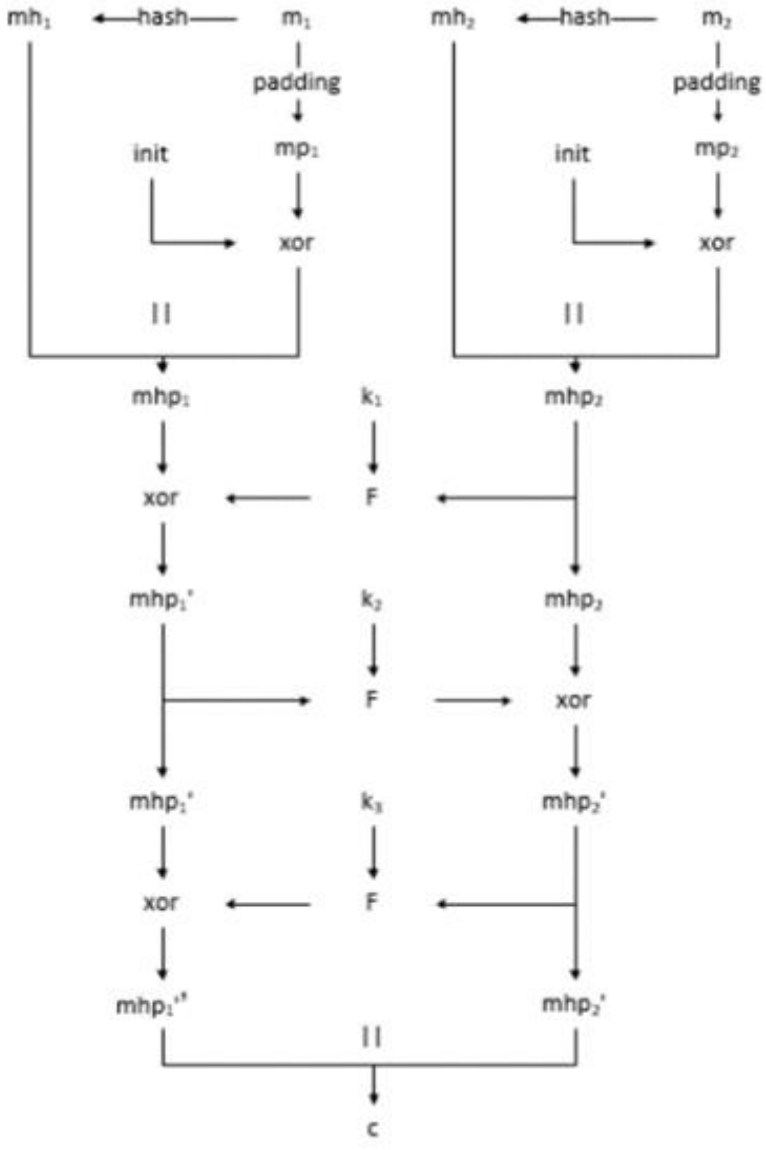

Figure 1. The encryption flow structure of Re:Bicycle algorithm

Encryption process: two blocks of plaintext m_1 and m_2 are hashed to get mh_1 and mh_2 respectively, and then m_1 and m_2 are filled to get mp_1 and mp_2, so that mp_1 and mp_2 are XORed with parameter init respectively, and the result is combined with mh_1 and mh_2 to get the processed plaintext mhp_1 and mhp_2. Then the plaintext mhp1 and mhp2 are encrypted with key k_1, k_2, k_3 and three round Feistel structure[6] to get ciphertext c.

The decryption flow structure of Re: Bicycle algorithm is shown in Figure 2.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

Decryption process: similarly, we decrypt the decomposed ciphertext in a symmetric process through three rounds of Feistel structure and three groups of given keys to obtain two groups of data mhp_1 and mhp_2. Then the verification algorithm is used to decompose the two groups of data and XOR with init to get mp_1, mp_2, mh_1 ', mh_2'. By inversely filling mhp_1 and mhp_2 to get m_1 and m_2, and then hashing the obtained m_1 and m_2 to get mh_1 and mh_2, compare them with mh_1 'and mh_2'. If the two are the same, the decryption is successful, otherwise, it is the opposite.

