A Pragmatic Study on Different Stream Ciphers And On Different Flavors of RC4 Stream Cipher

Pardeep
M.Tech Student (Computer Science)
Lovely Professional University
Phagwara, India

Pushpendra Kumar Peteriya
Assistant Professor (Computer Science)
Lovely Professional University
Phagwara, India

Abstract
This is an era of different kinds of computing (Cloud Computing, Distributed Computing, Grid Computing, Ubiquitous computing, etc). Undoubtedly, security is one of the important aspects in every kind of computing. Various cryptographic algorithms are used to secure the information over transmissions, in different aspects like: to restrict the unauthorized access, to ensure integrity, authentication etc. In this paper, different stream ciphers are discussed. Some flavors of RC4 stream cipher are discussed in detail because of its wide use in various standard Protocols (Secure Socket Layer (SSL), Wi-Fi Protected Access (WPA), Wired Equivalent Privacy (WEP), etc). Scopes of enhancement over RC4 are also discussed in the paper in different aspects.

Keywords:
Symmetric, Asymmetric, Stream Cipher

1. INTRODUCTION

Cryptography approaches are used to provide the security of data and information over the Network during transmission of data. In the Cryptography various algorithms are provided the various Security Services like Confidentiality, Data Integrity,
Authentication to protect against the attacks, for examples: - release of message contents, modification of message, masquerade etc. All the attacks are further categories under the two categories, Active and Passive attack. Active attack is where attacker after accessing the message attempts some modification over the message likes modification of message. In passive attack is where attacker just accessing the message not done the modification over the message contents likes release of message contents.
In Cryptography numbers of algorithms are used to provide the Security Services. The Cryptography algorithms are dividing into the two classes, Symmetric and Asymmetric encryption. Symmetric encryption is known as Single key encryption or Secret key encryption or Private Key encryption. In the Secret key encryption, during the encryption and decryption same secret key (same key) is used to convert the plaintext into the cipher text and cipher text into the plain text. In the Asymmetric encryption (Public key Encryption), during encryption and decryption two keys (Pair of keys) are used for encryption and decryption, one of the key is known as public key and second key is known as private key. The Symmetric Encryption class is important in modern Cryptography, reason being the Symmetric encryption Cryptosystem is faster as compare to the Asymmetric encryption cryptosystem [2].
In this paper, basically we focused on the Stream cipher and RC4 as stream cipher algorithm.
This paper is organized as follows: in section 2, we have the description over the Stream Cipher and in section 3; we have the discussion over the RC4 Stream Cipher. In the end in section 4, is providing the conclusion over the discussion given in the paper.

2. STREAM CIPHER

A. Introduction

The Symmetric encryption algorithms are dividing into one of the two classes, Stream cipher and Block Cipher. Stream cipher algorithm is encrypt and decrypt the data bit by bit, byte by byte, character by character, mean during encryption and decryption process converts the plaintext into the ciphertext and ciphertext into plaintext bit by bit, byte by byte, character by character in character fashion. In the streaming process one character encrypted or decrypted at a time. Block cipher algorithm is encrypt and decrypt in the block fashion, first prepare a block of specific size (16 bytes, 32 bytes, 64 bytes, 128 bytes) depend on the used algorithm approach, then whole of the block encrypt and decrypt at a time. In the blocking process of encryption and decryption more than one character, bytes, and bits process at a time. Stream cipher algorithm are faster, acquire less CPU time, less resources utilization, easy to implement as compare to the Block cipher algorithm [1]. Stream Cipher is the reason the Stream cipher also a popular and most used class for security.

Manuscript received March 5, 2012
Manuscript revised March 20, 2012

B. Types of Stream Cipher

Basically there are two types of Stream cipher. First is Synchronous stream cipher and Self- Synchronous stream cipher [2]. In Synchronous stream ciphers the key stream is generated from the key independently of the plaintext and the cipher text and in the Self-Synchronous stream cipher the key stream is generated from the key as well as fixed number of previous cipher text digits [2].

C. Performance Analysis of Stream Cipher

Now we discuss the performance of the Stream cipher algorithms that are used for the encryption and decryption of data for making secure the information.

Suhaila Omer Sharif and S.P. Mansoor [1] have given the performance analysis on the different Stream cipher algorithms RC4, Salsa20, HC-128, VMPC, and Grain. Analysis has performed over the Desktop computer with 3.06 GHz processor operating under UNIX was used. Java platform was implemented to write a GUI interface with Bouncy Castle Crypto API library.

