Al-Kitab Journal for Pure Sciences (2024); 8(2):31-47.
https://doi.org/10.32441/kjps.08.02.p4

Al-Kitab Journal for Pure Sciences
ISSN: 2617-1260 (print), 2617-8141(online)
https://isnra.net/index.php/kjps

Simulation of RC5 Algorithm to Provide Security for WLAN, Peer-to-Peer

Nasser Alwan Hussein*

Computer of Engineering Networks, College of Fine Arts, University of Diyala, Iraq

Corresponding Author: am.naseeralwan@uodiyala.edu.iq

ORCID: 0009-0002-6342-0865

Citation: Hussein NA. Simulation of RC5 Algorithm to Provide Security for WLAN, Peer-to-Peer. Al-Kitab J. Pure Sci. [Internet]. 2024 June. 10 [cited 2024 June. 10];8(2):31-47. Available from: https://doi.org/10.32441/kjps.08.02.p4.

Keywords Cellular Automata, WLAN, programming languages C#, RC5.

Article History

Received	06	Apr.	2024
Accepted	25	May	2024
Available online	10	June	2024

Abstract:

Information security is a significant viewpoint in different areas of correspondence. This paper manages information encryption as large numbers of data correspondence rely upon encryption information. In this paper, another proposition of an information encryption framework has been presented. The framework can be partitioned into two stages; the primary stage centers around creating a top-notch Pseudo Irregular Number generator PRNGs utilizing rudimentary, intermittent, and crossover rules of cell automata CA. The framework recommends another mix of CA rules in an undertaking to give high arbitrariness and to work on the strength of the proposed cryptosystem. The subsequent stage creates the Improved Rivest Code 5 ERC5 calculations which utilizes the produced arbitrary Number Succession RNS with an end goal to reinforce the security and haphazardness of the first Rivest Code 5 RC5 Algorithm. The outcomes show that the proposed PRNGs in light of CA can create RNS with a high period which can reach more than 100000 keys without reiteration or string duplication. In addition, the test exhibits that the proposed ERC5 works on the security of the first RC5 calculation. The proposed cryptosystem is assessed as far as Shannon's hypothesis of data entropy, irregularity tests, calculation time, and key space investigation. The outcomes confirm that the recommended information crypto-framework expands the development of the security

level of unique RC5 encryption calculation with a serious level of arbitrariness and privacy. It is executed this work to show the results rely upon the programming language C# and the correspondence was presented in a structure called disseminated through an association wireless local-area network WIFI.

Keywords: Cellular Automata, WLAN, programming languages C#, RC5.

محاكاة خوارزمية RC5 لتوفير الأمان لشبكة WLAN، الند للند

نصير علوان حسين

هندسة شبكات الحاسوب، كلية الفنون الجميلة، جامعة ديالى، العراق

am.naseeralwan@uodiyala.edu.iq

الخلاصة:

أمن المعلومات هو جانب مهم في مجالات الاتصالات المختلفة، يتناول هذا البحث تشفير البيانات حيث إن الكثير من اتصالات المعلومات تعتمد على تشفير البيانات، في هذه الورقة، تم تقديم اقتراح جديد لنظام تشفير البيانات. يمكن تقسيم النظام إلى مرحلتين؛ تركز المرحلة الأولى على إنشاء مولد أرقام عشوائية زائفة *PRNGs* عالي الجودة باستخدام القواعد الأولية والدورية والهجينة للأتمتة الخلوية *CA* يقترح النظام مجموعة جديدة من قواعد *CA* في محاولة لتوفير عشوائية عالية وتحسين قوة نظام التشفير المقترح. بينما تنتج المرحلة الثانية خوارزميات *Rivest Cipher 5 ERC5* المحسنة التي تستخدم تسلسل الأرقام العشوائي *RNS* الذي تم إنشاؤه في محاولة لتعزيز أمان وعشوائية خوارزمية *Rivest Cipher 5 RC5* الأصلية، أظهرت النتائج أن *PRNGs* المقترحة المعتمدة على *CA* يمكن أن تولد *RNS* بفترة عالية يمكن أن تصل إلى أكثر من ١٠٠٠٠٠ مفتاح دون تكرار أو تكرار السلسلة، علاوة على ذلك، يوضح الاختبار أن *ERC5* المقترح يعمل على تحسين أمان خوارزمية *RC5* الأصلية. تم تقييم نظام التشفير المقترح من حيث نظرية شانون لأنتروبيا المعلومات، واختبارات العشوائية، وزمن الحساب، وتحليل الفضاء الرئيسي، أثبتت النتائج أن نظام تشفير البيانات المقترح يزيد من نمو مستوى الأمان لخوارزمية التشفير *RC5* الأصلية بدرجة عالية من العشوائية والسرية، تم تنفيذ هذا العمل لإظهار النتائج بالاعتماد على لغة البرمجة *C#* وتم إدخال المراسلات في إطار يسمى الموزع من خلال منظمة الشبكة المحلية اللاسلكية *WIFI*.