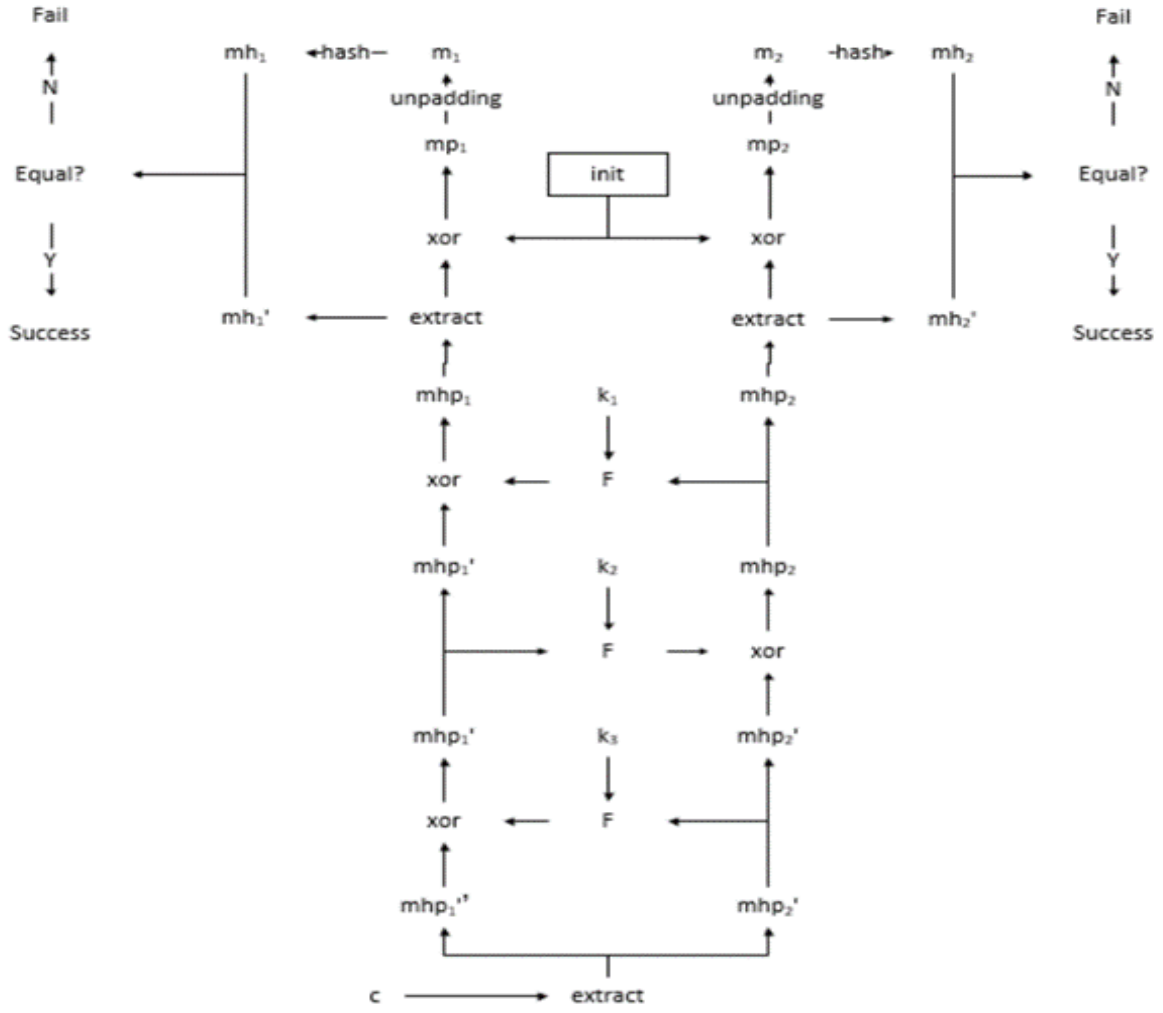

Figure 2. Decryption of Re:Bicycle

The hash algorithm used in this structure is MD5, mhp is used as the packet length, L is 256bit, and K is 128bit. The running speed of the algorithm is compared in the test. The filling algorithm uses PKCS7Padding algorithm[7].

