A New Robust Enrichment Symmetric Stream Cipher Approach for Confidentiality Based on RC4 Stream Cipher Algorithm

Jagdeep Singh
MTech (CSE) Student
Lovely Professional University

Kundan Munjal
Assistant Professor in Computer Science
Lovely Professional University

Abstract

This research paper is proposing new approach named as "Robust-RC4" for implements security over the different types of network like: Internet Network, Sensor Network, wired and wireless networks and E-Commerce Application. The approach "Robust-RC4" is introducing in the paper basically derived from the standard RC4 algorithm. The RC4 algorithm is most adopted security approach over the different types of network. The RC4 algorithm is also adopted in standard named WPA (Wi -Fi Protected Access), WEP (Wired Equivalent Privacy) and SSL (Secure Socket Layer) Protocols for providing the security. But there are lots of weaknesses and attacking point exist under the RC4 algorithm, that's the reason, it is easy to break this algorithm. So to make more robust to RC4 algorithm, "Robust-RC4" is proposed in this paper.

Keywords: Cryptography, Confidentiality, Stream Cipher, RC4,

1. Introduction

Presently, the area of network and communication is too vast. There are introducing different types of network at present as per the development in the field of network and communication. Some of the most used types of networks are internet network, sensor network, Wired Network, Wireless network and E-Commerce Networks and so on. The
Basic purpose of these all types of network is just the communication through the data and information transmission. With the emergence of communication of data and information, then becomes the need of security over the network. The need of the security becomes most needed because of the emergence of the business, commerce and banking on the network. Now the question if how the security is being implement on the data and information and over the network. So this need, emerge a new filed of computer science in concern to the network security and data/information security is the "**Network and Security**". Now to implement the security over the networks, arise a new area of research, where number of researcher being researched from the last long time and also done lots of research. So in this

concern lots of concept being introduced. Most considerable is known as “Cryptography”. [1, 2]

The Cryptography is the concept provides the different types of security level which being implemented and also provides the approaches and algorithms which can be used to implement the security level on the network and data and information. Basically the basic securities services provide by the cryptography are Confidentiality, authentication and authorization. Each type of services has its advantage in concern to the security over the network. The most concerned security services as compared to all other securities services, is the confidentiality where this paper most concentrated. **The confidentiality** means to make secure the data and information over the network from the accessing the unauthorized persons. To implement this way, cryptography provides the various algorithms of security. These algorithms are used to encrypt the data and send the data in encrypted form over the network so in this manner; the confidentiality service is being implemented over the network. [1, 2]

The Cryptography algorithms are further dividing into the two classes as per way of encryption and decryption, Symmetric and Asymmetric. Symmetric encryption is also known as private key encryption and same key encryption. In symmetric key encryption same key is used for encryption and decryption. And second side in Asymmetric key encryption is also known as public key encryption. in Asymmetric key encryption, pair to key is used for the purpose of encryption and decryption. The entire algorithm which is used for the purpose to provide the confidentiality services over the network are further consists in these two classes of encryption and decryption. At present, the researchers are considered symmetric encryption class is most important as compare to the Asymmetric in concern to confidentiality. Reason of this is symmetric encryption provides fast encryption as compare to the Asymmetric encryption [3].

The entire approaches are used for the encryption and decryption are dividing into two groups, stream cipher and block cipher as according to the way of encryption and decryption. In the stream cipher way of processing the data, data is encrypt and decrypt byte by byte by the algorithms. These all the approaches are consists under the category of stream cipher. In the block cipher mode of process, the data is encrypt and decrypt in blocking manner, so in this way possible to encrypt and decrypt more then one bytes at a time. The steam cipher algorithms are utilizing less hardware resources, less time during encrypt and decrypt the data as compare to the block cipher [4]. So this is the reason lots of research presently done in the stream cipher mode.

Stream Cipher and its applications

The stream cipher is the one of the important class of encryption and decryption algorithms. The stream cipher algorithms are encrypted and decrypt the data byte by byte, bit by bit. The two types of stream ciphers are First is Synchronous stream cipher and Self-Synchronous stream cipher [3]. In the synchronous stream cipher, the key stream is generated from key, plain text and cipher text independently. In the self- synchronous stream cipher, the key stream is generated from key as well as plaintext and cipher text dependently [3].

Performance evaluation of Stream Cipher

In this section, this paper is present the some of the parameters, discussion, result over the stream cipher performance which is being evaluated by the researcher [4].