الكلمات المفتاحية: الأتمتة الخلوية، شبكة الاتصال اللاسلكية المحلية، اللغة البرمجية # C، خوارزمية RC5.

1. Introduction:

With the development of the web, the security of data is acquiring more interest. The encryption strategies can effectively defend individuals' data communicated over open channels. Nonetheless, the traditional encryption frameworks have limitations in scrambling like low productivity, massive information, and the high relationship among examples, etc. **[1]**. Recently, cell automata have accomplished an extraordinary interest in managing the tricky of profoundly and quickly secure cryptosystems. Cell Automata (CAs) are profoundly circulated

and equal frameworks that can imagine refined ways of behaving [2]. The extensive variety of CA rules works with numerous ways of producing successions; additionally, cell automata are sorted out by just simple and basic rationale calculations with complex and pseudorandom ways of behaving. Creating great quality Random Number Arrangement (RNS) is certainly not a simple capability, Pseudo Random Number Generator (PRNGs) based CA draws in numerous specialists since they are not difficult to execute in both equipment and programming [3]. Cell robotization resembles a machine, and that implies that the information is set; the CA will utilize it to create a result. The advantages of cell automata in cryptography can be summed up as follows:

- Enormous development of rules space.
- Cell automata contain just rational tasks or whole number math, so these attributes lead to improving the calculation.
- Cell automata have parallelism and show complex ways of behaving.

Likewise, RC5 is a renowned block figure recognized for its speed, straightforwardness, reasonableness for programming and equipment execution, and low memory necessity. Besides, RC5 is a defined calculation and iterative in its plan. This gives the possibility for limitless adaptability in both the degree of safety and execution qualities [4]. In this paper, an upgrade technique for RC5 encryption calculation has been proposed by reinforcing its unique powerless keys through producing great quality irregular number arrangements by one rudimentary, occasional, and half and half CA. The remainder of the paper is coordinated as follows: related works are summed up in Segment 2. Segment 3 gives fundamental hypothetical meanings of cell automata while Area 4 creates a clarification of RC5 encryption calculation. Segment 5 gives a point-by-point portrayal of the proposed framework though Area 6 examines the security examination and consequences of the proposed calculations. At last, the primary end is summed up in Segment 7.

2. Related Works:

2.1 In 2009: Ho et al. [5] have endeavored to figure out the ideal mix of CA rules and coherent activities for picking von Neumann neighbors. The creators propose a different number of CA rules for phenomenal effect and presumed that the occasional limit is superior to the invalid limit. The creators come up short/pass rate among occasional and invalid limit conditions. Moreover, they reasoned that the non-uniform CA has a preferable impact over uniform CA.

2.2 In 2011: Osama [5] improved the RC5 block figure calculation considering turmoil for accomplishing higher security and better picture encryption. This was accomplished by

consolidating the cryptographic crude tasks and the tumultuous slant tent guide to foster another design for the key timetable, as well as the weighty utilization of information subordinate turns expanded the dissemination accomplished per round. The framework gives quick block figures other than high-security levels.