The plaintext is divided into 128 bits:

$$m_1 = m_{11}||m_{12}||\ldots||m_{1i},\ m_2 = m_{21}||m_{22}||\ldots||m_{2i} \quad (1)$$

Re: Bicycle algorithm needs some constraints on the key:

$$k_2 \neq k_1, k_2 \neq k_3 \quad (2)$$

k_1 can be equal or unequal to k_3, and there is no constraint between the two keys. If k_2 is equal to any other key, a part of plaintext will be exposed in the ciphertext, which will cause serious security problems.

The CBC block mode based on double plaintext is adopted in the block mode, and the structure is shown in Figure 3.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

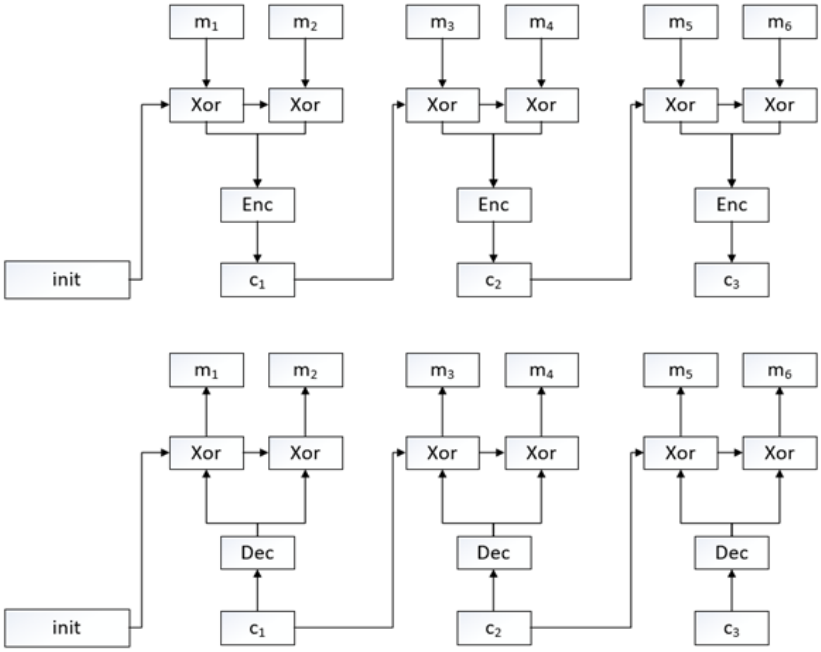

Figure 3. CBC mode based on double plaintext

Re: Bicycle algorithm uses three rounds of Feistel structure, and designs the corresponding CBC block mode based on the idea of double plaintext. It uses 'init', the initialization vector in CBC, to hash and XOR the results of filling plaintext, so as to achieve the purpose of hiding plaintext. In this way, if the attacker obtains the key and decrypts, mhp_1 and mhp_2 are obtained, but they are not exposed in the data so we can't get the real plaintext m_1 and m_2. Here for the convenience of presentation, the wheel function in Feistel structure is defined as XOR operation. In actual operation, the calculation mode of wheel function can be changed arbitrarily according to the demands, such as all kinds of replacement operation, cyclic shift operation and so on.

Round function:

```
RoundF(R,k){
        return R xor k
}
```

Encryption algorithm (single block):

```
ReBicycleEncrypt(m1, m2, k1, k2, k3,init){
    k[ ]=[k1, k2, k3]
    mh1=hash(m1)
    mh2 = hash (m2) // generate hash values of m1 and m2
    mp1=padding(m1)
    mp2 = padding (m2) // fill m1 and m2 to equal length
    mhp1=mh1|| (mp1 xor init)
    mhp2 = (mp2 xor init) | mh2 // splice the xor mp1 and mp2 with mh1 and mh2 respectively
    L= mhp1
    R= mhp2
    for(i=0; i<3; i++){
        L=L xor RoundF(R,k[i])
```