In this performance analysis among the Stream ciphers, calculated the encryption and decryption time using different sizes input files and also compute the though put in Megabytes/sec.

After the simulation, calculated result shows RC4 having faster encryption and decryption among the other stream cipher algorithms and also having better throughput than the other Stream ciphers.

Figure1 and Figure 2 show the results of all the stream ciphers.

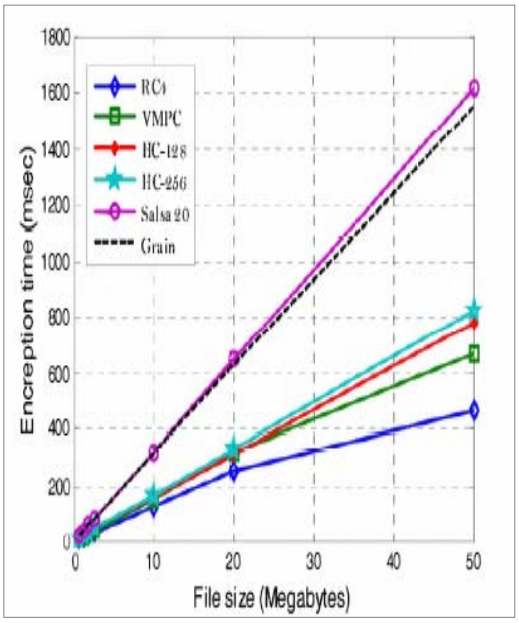

Figure1 Encryption/Decryption time for the stream cipher [2].

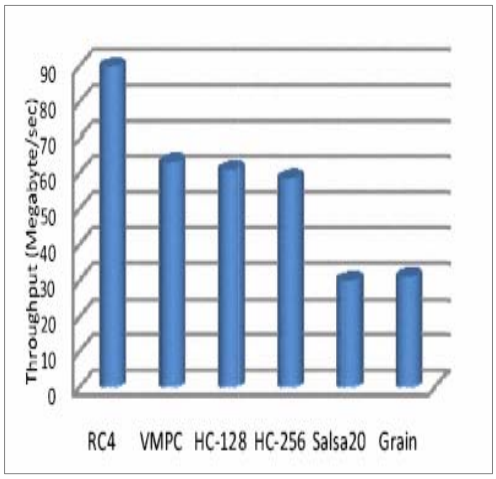

Figure2 Through put of the Stream cipher algorithm [2]

In this study also done the performance analysis on the Block cipher algorithm, finally result shows the superiority of RC4 among all the other algorithms in term of speed and through put.

D. Standardization of Stream cipher

Stream cipher Algorithm is used in the various information procession system. The three main significant ones are A5/1 in GSM networks, E_o in Bluetooth Standard and RC4 in WEP (802.11 Wireless LAN standard) [2].

3. RC4 STREAM CIPHER

A. Introduction

RC4 Stream cipher was introduced in the year 1987 by Ron Rivest of RSA security [5]. The official name of RC4 is “Rivest Cipher 4”. From 1987 to 1994 RC4 kept secret, mean not disclose the internal design of this approach into market. In September 1994, the detail of the algorithm design was posted to the Cypherpunks mailing list. After it was also posted to the sci.crypt newsgroup and from there posted to the various site over the internet [5]. Mean openly disclose the design of the RC4 stream cipher. Because the algorithm is now well known, so it is no longer a secret, we should note that there is a trademark associated with the name “RC4” and an interesting remark says that “The current status seems to be that unofficial implementation are legal, but cannot use the RC4 name” [5]. RC4 is the most used Stream cipher algorithm in the various standard like SSL to secure the internet traffic and also mainly used to secure the E-Commerce transaction and information over the Network, also adopted in WEP and WPA to secure the wireless Network. RC4 stream cipher have various advantages that’s why the most of the standard adopt this algorithm to making secure the information, it have the high speed of encryption and

decryption the data, simple, easy to use , easy to design , easy to implements , having low time complexity , not consume the resources, implementation on both hardware and software level. Number of operation requires performing the encryption and decryption of data too small which make this algorithm too efficient.

B. Description of RC4

RC4 stream cipher most preferred Stream cipher algorithm. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process of algorithm, mean RC4 basically two stages process.