2.3 In 2014: Dogaru Radu et al. **[6]** thought about numerous answers for building a decent Pseudo Random Number Age (PRNG) for a cryptographic framework. The framework depends on half and half-cell automata (HCA). The primary arrangement depended on making chains of HCA, for example, the non-direct guide which changed powerfully was constrained by another HCA map inside a chain (to guarantee the greatest throughput). The subsequent arrangement depended on a solitary HCA yield, which was down-examined by an element D. The proposed plot furnishes a decent PRNG with low intricacy achievements. Besides, the framework is expected to have a high resistance to various kinds of assaults.

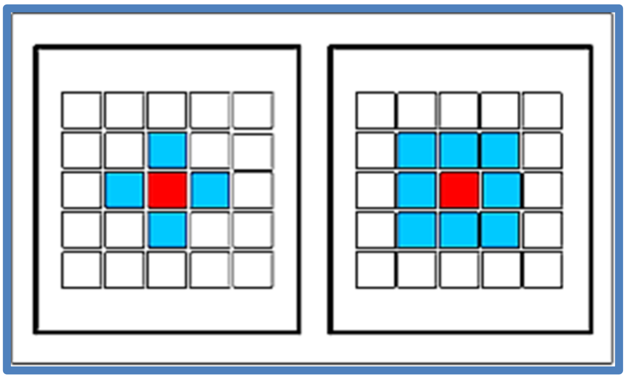
3. Cell Automata:

The CAs are a sort of dynamical framework that have been really and extensively used in major areas of strength to develop by taking the benefits of their arbitrariness and dynamical properties, with the ability to uncover flighty and a complex way of behaving **[7]**. A cell robotization incorporates a cross-section (lattice) of indistinguishable cells inside a Boolean incentive for every cell, referenced as the present status of the cell. The condition of every cell is refreshed at a discrete time step as per a nearby update rule. The same decimal of the 8 results is called 'rule' **[8]**. Cell robot is formed by the four following snippets of data: A letter in order (S): The restricted arrangement of every single adequate state. A cross-section (ι): an arranged matrix, ordinarily Zd, with a d-layered grid and d ϵ Z+. An area (N): a limited efficient sub-set of ι. A nearby progress capability or rule (f): The following conditions of every cell are chosen by its standard **[9]**. CA cross section can be created by two primary capabilities, nearby and worldwide. In the neighborhood progress capability: SN $\rightarrow$ S, SN addresses the arrangement of all potential expresses that the area can be in, with every one of the qualities as a tuple of states (S0, S1, S2, …, SN - 1), with Si ϵ S. For instance, if S= {0, 1} and |N| = 3, SN can be addressed by the set {(0,0,0), (0,0,1)..., (1,1,1)}. The nearby progress capability (rule) decides how the condition of every cell is transformed from a moment to the following. This choice is normally founded on the cell's present status and of its neighbors. In the worldwide capability, if c is considered as the ongoing design of the automata with c ϵ Zd. The CA's next setup is given by ϕ(c), where ϕ: $\sum$ Zd $\rightarrow$ Zd. ϕ Called a worldwide guide or worldwide capability. The CA's transient advancement is then, at that point:

$$c \rightarrow \phi (c) \rightarrow \phi 2 (c) \rightarrow \ldots \quad (1)$$

The name of the grouping c, ϕ(c), ϕ2 (c)… is the circle or populace of c. The cell neighborhood of a cell comprises itself and the encompassing (nearby) cells [10]. There are two essential kinds of CA aspects [8]: One-layered (1D) CA where every cell has two potential states and a cell's neighbors are the nearby cells on each side of it. Figure.1 exhibits the 1D CA. 2D CA has a portion of the comparative elements as does 1D CA. Two fundamental sorts of areas are for the most part pondered. The principal type is the Von Neumann neighborhood which comprises the 4 or 5-cell exhibit considering whether the focal cell is counted. The subsequent kind is the Moore neighborhood which comprises the 8 or 9-cell cluster considering whether the focal cell is counted. **Figure 1** shows the Von Neumann Area and Moore neighborhood [11].