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

```
            If (i = = 2) break; // after the last XOR operation, the loop is terminated without L&R
        swapping
            temp=R
            R=L
            L=temp
        }//Feistel cycle
c = L || R //left and right splicing
}
```

Decryption algorithm (single block):

```
ReBicycleDecrypt(c, k1, k2, k3,init){
    k[ ]=[k1, k2, k3]
    L=extractL(c)
    R=extractR(c) //Decomposing ciphertext
    for(i=2;i>=0;i--){
        L=L xor RoundF(R,k[i])
        if(i==0) break;// After the last exclusive or operation, the loop is terminated without L&
exchange
        temp=R
        R=L
        L=temp
      }//Feistel cycle
      mhp1=L
      mhp2=R
      mh1'=extractL(mhp1)
      mp1=extractR(mhp1) xor init
      mp2=extractL(mhp2) xor init
      mh2'=extractR(mhp2)// Decompose hash value and unknown data respectively
      m1=unpadding(mp1)
      m2=unpadding(mp2)// fill two unknown data inversely
      mh1=hash(m1)
      mh2=hash(m2)// MD5 algorithm is used to hash two plaintexts obtained by decrypting
      unknown data
      if((mh1== mh1')&( mh2== mh2'))
        print(m1, m2)
}// Compared with the hash value, if equal, the decryption is successful
```

CBC mode based on double plaintext:

```
DoubleCBCEncrypt(m1[ ], m2[ ],k1, k2, k3){
      init = random()//Generate random initialization vector
    c[ ] = NULL// Generate an empty ciphertext list
    for(i=0;i++;i<=BLOCKNUM-1){
        L = m1[i] xor init
```

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

```
        R = m2[i] xor L// the two plaintexts xor with initialization vectors
        c0 = ReBicycleEncrypt(L,R,k1,k2,k3,init)//Encryption
        c[ ].append(c0)// Get the ciphertext and input it into the ciphertext list
        init = c0// This block of ciphertext is used as the initialization vector for the next block of block encryption
    }
return c[ ]
}
```

DoubleCBCDecrypt(c[ ],k1,k2,k3, init){

```
    m1[ ] = m2[ ] = NULL// Generate two empty plaintext lists
    for(i=0;i++;i<=BLOCKNUM-1){
        L0, R0 = ReBicycleDecrypt(c[i], k1, k2, k3)//Decryption
        L = L0 xor init
        R = R0 xor L// The decrypted data xor with the initialization vector
        m1[ ].append(L)
        m2[ ].append(R)// Input the obtained plaintext data into the plaintext list
        init = c[i]// This block of ciphertext is used as the initialization vector for the next block of packet decryption
    }
    return m1[ ], m2[ ]
}
```

4. Experiments and Evaluation

The test environment is as follows:

CPU: Intel(R) Core(TM) i7-10750H 2.60GHz

Graphics card: NVIDIA geforce rtx2070super

RAM:16GB

Compiler environment: Python 3.6.0

System environment: Windows 10

In this paper, we implement Re: Bicycle with 256 bits as the packet length and 128 bits as the key length, and test the encryption and decryption speed of 10 groups of random plaintext and random key for 100 times, and compare it with Bicycle. The test results are shown in table 1.

Table 1. Running time of Re: Bicycle

Test Num.	Encrypt Time/sec	Decrypt Time/sec
1	0.59	0.15
2	0.42	0.18
3	0.52	0.21
4	0.48	0.21
5	0.46	0.15
6	0.49	0.17
7	0.51	0.12
8	0.54	0.13
9	0.47	0.14
10	0.51	0.15

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

Table 2 shows the test results of Bicycle. The packet length is 16 bits and the key length is 128 bits.

