Analysis of a Modified on Rivets Cipher (RC4) Algorithm by Chaotic Algorithm

Ass.Prof . Maysaa abd ulkareem
Dep. information system
Iman Qays Abduljaleel
dep. Computer Science
Basra University / College of Computer Science and Information Technology

Abstract

In this paper a simply modified RC4 algorithm is presented. RC4 is the most widely used stream cipher and it is not considered as a cipher that is strong in security. Therefore, the nowadays research focused on the development the cipher algorithms to overcome the cleared drawbacks. Rivets cipher (RC4) algorithm is one of the ciphering methods that suffer from numerous weaknesses. These weaknesses include in the algorithm design itself as well as the problem of attaching the WEP by hackers. As a result, these weaknesses encourage the hackers to attach the transmission information. In this paper, a modified cipher algorithm is presented, which combines the RC4 and developed chaotic cipher algorithms. The objective of the proposed algorithm is to encrypt the plain text in two levels. Firstly, this text is encrypted utilizing the well-known RC4 and secondly the resulting ciphered text is encrypted using the modified chaotic algorithm. The output text is the results of the introduced algorithm of this paper with high security and resiliency against the attaching actions. The results show that the modified algorithm is better than the original RC4 in the aspects of secrecy and performance.

Keywords: *Cryptography, RC4, chaotic key, Stream Cipher*

1. Introduction

Cryptography is an indispensable tool for securing the confidentiality of communication and different methods are adapted to encrypt and decrypt data to protect the message. Encryption prevents the invisible modification or deletion of data and regarded as a sign of authentication hat actually resides in the communication systems. Although modern efforts step towards the standardization of algorithms and protocols to make the encryption easier and cheap, many systems fail to meet security [1].

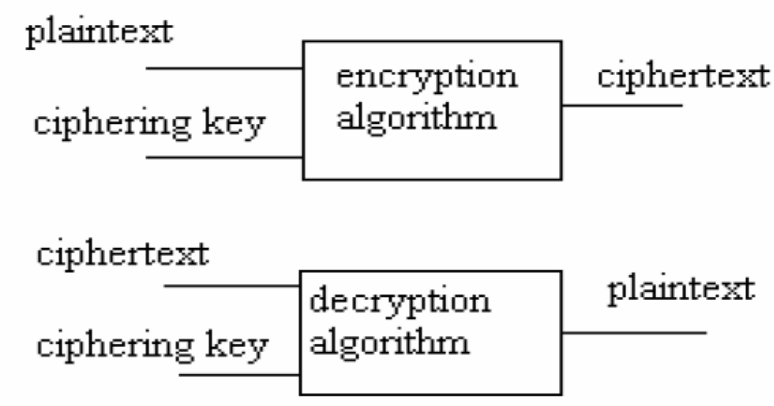


Fig.1 Encryption/Decryption Block Diagram

The primary intention of keeping images protected is to maintain confidentiality, integrity and authenticity. Different techniques are available for making images secure and one technique is encryption. Generally, Encryption is a procedure that transforms an image into a cryptic image by using a key [3].

Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity [3]. All modern cryptographic systems are based on Kerckhoff's principle of having a publicly-known algorithm and a secret key. Many cryptographic algorithms use complex transformations involving substitutions and permutations to transform the plaintext into the cipher text. However, if quantum cryptography can be made practical, the use of one-time pads may provide truly unbreakable cryptosystems [4].

Cryptographic algorithms can be divided into symmetric-key algorithms and public-key algorithms. Symmetric-key algorithms mangle the bits in a series of rounds parameterized by the key to turn the plaintext into the ciphertext. Triple DES and Rijndael (AES) are the most popular symmetric-key algorithms at present. These algorithms can be used in electronic code book mode, cipher block chaining mode, stream cipher mode, counter mode, and others [4].

Public-key algorithms have the property that different keys are used for encryption and decryption and that the decryption key cannot be derived from the encryption key. These properties make it possible to publish the public key. The main public-key algorithm is RSA, which derives its strength from the fact that it is very difficult to factor large numbers [5].

The RC4 algorithm is most used stream cipher algorithm. Different protocol standard used this algorithm to make secure networks. Some of the names of the standard protocols are WPA (Wi-Fi Protected Access), SSL (Secure Socket Layer Protocol), and WEP (Wired Equivalent Privacy) [6]. On the other hand Chaos-based encryption has become an attractive research topic today [7]. Chaos system is used in cryptography for three reasons [8]:

1. The nature of chaos is sensitive to initial conditions of the system,
2. Random chaotic behavior, and
3. The values do not have a period of chaos.