Figure 1: One-dimensional Cellular Automata [11]



(a) Von Neumann neighborhood **(b) Moore neighborhood**

Figure 2: Two-dimensional Cellular Automata [11]

3.1 Rudimentary Cell Automata: A neighborhood of a cell x with sweep r is the arrangement of the r cells both to the left and right of x, including cell x. An ECA is any cell automata with r=1 and a paired state set S = {0, 1}. The condition of ECA can be as per the following:

$$X_i^{t+1} = f\,(x_i^{t-1}, x_i^{t}, x_i^{t+1}) \quad (2)$$

Where X_i^t is the cell's state, X_i^{t+1} is the cell's next state, x_i^{t-1} is the condition of the cell's left neighbor, x_i^{t+1} is the condition of the cell's right neighbor and *f* is the standard capability. 1D ECA is an extraordinary class of discrete dynamical frameworks shaped by a limited 1D exhibit of N cells. The all-out number of rules for span r area is 2^n where $n = 2^{nr+1}$**[12]**. Hence, ECA has $2^{23} = 256$ potential guidelines **[10]**.

3.2 Limits of Limited Grids: Endless CA has no limits accounts related to them. At the point when we are managing CA with a limited *ι*, the area utilized by the nearby change capability surpasses the cross-section limits. There are essential answers for this issue: Invalid limit CA, in an invalid limit where the CA contains - cells as *X1, X2, Xn,* the furthest left neighbor of *X1* and the furthest right neighbor of *Xn* are considered as zeros for every one of them. Additionally, on the off chance that *Xn* is taken as the furthest left neighbor of *X1* and *X1* is taken as the furthest right neighbor of *xn* then it is called cyclic or intermittent limit CA **[8]**.

3.3 Sorts of CA Reasonable for Cryptography: There are many kinds of CA appropriate for cryptography, if phone mechanization uses some control signals, it is known as Programmable Cell Automata (PCA) **[12]**. If CA generally gets back to its underlying state, it will be called Reversible Cell Automata **[13]**. What's more, if similar principles decide the following piece cells of CA, it is called uniform CA in any case it is called non-uniform CA or Crossbreed Cell Automata (HCA) **[14]**. The HCA creates more intricate examples than a uniform cell machine. This property is exceptionally valuable on account of cryptography, as it will create more complicated figures **[15]**.

4. Rivest Code 5 (Rc5) Algorithm:

RC5 is a block, symmetric key encryption calculation; its basic plan makes it proper for execution in programming and equipment. RC5 has a serious level of adaptability as far as security and execution because of its adaptable choices, for example, factor key size which chips away at 0 up to 2040 pieces, variable block size 32-, 64-, or 128-piece blocks of information) and variable (0 to 255) **[4]**. The boundaries of RC5 are as per the following: w alludes to the block size, r alludes to the quantity of rounds and b alludes to the vital length in bytes, essentially composed as RC5-w/r/b. Ronald L. Ronald L. Rivest demonstrates that the more noteworthy the security/encryption level when the higher the number of rounds **[16]**. the general plan of RC5 is separated into 3 phases: key development, encryption stage, and unscrambling stage. The critical activities in these three phases are Spot-wise XOR of words, expansion of words modulo 2w, and change in two courses left (<<) and right (>>).

5. Core Requirements

The proposed framework can be restated into two stages, the primary stage is planned as a pseudo-random number generator given the cell automata stage, though the subsequent stage is made from the improvement of the RC5 encryption stage. In **Figure 1**, the general design of the proposed Simulation RC5 Algorithm is based peer to peer.