In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage

Following steps are done

1. inputting the variable length key of size from 1 to 256
2. initialize the key matrix as per the size of the input key
3. Initialize the State table of fixed size 256 bytes from the value 0 to 255 in ascending order.
4. using the key matrix of variable size done the permutation on the S table
5. Output of the KDA, the final prepare S table after shuffling operation.

In this manner the KDA generate the State Table (State Matrix) of 256 bytes.

Now let's discuss the algorithm of the KDA as following

KSA

1. for i=0 to N-1
2. s[i]=1
3. j=0
4. for i=0 to N-1
5. j=(j+s[i]+k[i]) mod N
6. swap(s[i],s[j])

Now we going to discuss the second stager of the algorithm known as PRGA

These stages basically used to generate the output key stream that used to encrypt and decrypt the data by XORing operation.

The algorithm description the algorithm as following

PRGA

1. i=j=0
2. Loop
3. i=(i+1) mod N
4. j=(j + s[i]) mod N
5. swap(s[i],s[j])
6. output= s[s[i] + s[j]] mod N]

From the last long time there are lots of weaknesses and attack to be found over the RC4 algorithm, some of the weaknesses detect in the KSA and some of the weakness is detect in PRGA of the algorithm.

C. Attack over RC4

In 1994, the RC4 algorithm was disclosed in to the market and then experts start to analyze the RC4 algorithm and find out the lots of weaknesses in both the stages of the algorithm KSA and PRGA. Many cryptanalysis of the algorithm was divided into the two parts, analysis of the initialization of RC4 which focuses on the initialization of KSA and analysis of the output key stream generation which focuses on the internal state and the round operation of PRGA [4].

Mantin and Shamir [6], was find out the weakness in the second round the probability of Zero output bytes as the major weakness of the algorithm.

Fluher et al. [7], was discovered the big weakness in the RC4, if anyone now the portion of the secret key than possible to attack fully over RC4.

Paul and Maitra [8], was discovered the secret key by using the initial state table. They generated some equation on the bases of initial state table and they select some of the bytes of secret key on the bases of guess and remain secret key find out by using the equation.

So we know that the security of RC4 depends on the security of the secret key and the internal states of S-box, so many attacks focus on resuming the secret key of the internal states of the S-box.

And also there is lot of other weaknesses and attacks are to be found over the RC4 algorithm. To making secure the RC4 that capable to stand against the attack, lot of research done over RC4 to enhancing the security of RC4.

D. Enhancement description on RC4

Now we know the RC4 stream cipher algorithm having lots of weaknesses and vulnerable point. So over the time, some of the experts, researcher is introduced some of the enhancement on the RC4 stream cipher to increase the security of the RC4, to making it strong against the attack. Now we discuss in the previous section in this paper, there are lot of weaknesses find out in the both stages of the algorithm, KSA and PRGA. So some of the researcher working some of the enhancement over the KSA and some of over the PRGA to making strong to both the stages against the attacks, find out in both the stages over the times.

Now let's discuss some of the enhancement proposed by the some of the researcher to increase security of the RC4.

(a). FJ-RC4 Stream Cipher

Fahime, Mohammad, Hamid, Payman, shows [3], the new developed approach based on the RC4 for the purpose to making strong the RC4 approach against the attacks. In this study shows the new KSA stage of the RC4 having vulnerable stage against the attack so in this study introduced new approach named as FJ-RC4 on the bases of the new developed KSA algorithm to making strong the stage against the attacks and also to the RC4 stream cipher. In this self developed new algorithm, FJ-RC4 is built from the new KSA, which uses the key stream in three stages process and shares the PRGA structure same as based on the previous structure of the PRGA of RC4, just one difference in PRGA stage of the FJ-RC4 algorithm, it is three stages encryption and decryption process but in the PRGA of RC4 having one stage encryption and decryption process.

Let's discuss the algorithm in detail

Key Scheduling Algorithm

In this KSA process of FJ-RC4 is introducing the new KSA algorithm to making strong the stage against the attacks. In this stage of FJ-RC4, the main key is further dividing in to the three equal portions in form of three sub keys. If the length of the main key is not divisible by the three for the purpose to divide it into the three different equal portions than Zero padding have done over the key to making it divisible by 3.

