Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Comp Page 27 - 32 Mustafa .M/Soukaena .H

Lightweight RC4 Algorithm

Mustafa M. Abd Zaid **Soukaena Hassan**

University Of Technology , Computer Sciences Department
mustafamajeed2014@gmail.com Soukaena.Hassan@Yahoo.Com

Recived : 9\10\2018 **Revised 14\10\2018** **Accepted : 21\10\2018**

Available online : 25/1/2019

DOI: 10.29304/jqcm.2019.11.1.464

Abstract.

As a significant number of applications in mobile transactions and wireless sensor networks are characterized by short duration sessions, security issues turn into a focal concern.

RC4 algorithm is a standout amongst the most broadly utilized stream ciphers which locates its application in numerous security conventions, for example, Wired Equivalence Privacy (WEP) and Wi-Fi Protocol Access (WPA).

In this paper, we suggest a lightweight variation of the well-known RC4 algorithm that is exceptionally appropriate for resources of computational compelled gadgets and energy in remote systems, when contrasted with RC4 and its variations like, HC128, Grain-128, and so on.,. We propose new PRGA which is replaced the PRGA keystream generation algorithm of RC4.

The proposed LRC4 execution is surveyed in terms of randomness test and time under an arrangement of analyses. The trial comes about demonstrate that the resulting stream are random, and the suggested algorithm quicker compared to standard RC4, the results indicate the average of speed improvement is about 54% in both encryption/decryption sides.

Keywords: Random Number Generator, Stream Cipher, Key Scheduling Algorithm, RC4, Lightweight cryptography .

1. Introduction

The computing devices utilized as a part of an extensive class of remote correspondence systems, for example, cell phones, Internet of Things (IoT), body area networks (BANs), remote sensor systems (WSNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), and so on., are little and asset compelled. To guarantee the security of information correspondence sessions in such systems, Stream ciphers algorithms have been used. In particular, hardware stream ciphers and software stream ciphers are the two sorts of stream ciphers each of them contingent upon the stage most suited to their execution[1].

One of the stream ciphers algorithms, Ron Rivest outlined the RC4 algorithm in 1987 but the algorithm kept mystery until the point that it was as often as possible to the cypherpunks mailing list in 1994. RC4 is the most satisfactory stream cipher; it is utilized as a part of numerous web conventions, for example, Wireless Protected Access (WPA), Wired Equivalent Privacy (WEP), and Secure Socket Layer/ Transport Layer Security (SSL/ TLS) [1]. It is likewise utilized as a part of use, for example, Skype. RC4 proves its efficiency in both hardware and software and speed. It is extremely straightforward and quick equivalent to other encryption algorithms. RC4 algorithm predominantly comprises of two phases: the KSA (Key Scheduling Algorithm) to produce, from the key, an initial permutation of the S array and the PRGA (Pseudo Random Generation Algorithm) to create the key stream[2].

RC4 is as yet the most famous stream cipher algorithm because of its straightforwardness, speed, and simplicity of usage although more secure and efficient stream ciphers have been found after it [1].

2. Related Work

Numerous researchers have endeavored to upgrade the security of RC4 and make variation algorithms. However, this improvement impeded the execution speed. On the other hand, many researchers have attempted to improve algorithmic speed, but this caused a decrease in the randomness [3].

Jian et al, 2010 [3] introduced an enhanced RC4 in [3] . They improved the speed of RC4, and security. However, regardless of whether the enhanced RC4 in [3] has different escape clauses stays to be tried.

Weerasinghe, 2013 [4] proposed algorithm it is cost-effective than the first RC4 and different changes of RC4 utilized as a part of the examination. Since there are numerical qualities to portray the security level of the ciphers, anyone can get a major picture of the secrecy of the pertinent ciphers. Higher estimations of mystery areappeared by the new stream cipher, which implies the randomness of the cipher is higher than that of others, which is highlight of a decent cipher. The explanation for having a higher secrecy can be the expanded number of more activities and modifications in the PRGA.