2. Chaos functions

Chaos functions have mainly used to develop mathematical models of non linear systems. They have attracted the attention of many mathematicians owing to their extremely sensitive nature to initial conditions and their immense applicability to modeling complex problems of daily life. Chaotic functions which were first studied in the 1960's show numerous interesting properties. The sequences produced by such functions [9] has very good random and complexity. These functions have an extreme sensitiveness to initial conditions [9].

3. Chaotic map

Logistic Chaotic algorithm. A wide range of ciphers are Included in the chaotic stream cipher, which is a hybrid algorithm of chaotic system and stream cipher. Chaotic system is an important sub discipline of nonlinear science, which includes a one-dimensional Logistic map, bedim tensional Doffing Equation and Henon chaotic system, three-dimensional Lorenz system, Chua's system and CLHE hyper chaos system, and four dimensional R¨ossler hyper chaos system.

Chaotic systems can be roughly classified into two types, chaos and hyper chaos. The essential difference between chaos and hyper chaos lies in the number of positive Lyapunov exponents associated with them. There is a positive exponent In a dynamical system, which is usually taken as an indication that the system is chaotic. A chaotic system with at least two

Positive Lyapunov exponents is typically defined as hyper chaos [10]

Chaotic logistic map can be describe as shown in equation (1) [11]:

$$X_{n+1} = \lambda X_n(1 - X_n) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

Where λ is a control parameter on the interval $\lambda = [0,4]$ and X_n is real number on the interval $X_n = [0,1]$.

This system is said to be chaotic if λ has a value on the interval $= [3.569955672,4]$. In this paper we used $\lambda = 3.57$ so the complete formula is shown in equation (2)

$$X_{n+1} = 3.57 X_n(1 - X_n) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

4. Analysis of RC4 ALGORITHEM

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XOR ed with the plaintext to

give the cipher text. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted [12, 13].

The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The initialization process can be summarized by the pseudo-code [14].

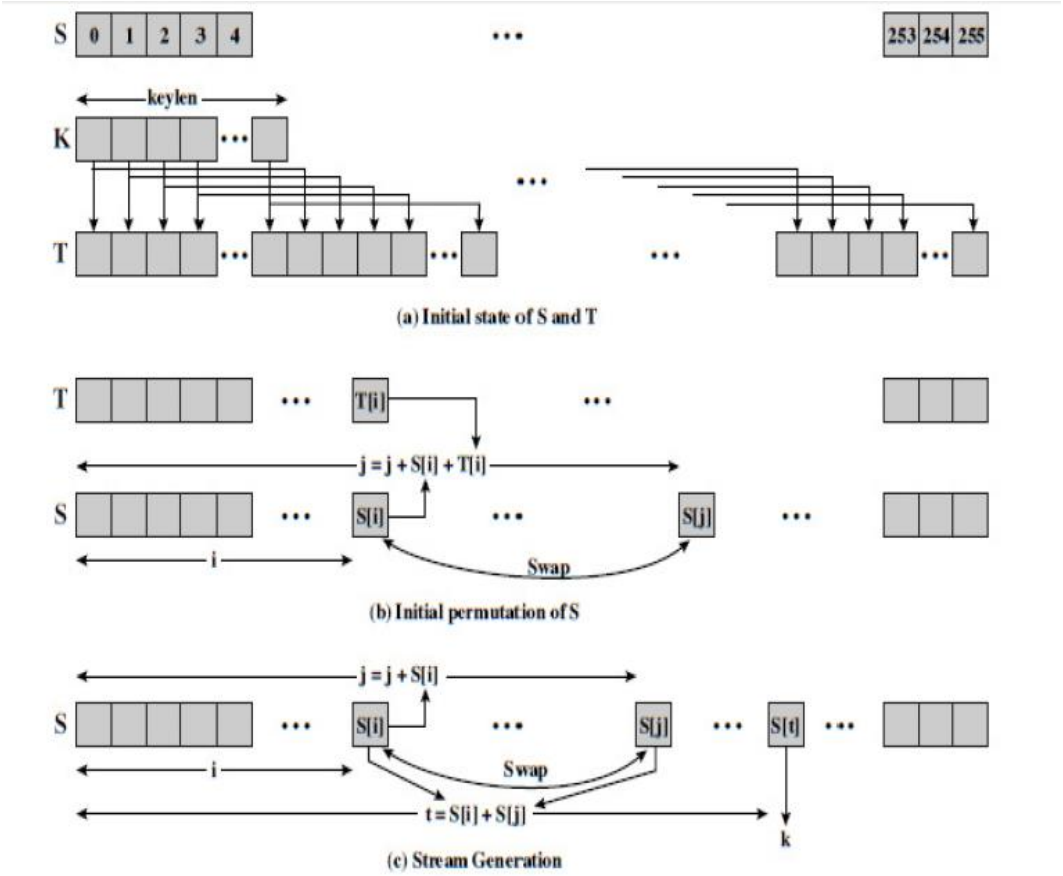
```
j = 0;

 for i = 0 to 255:

     S[i] = i;

 for i = 0 to 255:

     j = (j + S[i] + K[i]) mod 256;

swap S[i] and S[j];
```