The researchers are taking different stream cipher algorithms named as RC4, Salsa20, HC-128, VMPC, and Grain. The environment where simulates the entire algorithms for performance analysis, is having desktop computer with 3.06 GHz processor with UNIX operating system. And java platform is used for write GUI interface with Bouncy Castle Crypto API library**.** [4]

Now let's see the some of the performance result which shows by the researchers,

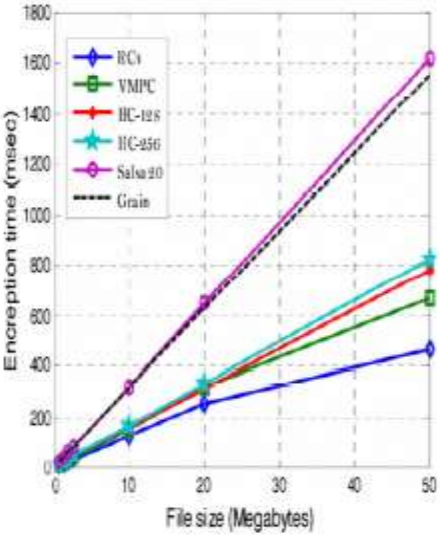

Figure 1:- Encryption and Decryption time of the algorithms [4]

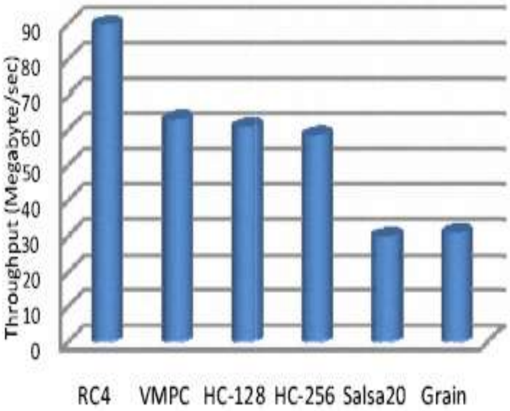

Figure 2:- Shows the through put of the stream cipher algorithms [4]

As per the above study and simulation result shows the RC4 stream cipher algorithm is faster than then the other stream cipher algorithms. And in this paper researcher are take some block cipher algorithm and simulate all in same manner. And in last shows the RC4 stream cipher algorithm is faster then the Other steam cipher algorithms and block cipher algorithms which are taken in this paper.

RC4 Steam Cipher

Introduction of RC4 algorithm

In this section, this paper described the RC4 stream cipher algorithm. RC4 algorithm was introduced in 1987. The Ron Rivest is the name of the person who's introduced this algorithm. RC4 is named as " Rivest Cipher 4". The RC4 algorithm is remain secret from 1987 to 1994. After this time, RC4 algorithm is disclosed in the market/ on internet. Then after the disclosing of this algorithm, the researches are started to research on this approach. Then researchers are found lots of weaknesses in this algorithm.[5]

No doubt the RC4 algorithm is the most used stream cipher algorithm. This algorithm has lots of positive point like: less time utilization during encryption and decryption, less resources utilization, simple implication, easy to understand, easy to work, little line code inside the algorithm. So this the reason, RC4 algorithm is adopted over lots of networks and standard to provide the confidentiality security. Some famous standard like: SSL, WEP, WPA are preferred this algorithm to implement the security over the network.

But after disclose ness of this algorithms, attacker and cryptanalytic are find lots of weak point and attacking point in this approach. So this approach is not secure to use for security purpose. Mean required to improve the level of security provide by the RC4 algorithm. Lots of researchers are doing lots of work and also some of introducing some enhances approaches to improve the security of the algorithm.

Description of RC4 Algorithm

RC4 algorithm is further dividing into two stages known as KSA, PRGA. Means the RC4 algorithm during encryption and decryption is passes through the two stages. In the first stage in KSA, does the randomization of the state matrix of size 256. And the after starts the second stage. In the second stage randomly generated the bytes to encrypt and decrypt the each and every character of the data being inputs.[6]

Now let’s discuss algorithm in detail:-

Initialization point:-

State_matrix [256]
Key_matrix [256]
N=256

KSA:-

```
j=0
for i=0 to N-1
    j=(j+state_matrix [i]+key_matrix [i]) mod N
    swap(state_matrix[i],state_matrix [j])
End for
```

PRGA

```
i=j=0
Loop
    i=(i+1) mod N
    j=(j + state_matrix [i]) mod N
    swap(state_matrix [i], state_matrix [j])
    output=state_matrix[state_matrix [i] + state_matrix [j] ] mod N]
```

Attack over RC4

In 1994 the RC4 algorithm discloses 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 [5].

Mantin and Shamir [7] find out the weakness in the second round the probability of Zero output bytes as the major weakness of the algorithm.

Fluher et al. [8] 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 [9,10] was discovered the secret key by using the initial state table. They generate 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.[11]

So we know 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. [12]

Self detected Weaknesses in RC4

In RC4 algorithm, basically the key concept using behind the algorithm is the randomization. In KSA, performs the randomization on state matrix. Randomization just depends on the key matrix [256] which contains the random bytes. But this level of randomization is too low from the security concern. Attacker can easily attack on this parameter. And no any randomization is provided on the index level. In KSA, i value uses to generate index, which directly checks index generated by this i value from 0 to 255. So attacker can easily judge this strongest point of the algorithm.

Same in PRGA, value of i is all the time generated from 1 to 256 this also directly understandable from the first line of the PRGA algorithm. Same on index level also no any randomization in PRGA. Attacker can easily attacks on the index level. And also the randomization just only provides by the state matrix in PRGA which already randomize. So require to improve this level of randomization by including some other parameters.