Nishith et al, 2014 [5] The algorithm proposed in [5] enhanced the security of Improved RC4 algorithm by forcing substitution, along these lines changing over it into an item cipher. Time taken for encryption and decryption utilizing the proposed algorithm is hardly more than the Improved RC4 Algorithm.

Maytham et al, 2015[6] to solve the powerless keys issue of the RC4 utilizing a random introduction of inward state S. An arbitrary starting state (RRC4) was used to produce RC4 algorithm. Additionally, two state tables (RC4-2S) were used to propose RC4 algorithm. At long last, [6] they proposed RC4 algorithm with two state tables to create four keys (RC4-2S+) in each cycle which additionally upgrades randomness over RC4-2S and RRC4.

Sarab et al, 2016 [2] to overcome the weakness of the key scheduling algorithm of the original RC4, they presented a new modified key scheduling algorithm. The modified algorithm enhances the secrecy of the ciphertext especially when the key size is small and proves to be more random than the original RC4. Furthermore, the time of encryption of both algorithms is comparable.

Soumyadev et al, 2017 [1] They proposed a lightweight stream cipher algorithm. The suggested algorithm secure as Grain-128, orginal RC4 and other stream ciphers with regards of wireless applications that utilization short sessions.

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

3. Description of RC4

RC4 picks a cluster (S_{box}) and a secret key (K), the cluster known as Sbox which includes N (N=2^n) (N=256, where n=8). KSA and PRGA are two algorithms contained in RC4 algorithm [4].

A variable key length is used in RC4, which runs between (0-255) bytes for instating 256-byte array in the underlying state by components from S_{box} [0] to S_{box} [255] [3]. The KSA uses the symmetric key to permute an array S containing 256 entries. S array is initialized with identity permutation ranging from 0 to 255,(As suggested in [2][1] RC4 must utilize a key longer than 128 bytes). Then, a 256-iteration loop is utilized to produce a random permutation of the exhibit S, where the entries of the S array are continually swapped using the key value[2].

Algorithm of KSA:

set N ← 256
set ki to 0
while (true)
begin
S_{box} [ki] ← ki
ki←ki+1
end while
set kj←0
set ki←0
while (true)
begin
kj← (kj+S_{box} [ki]+k[ki]) Mod N;
swap(S_{box}[ki],S_{box}[kj])
ki←ki+1
end while

Figure 1: KSA of RC4

The objective of PRGA is to create a sequence of key stream. In the PRGA, two indices ki, kj are initialized to zero. In each iteration, ki is recomputed as (ki+1) and kj is recomputed as (kj+S_{box} [ki])mod 256 , and then a swap operation is conducted between S[ki],S[kj]. The key stream that is XORed with clear-text is generated as (S_{box} [(S_{box} [ki]+ S_{box} [kj]) mod 256) [1][2][6].PRGA steps show in figure2 :

Algorithm of PRGA:

set N←256
set ki←0
set kj← 0
while (generate key-stream)
begin
ki←ki+ mod N;
kj←kj+S_{box} [ki]mod N
swap(S_{box} [ki], S_{box} [kj])
Output←S_{box} [(S_{box} [ki]+ S_{box} [kj]) mod N]
end while

Figure 2: PRGA of RC4

4. Proposed Algorithm

In this paper, we produce an efficient stream cipher algorithm which is a lightweight compare to original RC4. The propose algorithm bring down cost of computational overhead when compared with the ordinary stream cipher like RC4. The suggest lightweight algorithm is sufficiently secure for use in many low term wireless communication application situations.

For creation of the random initial permutation S, utilize the KSA algorithm (first Algorithm) from RC4, but supplant the PRGA of RC4 new PRGA(lightweight PRGA). Lightweight PRGA is utilized for keystream creation from the (S_{box}) the input permutation (result from KSA). The new PRGA algorithm shows in figure3:

Proposed PRGA Algorithm:

set ki←0
set kj←255
set t←0
for ki←0 to N-1 **do**
begin
t← (S_{box}[ki]+ S_{box} [kj]+kj) mod 256
kj←ki
ki←S_{box} [ki]
S_{box} [kj] ←t
Output Z←S_{box} [ki] XOR S_{box} [kj]
end for

Figure 3: Proposed PRGA Algorithm

The yield of the PRGA algorithm is a key arrangement that will be XORed with cleartext/ciphertext) to get the ciphertext/cleartext.