It is important to notice here the swapping of the locations of the numbers 0 to 255 (each of which occurs only once) in the state table. The values of the state table are provided. Once the initialization process is completed, the operation process may be summarized as shown by the pseudo code below [14]:

```
i = j = 0;

 for (k = 0 to N−1) {

 i = (i + 1) mod 256;

 j = (j + S[i]) mod 256;

swap S[i] and S[j];

 pr = S[ (S[i] + S[j]) mod 256]
```

output M[k] XOR pr }

Where M [0..N−1] is the input message consisting of N bits. This algorithm produces a stream of pseudo-random values. The input stream is XORed with these



values, bit by bit [15].

Fig (2) Analysis of RC4 ALGORITHEM

Some of the RC4 algorithm features can be summarized as:

1. Symmetric stream cipher

2. Variable key length

3. Very quick in software

4. Used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol [13].

5. Proposal algorithm

In the proposed algorithm, RC4 and chaotic Cipher have been combined the Following fashion:

Step 1: Generate k using RC4.

Step 2: J = random (0,255).

Step 3: S The preparation of the key steps of Chaotic Key:-

(1) Take the values of the primary variable X_0, Let $X_0 = 0.95$.

(2) We read the two keys Key1 and Key2,

Let: - key1 = 113, key2 = 233 and read the values of α, a

Primary α = 3.9.

(3) generate the matrix X, which represents the values that will get it from the application of equation (1) as follows: --

X (i) =α *X(i -1) * (1-X(i-1)) - - - - - - - - - - ---------- - --(1)

Where: i=1...36

(4) The establishment of a new matrix(y), representing the private key Chaotic Key, by

Comparing the value of X with the value 0.5 on the basis of which

The key is created in the

Matrix of the single 0 and 1 as follows: --

If X(i)>0.5

y(i)=0

else

y(i)=1

step 4: C =chaotic (CRC4, K) , k=key1 or key2 .

Bitxor (k,s (i,j))

- Target text to be encrypted and the stream secret Key values with length between 0-255 byte
- Generate state table contain all the different status with size 256 byte
- Used PRGA between state table and the asXcii code to the secret key
- Apply XOR operation with randomly generated pseudo code and replace the pixel value of the selected portion's matrix. Now we get the selected regions encrypted.

6. RESULTS AND ANALYSIS

In this section found in this paper has been classified into two approaches, the time required for the Encryption/Decryption Algorithms and the time required for crack algorithms.

T able 1 . Average Secrecy Value Vs Key Length

key Length/Bits	Average Secrecy of RC4	Average Secrecy of modified RC4
64	0.0325	0.0119
320	0.1101	0.1438
576	0.1807	0.1045
832	0.1538	0.1882

Table 2. Average Encryption Time Vs Key Length

Key Length/Bits	Average Encryption Time of RC4/ us	Average Encryption Time of modified RC4/ us
64	101.4	98.1
576	84.1	73.3
1088	85.7	77.6
320	88.2	79.5

7. CONCLUSIONS AND FUTURE WORK

Thus, a conclusion can be made upon the evident results; the proposed algorithm represents a combination of RC4 and modified chaotic algorithms. This combination produces an algorithm that can tackle the weaknesses of RC4 method.