Table 2. Running time of Bicycle

Test Num.	Encrypt Time/sec	Decrypt Time/sec
1	2.53	0.06
2	2.40	0.07
3	2.41	0.07
4	2.41	0.05
5	2.43	0.07
6	2.36	0.05
7	2.53	0.05
8	2.58	0.05
9	2.53	0.05
10	2.52	0.06

The test results of Bicycle based on the 16 bit and 32-bit block length are very small. Generally, the key length rather than the block length affects the operation performance in the cryptographic algorithm, so the 32-bit test results are no longer listed. From the above test results, we can see that the Re: Bicycle is 1.97 seconds faster than the Bicycle algorithm in encryption and 0.1 seconds slower in decryption. The deceleration of decryption speed is almost negligible compared with the optimization of encryption speed. Moreover, the Re: Bicycle algorithm can encrypt and decrypt on the basis of basic random plaintext and key data, which is very restrictive to the data It needs less data and does not need the support of special data. From the above test data, it is not difficult to see that Re: Bicycle has a very significant advantage over the Bicycle algorithm in terms of comprehensive computing performance.

Re: Bicycle algorithm uses hash function in data preprocessing, and MD5 hash algorithm is used in design and actual test. MD5 hash algorithm has strong collision, it is difficult for an adversary to find two different information corresponding to the same hash value. The main part of encryption and decryption algorithm is based on Feistel structure. Feistel structure with three rounds or more can trigger avalanche effect well. Small changes in plaintext and key will also make great changes in ciphertext. Compared with binary first-order equation encryption in Bicycle, the avalanche effect produced by Feistel structure with three rounds can make it difficult for attackers to infer from ciphertext through rules in data what is plaintext. The verification algorithm in Bicycle is redesigned to make it effective. The hash value in ciphertext is compared with the hash value of decrypted plaintext, which ensures the accuracy and integrity of data in the transmission process and realizes the anti-tampering function. The block mode of the algorithm is the block structure of CBC, and the structure of single block and double plaintext is applied in this mode. Compared with the ECB mode in the Bicycle algorithm, each block in the new block mode is no longer independent of each other, and the attacker can no longer decode the password by analyzing the repeated combination of plaintext and ciphertext rules, which can not only prevent exhaustive attack like the Bicycle algorithm, but also be more effective It can effectively resist the chosen plaintext attack.

5. Conclusion

Re: Bicycle algorithm is a truly feasible encryption and decryption algorithm. It optimizes and improves the tamper proof verification algorithm, and is superior to the Bicycle in the overall efficiency of encryption and decryption. The algorithm is based on Feistel network structure for encryption and decryption. In the process, three groups of keys are needed to decode two blocks of plaintexts, which greatly increases the difficulty of decoding. The symmetric data encryption algorithm of double plaintext can be mainly applied to track compression data and other data encryption transmission with double plaintext characteristics. For example, because track data is generally stored in the form of latitude and longitude coordinates or X&Y coordinates, it is very

ISSN: 2414-1895 DOI: 10.6919/ICJE.202105_7(5).0017

consistent with the idea of double plaintext transmission. But the algorithm also has some problems because the algorithm design idea is carried out in the ideal transmission environment, if there is noise in the data transmission process, it will cause difficulties to the decryption work.

References

[1] Gambhir, A., RSA Algorithm Or DES Algorithm? 2014.

[2] Singh, A., et al., Comparative Study of DES, 3DES, AES and RSA. International Journal of Computers & Technology, 2013. 9(3): p. 97–102.

[3] Antariksa, F.A., Ransomware Attack using AES Encryption on ECB, CBC and CFB Mode. Jurnal Ilmu Komputer, 2019. 12(1): p. 8.

[4] Yongqian Xiang, Zhiqi Song, and Tianyu Wang, A Data Symmetric Encryption Algorithm Based on Double Plaintext. Netinfo Security, 2018. (In Chinese)

[5] Rfc, B., 1321, The MD5 Message-Digest Algorithm. Network Working Group Ietf, 1992.

[6] Ahmed, M., A. Ahmed, and I. Mohamed, Provably Secure Encryption Algorithm based on Feistel Structure. International Journal of Computer Applications, 2016. 139(1): p. 1-8.

[7] Lt, B.K., Com, and B. Gt, PKCS #7: Cryptographic Message Syntax Version 1.5. Rfc Ietf Internet Proposed Standard, 1998.