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

5. Simple Example

Key= "password"

Plaintext= "mymessag"

Table1: Simple LRC4 example

S[i]	S[j]	Key-stream	Plaintext	Cipher-text
249	91	162	207	109
167	84	243	138	121
26	71	93	48	109
252	90	166	195	101
112	253	141	254	115
99	135	228	151	115
25	230	255	158	97
45	111	66	37	103

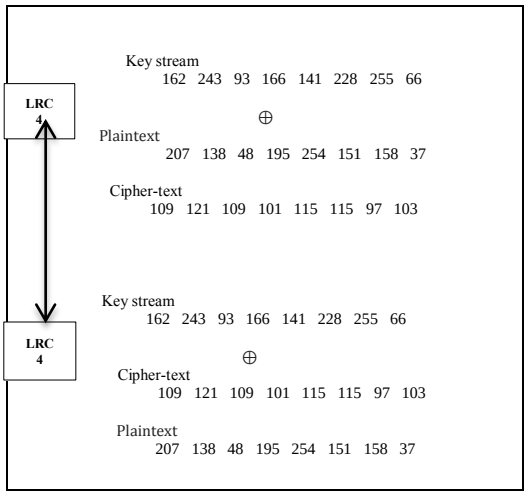

Figure 4:Simple example

6. Performance Evaluation

Different criteria can be used to measure the security level and performance of a given encryption algorithm. In this paper, two measurements: the randomness test of NIST (the National Institute of Standards and Technology) statistical test suite and time are utilized to assess the suggested algorithm.

6.1 Randomness Test

The statistical test suite (NIST) is the most broadly utilized one in the field of cryptography, which we have utilized for contrasting the standard RC4 and proposed LRC4 Algorithm. In this paper, three tests namely Approximate entropy, Run test and Linear complexity in the statistical test Suit are used to measure the randomness of the cipher-text created from RC4 and proposed lightweight RC4.In the wake of applying the NIST test suite, we use 10 random keys to test algorithms as showing in table2.

In this paper, the significance level, (p-value) is set to 0.01. The statistical tests suit (NIST) results indicates success of output (ciphertext) of all tested algorithms. In other words, all the test type of statistical test Suit are adequate and have good randomness for the two tested algorithms.

Table2: NIST Tests Applied to Standard and Modified RC4 Algorithms.

KEY	Standard RC4			Proposed LRC4		
	Approximate entropy	Run test	Linear complexity	Approximate entropy	Run test	Linear complexity
AEDW	0.021265	0.475773	0.955719	0.0553588	0.690328	0.6766
FmADDwerdf	0.075948	0.723729	0.808846	0.222083	0.166203	0.8088
0eey6tw453f15d2154f16a6883c	0.27209	0.7045	0.42319	0.09743	0.36818	0.8395
32881e0435a3137f6309807a88da234	0.099388	0.88353	0.398762	0.481929	0.678082	0.8088
2232d95de24a1b6b79fad3b37a427ea0	0.077827	0.523502	0.398762	0.062620	0.3722	0.1394
3040fa18f19085986569822223fa2dd8d	0.028795	0.523378	0.902774	0.418634	0.109129	0.3798
ndgekh77f1128598656982223ra2yt6d	0.018869	0.924253	0.320847	0.06648	0.497926	0.7306
34uiaff70eey67cpl6d2154f16a6441w	0.050375	0.533358	0.186466	0.609536	0.664365	0.1173
3uidd670eey655rt6d215wetr4a4kms2	0.2424	0.93857	0.46154	0.5826516	0.546237	0.7804
2b28ab097eaef7cf15d2154f16a6883c	0.408949	0.543813	0.962877	0.905865	0.925194	0.8929
Average	**0.129591**	**0.67744**	**0.581978**	**0.350259**	**0.50178**	**0.6174**

6.2 Encryption Time

We used different size of text files to test the speed of the proposed algorithms, and we compared the calculated time of both the standard RC4 with lightweight RC4.