Modified RC4 gave good results, thus it is clearly obvious that if more samples were taken the results could have been much better. So, the

Simple modification in made RC4 to give better secrecy and performance simultaneously.

Same known plaintext attack for the modified RC4 and original RC4 and evaluate the tolerance levels.

8. References.

[1] R. Tamijetchelvy, P. Sankaranarayanan, S. Kumudham, T. Adhithya, " Robustic and Resilient Multi Key Security in Image Encryption", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Special Issue 3, 2014, India.

[2] Mohit Kumar, Akshat Aggarwal, Ankit Garg," A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications , Vol. 96, No.13, 2014.

[3] Andrew S. Tanenbaum, Computer Networks, Fourth Edition, Prentice Hall, 2003.

[4] David Groth, Network+ ™, Study Guide, Third Edition, SYBEX, Inc., Alameda, CA, 2002.

[5] Glover, P. and M. Grant, Digital Communications, 2nd edition, Person Education, 2004.

[6] Pardeep, Pushpendra, "A Pragmatic Study on Different Stream Ciphers and on Different Flavors of RC4 Stream Cipher", IJCSNS, Vol.12, No.3 , pp. 37-42, 2012.

[7] A. Gautam, P.R Gupta, "A New Image Encryption Approach Using Block Based Transformation Algorithm ", International Journal of Advanced Engineering Sciences and Technologies, Vol.8, No. 1, pp. 090-096, 2011.

[8] Mahfuzulhoq Chowdhury, Md. Moniruzzaman and Parijat Prashun Purohit," Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher", International Journal of Grid Distribution Computing, Vol.7, No.3, pp.189-198, 2014.

[9] Bassem Bakhache, Kassem Ahmad, Safwan el Assad," A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks", International Journal of Intelligent Computing Research (IJICR), Vol. 2, Issues 1/2/3/4, 2011.

[10] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using

chaotic logistic map", Image and Vision Computing, Vol. 24, No.9, pp. 926–934, 2006.

[11] Ni G. A. P. Harry Saptarini, Yosua Alberth Sir," Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Systems International Conference (ISICO), 2013.

[12] Rasha H.Ali, Sawsan H.Jaddoa, " HIDING SECRET TEXT IN IMAGE USING RC4 AND RIJINDEAL ALGORITHM ", International Journal of Computer Engineering and Technology (IJCET), ISSN 0976-6367, Vol. 6, Issue 1, pp. 12, 2015.

[13] Sapna Sasidharan and Deepu Sleeba Philip, "A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITH WAVELET TRANSFORM AND RC4", International Journal of Advances in Engineering & Technology, Vol. 1, Issue 4, pp. 322-331, 2011.

[14] Sapna Sasidharan, Jithin R, "Selective Image Encryption Using DCT with Stream Cipher", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 4, 2010.

[15] Wei Zhang, Qing Chen, Jia Li, Liping Zhang, Shanyu Tang, "Security Improvement in ETC Network Using RC4-Logistic Chaotic Encryption", International Journal of Advancements in Computer Networks and Its Security– IJCNS, Vol. 4 , Issue 4, ISSN 2250-3757, 2014.

تحليل وتطوير خوارزميه RC4 بواسطه خوارزميه Chaotic KEY

ا.م.ميساء عبد الكريم ناصر ايمان قيس
قسم نظم المعلومات قسم علوم الحاسبات
كليه علوم الحاسبات وتكنالوجيا المعلومات

الملخص

ركز البحث على تطوير خوارزميات التشفير للتغلب على عيوبها والخوارزمية المستخدمة هي (RC4) .الخوارزمية هي واحدة من أساليب التشفير التي تعاني من العديد من نقاط الضعف. وتشمل نقاط الضعف هذه في تصميم الخوارزمية نفسها فضلا عن مشكلة ربط WEP من قبل القراصنة. في هذه الورقة، تم تقديم خوارزمية تشفير معدلة، والتي تجمع بين RC4 و خوارزميات التشفير الفوضوي. الهدف من الخوارزمية المقترحة لتشفير نص عادي في مستويين. أولا، النص مشفر باستخدام RC4 المعروفة وثانيا نص مشفر باستخدام خوارزمية chaotic وتعديلها. نتائج الخوارزمية تقدم اجراءات امنية مشددة .أظهرت النتائج أن الخوارزمية المعدلة هي أفضل من RC4 الأصلي في جوانب السرية والأداء.