Proposed Algorithm Robust-RC4

The RC4 algorithm is so simple and some lines algorithms. But the level of security requires presently from the confidentiality point is too high. So this paper works in this concern. The proposed algorithm in this paper is trying to improve the strong ness of the RC4 algorithm and trying to improve the algorithm from the weak points.

This proposed algorithm is providing two stages encryption and decryption. During encryption as well as decryption, data is being processed two times. This proposed algorithm is trying to making the RC4 algorithm too strong. Also this proposed algorithm also proposed some enhancement inside the KSA and PRGA sub steps inside the RC4 algorithm.

So weakness detects in both the stages KSA and PRGA. So to making secure the RC4 algorithm required to enhance the KSA and PRGA for the purpose to secure the RC4 Algorithm. So this algorithm, also introduces the different way inside the KSA and PRGA.
Let’s now see the proposed algorithm:-

Algorithm:-

Initialization:

```
State_matrix1 [256]
State_matrix2 [256]
Key [256]
Key1 [256]
Key2 [256]
```

KSA:

```
1. J1=j2=0
2. For i=0 to N-1
3. J1= j2+ state_matrix1 [i]+ key2 [i] +key2 [j2] + key[i] % N

4. J2= j1+ state_matrix2 [i]+ key1 [i] +key1 [j1] + key[i] % N

5. Swap (state_matrix1 [i], state_matrix1 [j1])

6. Swap (state_matrix2 [i], state_matrix2 [j2])

7. End for
```

PRGA:

```
1. J1=j2=0
2. While (true)
3. i=i+1 % N
4. j1= j1+sate_matrix1 [i] + key1 [i] % N
5. j2= j2+sate_matrix2 [i] + key2 [i] % N
6. Swap (state_matrix1 [i], state_matrix1 [j1] )N
7. Swap (state_matrix2 [i], state_matrix2 [j2])N
8. in1=state_matrix1 [i] + state_matrix1 [j1]
8. in2=state_matrix2 [i] + state_matrix2 [j2]
9. op1= PT  Xor state_matrix1 [in1]
10. op2= op1  Xor state_matrix2 [in2]
11. end while
```

Description of proposed Algorithm

The proposed algorithm introduced the new way of RC4 working. The proposed algorithm introduced a new algorithm for the both staged KSA and PRGA. This algorithm is taken two additional key matrix key1 and key2 which created on the behalf of key size given by the user. Then also takes the two state matrixes which have taken 256 bytes. From this state matrix, this algorithm chooses the random bytes used to encrypt and decrypt the data. Inside the KSA, generates two index pointer j1 and j2 for the purpose to randomize the both state matrixes. Also during generated the j1 and j2 does not only use the state matrix and key matrix as RC4, this approach uses the also the key2 and key1 matrixes to improve the randomization level inside the KSA. Also in KSA, uses the j1 and j2 at the index level to provide the randomization on the index level which not available in RC4 algorithm.

In PRGA, using two index pointers are j1 and j2. j1 and j2 both generate not only on the behalf of state matrix but also on the behalf of key1 and key2 to improve the randomization level inside the PRGA stage. This generates two random index pointers in the end in1 and in2 from where access the bytes from state matrix1 and state matrix2 and done the two times encryption and decryption. Also in proposed algorithm used the key matrix not in the KSA but also in both the stages this provides the additional better security level inside the algorithm.

The main advantage in this algorithm is during attacks attacker required to check

256 x 256 bytes in each character of the cipher text and then again a tough pattern matching. But in RC4 algorithm is just required to check 256 bytes on each character to cipher text.

No doubt, this approaches utilizing more time and more resources as compare to the RC4 algorithm, but this algorithm better from the confidentiality point which more demanding over the different types of network like: E-Commerce and Internet networks, where resources utilization not matter more as compare to other types of network like: Sensor network.

Conclusion

This paper describes the some basic introduction of security and stream cipher and RC4 stream cipher algorithm. This paper is basically provides the enhanced algorithm to improve the security of the RC4 stream cipher. The detail about the algorithm is provides in detail manner.

References

1. William Stalling, "Network security and cryptography".

2. Atul Kahate ,"Cryptography and Network Security" , 2008.

3. C.S Lamba, "Design and Alnalysis of Stream Cipher for Network Security ", Second International Conference on Communication Software and Networks, 2010.

4. Suhaila Omer Sharif, S.P. Mansoor, "Performance analysis of Stream Cipher algorithms", 3rd international conference on Advanced Computer Theory and Engineering (ICATE), 2010.

5.Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher ", International Conference on Computer Application and System Modeling (ICCASM), 2010.

6. 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.

7. I. Mantin, A. Shamir "A practical Attackon Broadcast RC4", FastSoftware Encryption 2001 (M.Matsui,ed.), pp. 152-164, Springer-Verlag, 2001.

8. 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.

9.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
10.A. Klein, Attacks on the RC4 Stream Cipher, http://cage.ugent.be/-klein/RC4/RC4-rn.

11.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.

12.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.