Table3:Encryption time in second

File Size	Standard RC4	**Modified LRC4**
1.00 kb	0.00347	**0.00148**
2.01 kb	0.00433	**0.00262**
20.0 kb	0.04263	**0.024217**

In this evaluation step we have tested several files in order to prove that how fast the modified LRC4 algorithm than the standard RC4.

According to this test, we can indicate that the modified LRC4 (Lightweight RC4) algorithm is faster than standard RC4 algorithm and the results indicate the average of speed improvement is about 54% in encryption/decryption sides.

7. Conclusion

We have introduced a lightweight stream cipher algorithm and secure as original RC4. This paper presents a new modified PRGA algorithm to produce lightweight RC4 algorithm compared to the original RC4. Proposed algorithm is efficient; in other words, it is cost-effective than the standard RC4 and it is faster, The generated output sequences of proposed algorithm has passed the NIST suite of statistical tests. This makes the proposed LRC4 to a great degree appropriate for actualizing secure correspondence in a wide range of wireless applications like: Wi-Fi Protocol Access (WPA), where devices are compelled by either cost, energy or processing ability.

Reference:

[1]: S.Maity, K.Sinha and B.P. Sinha, "An Efficient Lightweight Stream Cipher Algorithm for Wireless Networks", IEEE , 2017.

[2]: S.M.Hameed and I.N.Mahmood, "A Modified Key Scheduling Algorithm for RC4", Iraqi Journal of Science, Vol. 57, No.1A, pp: 262-267, 2016.

[3]: J.Xie and X.Pan, "An Improved RC4 Stream Cipher", International Conference on Computer Application and System Modeling, IEEE, pp.156-159, 2010.

[4]: T.D.B Weerasinghe, "An Effective RC4 Stream Cipher", IEEE 8th International Conference on Industrial and Information Systems, pp.69-74, 2013.

[5]:N. Sinha, M.Chawda and K.Bhamidipati, "Enhancing Security of Improved RC4 Stream Cipher by Converting into Product Cipher", `International Journal of Computer Applications (0975 – 8887) Volume 94 – No. 18, pp.17-21, May 2014.

[6]: M.M.Hammood, K.Yoshigoe and A.M.Sagheer, "Enhancing Security and Speed of RC4", International Journal of Computing and Network Technology, ISSN 2210-1519, pp.37-48,2015.

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

خوارزمية ريفست 4 خفيفة الوزن

مصطفى مجيد عبدزيد سكينة حسن

الجامعة التكنولوجية ، قسم علوم الحاسوب

المستخلص:

نظرًا لتميز عدد كبير من التطبيقات في معاملات الجوّال وشبكات الاستشعار اللاسلكية بجلسات قصيرة المدة ، تتحول مشكلات الأمان إلى قلق محوري.

خوارزمية ريفست٤ هي من ابرز الخوارزميات المستخدمة على نطاق واسع والذي يحدد تطبيقها في العديد من الاتفاقيات الأمنية ، على سبيل المثال Wired Equivalence Privacy (WEP) و Wi-Fi Protocol Access(WPA).

في هذه الورقة ، نقترح تباينًا خفيفًا لخوارزمية ريفست٤ المعروفة والتي تعتبر مناسبة بشكل استثنائي لمصادر الأدوات الحاسوبية والطاقة في الأنظمة البعيدة ، عندما يقارن مع RC4 واقرانها مثل: HC128 ، Grain-128 ... الخ. اقتراحنا خوارزمية PRGA جديدة والتي تستبدل الخوارزمية الموجودة لتوليد المفتاح في ال RC4الاصلية.

تنفيذ الخوارزمية المقترحة تم فحصها من حيث اختبار العشوائية والوقت. اثبتت التجربة أن التدفق الناتج عشوائيًا للخوارزمية المقترحة ،وهي أسرع مقارنةً بالخوارزمية الاصلية ، حيث اثبتت النتائج ان معدل تحسن السرعة هو حوالي ٥٤%.