Above is giving the description of the

KSA Algorithm.

```
String key;
String [] array = new String[3];
int remain = 3 – (key.length() % 3);
if(remain != 3)
{
        for(int i=0; i<remain ; i++)
        {
                key = key + "0";
                Repeating o as necessary;
                }
}
int temp = Key.length() / 3;
array[0] = key.subsrting ( 0, temp);
Fill the first string array;
array[1] = Key.substring( temp,  temp+temp);
Fill another array of the same size with the Key
Array[2] = Key.substring9 temp +temp, Key.length());
```

During the encryption process, in the first stage, the plaintext XOR with the key stream generated on the basis of first key than in the second stage, the encrypted output of the of the first stage XOR with the key stream generated with the help of second sub key and then in the final stage, the second double encrypted message then again encrypted with the key stream generated on the basis of the third sub key.

In this study shows the new developed algorithm on the basis of RC4 is stronger than the previous RC4 against the attack, it takes more time to find out the key as compare to the RC4.

These approaches also require more resources than the RC4 and Key scheduling in FJ-RC4 slower then the RC4 because of the three key processes. But this algorithm proves to be more secure than RC4.

(b). an Improved RC4 Stream Cipher

Jian and Pan, shows [4] new work on the enhancement over the RC4 stream cipher. In this study, the researcher work on the PRGA the second stage of the RC4 algorithm which is also detect to be vulnerable. To making secure the RC4 as well as to increase the security of the PRGA against the various attacks and to protect against the attack, in this study is introducing the new PRGA algorithm and shows the new enhancement over the RC4 to increase the security of the algorithm.

In this study basically discuss the one of the weakness of the PRGA is the relations between the S-boxes in different time. Many attacks tried to resume the initial state of the PRGA and achieved good efficiency. In this paper, mainly focus on the weakness of the PRGA and introduced the new improved RC4 to protect PRGA against the attack named as "An improved RC4 stream cipher".

Algorithm Description

In this improved rc4 algorithm researcher in the KSA stages generate 2 S-Boxes on the based of the two secret key secret key1 and secret key2.

KSA;

```
For i=0 to N-1
{
        s1 [i] = i;
```

```
        s2 [i] = i;
}
j1=j2=0;
for i=0 to N-1
{
        j1=(j1 + s1[i] + k1[i] ) mod N;
        swap( s1 [i], s1 [j1] );

        j2=(j2 + s2[i] + k2[i] ) mod N;
        swap( s2 [i], s2 [j2] );
}
```

PRGA;

```
I=j1=j2=0;
Loop
{
        i=i+1;
        j1=j1+s1[i];
        swap ( s1[i], s1[j1] );

        j2=j2+S2[i];
        swap (s2[i], s2[j2]);

        output= s1[ (s1 [i]) + s1 [j1]) mod N ];
        output= s2[ (s2 [i]) + s2 [j2]) mod N ];

        swap ( s1[s2[j1] , s1[s2 [j2]] );
        swap ( s1[s2[j1] , s1[s2 [j2]] );
}
```

and in the PRGA stage, two state boxes s1 and s2 are used to getting the output random key stream that used for the encryption and decryption. However, the elements of S-box are swapped only by a public pointer i and a secret pointer j+ s [i] in RC4, which leads to the relations between the states of S box. Therefore, our efforts focus on destroying the relations. In the improved RC4, we can get two secret parameters j 1 and j2 from the S boxes s 1 and s2 at the end of every loop. By the secret parameters j1 and j2, we can calculate four secret index-pointers s2 [j1], s [j2], sI [j1], s [j2]. The elements of s1 are swapped by the pointers s2 [j1] and s2 [j2] and the elements of s2 are swapped by the pointers sI [j1] and s [j2] at the end of every loop. As the index-pointers s2 [j1], s2 [j2], s1 [j1] and s1 [j2] are secret, which elements of sI and s2 are swapped is unknown. This is one of the innovations in this paper. More elements are swapped increases more confusion in the S-box. By this, the relations between the S-boxes are no longer existence in the improved RC4.
The new algorithm enhances the security of the RC4 and it is faster than RC4.

(c). RC4A Stream Cipher

Abdullah, Roslina, Abdul, Liakot shows [10] RC4A, an RC4 family stream cipher algorithm, developed by S. Paul and B. Preneel [11] which attempts to increase security without decreasing efficiency. RC4A stream cipher works in two phases, KSA (Key Scheduling Algorithm) phase and PRGA (Pseudo Random number Generation Algorithm) phase. During PRGA two successive output bytes are generated. The goal behind RC4A was to increase security primarily by increasing the internal complexity of the algorithm [9]. RC4A is made through improvement on the RC4, i.e., providing 2 S arrays (S1 and S2) that are Independent from each other and so that RC4A should not have bias in consecutive output byte. RC4A uses three counter i, j1, and j2. Variable j1 and j2 are introduced, corresponding to S1 and S2. In KSA for RC4A, like KSA of RC4, the array S1 is initialized, using the secret key K, Key stream, WK, are generated from the array S1 like PRGA (Pseudo Random number Generation Algorithm) of RC4. Then, like S1, the array S2 is initialized using WK. Unlike RC4 in PRGA of RC4A two successive output bytes are generated. All the arithmetic operations are computed
Modulo N (N=256) [11].

Algorithm
KSA (K)
RC4_KSA(K,S1)
For i=0…….I-1
WK[i]=RC4_PRGA(S1)
RC4_KSA(WK,S2)

PRGA(S1,S2)
Initialization
i=0
j1=j2=0
Generation loop;
I=i+1
J1=j1+s1[i]
Swap(s1[i],s1[j1])
Output z1=s2[s1[i] + s1[j1]]
J2=j2+ s2[i]
Swap(s2[i] , s2[j2])
Output z12= s1[s2[i] + s2 [j2]]

4. CONCLUSION AND FUTURE WORK

Through the discussion over the paper we discussed first the basic behind the Cryptography then later in the Discussion move to the Symmetric Stream Cipher one of the most important and most used class of the Symmetric algorithm. We also discuss the survey over the performance of the various stream cipher algorithms and RC4 stream cipher is proved to be batter than among all.

So in the end of the paper, we discussed the RC4 stream cipher algorithm in detail and discussed the various applications where we used the RC4 for the security purpose, basic algorithm, attacks and the various enhancements on RC4, is introduced by the some of researcher to increase the security of the RC4 stream cipher against the attacks and weaknesses.
So in this manner, we just see the enhancement over the RC4 stream cipher done by the different experts to increase the security of the RC4 stream cipher. Still lots of research to be done to improved the security of the RC4 to increase the security of the application where we used the RC4 to securing the information like SSL in internet, WEP and WPA in wireless network and also in sensor network.

REFERENCES

[1] Suhaila Omer Sharif, S.P. Mansoor, "Performance analysis of Stream Cipher algorithms", 3rd international conference on Advanced Computer Theory and Engineering (ICATE), 2010.
[2] C.S Lamba, "Design and Alnalysis of Stream Cipher for Network Security ", Second International Conference on Communication Software and Networks, 2010.
[3] Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghinghat, "A New Symmetric Crtptographic Algorithm to Secure E-Commerce Tracsactions", International Conference on Financial Theory and Engineering, 2010.
[4] Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher ", International Conference on Computer Application and System Modeling (ICCASM), 2010.
[5] Atul Kahate ,"Cryptography and Network Security" , pp-123-125, 2008.
[6] I. Mantin, A. Shamir "A practical Attackon Broadcast RC4", FastSoftware Encryption 2001 (M.Matsui,ed.), pp. 152-164, Springer-Verlag, 2001.
[7] S.Fluthrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", SAC2001 (S. Vaudenay, A. Youssef,eds.), col. 2259 of LNCS, pp. 1-24, springer-Verlag, 2001.
[8] G. Paul, S.Maitra, "RC4 state in formation at Any Stage Reveals the Secret Key ", In proceedings of SAC2007, http://eprint.iacr.org/2007/208.pdf, 2007
[9] A. Klein, Attacks on the RC4 Stream Cipher, http://cage.ugent.be/-klein/RC4/RC4-rn.
[10] A.A. Noman, Dr. Roslina b. Mohd. Sidek, Dr. A.R.b. Ramli, Dr. L. Ali, "RC4 Stream Cipher for WLAN Security: A Hardware Approach", 5th International Conference on Electrical and Computer Engineering, ICECE 2008.
[11] S. Paul, and B. Preneel, "A New Weakness in the RC4 Keystream Generator", Fast Software Encryotion, FSE 2004, LNCS 3017, 245-259, Springer- Verlag, 2004.