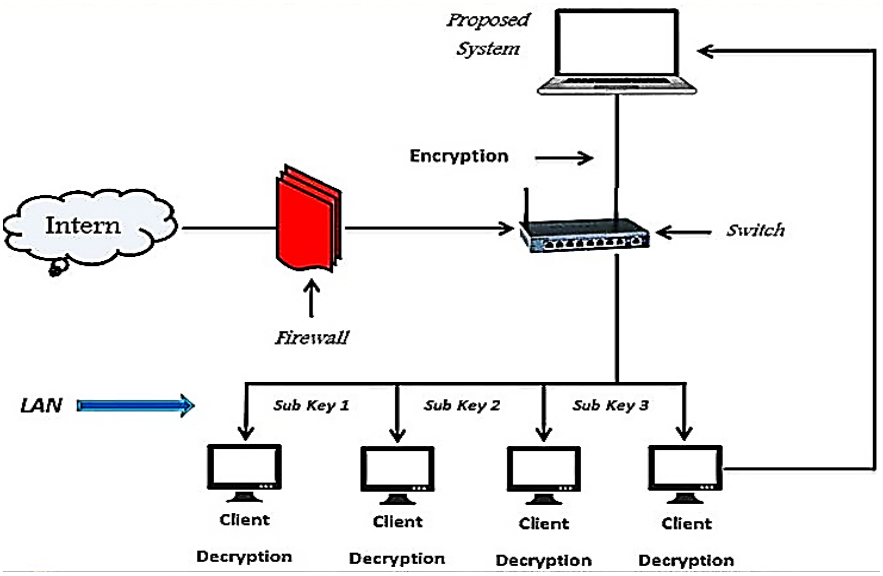


Figure 3: The design of the proposed Simulation RC5 Algorithm based peer to peer (SRPP)

5.1 Stage One: Plan a Pseudo Random Number Generator In light of Cell Automata:

In this stage, a symmetric key cryptographic strategy utilizing CA has been executed through Pseudo pseudo-random number Generator In light of Cellular Automata (PRNGs-CA). The calculation utilizes rudimentary, occasional, mixture, and programmable CA with rules set specifically 30, 90, and 150 CA to shape a succession of 128-cycle irregular numbers. The PRNGs calculation can be separated into three sections as roar:

5.1.1 Producing Starting Seed: The Underlying Random Seed (URS) of the framework is characterized by creating an arbitrary string made from 1024 characters. Then, the irregular rings pass to the MD5 calculation to produce the URS which comprises 128 pieces (16 bytes) that are addressed because of MD5". The motivation behind passing the string to the MD5 calculation is to guarantee that it is infeasible to deliver two messages having a similar hash esteem or to create any URS having a given pre-characterized target message digest, in this manner expanding the strength of the URS to makes the beast force assault more troublesome.

5.1.2 Rule Planning System: to make the CA a PCA, this part has been applied to build the strength of the calculation and make the cryptanalysis more troublesome. The standard planning calculation includes picking which rules set of CA would be applied to the blocks of produced

RNS (as of now eight principles sets have been remembered for this study). Random Integer Number (RIN) is addressed as an irregular number with a worth somewhere in the range of 1 and 8. Then, at that point, the standards set will be picked in light of this RIN. For each sub-key (depicted in subtleties by the following sub-area), the worth of RIN will be changed, and, in this way, the standards set would be different with each sub-key. The principal objective of the standard booking calculation is to make cryptanalysis infeasible, thus expanding the framework's heartiness against assaults, and building the strength of the framework. **Table 1** shows which rules set will be applied considering RIN esteem. This blend of rules is utilized in the third part which comprises creating symmetric keys.

Table 1: RIN value and its corresponding rules set

RIN value	Rules set
A	30, 90, 30, 150, 150, 90, 90, 30
B	150, 30, 90, 150, 90, 30, 90, 90
C	30, 150, 30, 90, 150, 30, 150, 90
D	150, 90, 90, 30, 30, 30, 90, 150
E	30, 150, 150, 30, 30, 90, 90, 90
F	150, 30, 150, 30, 90, 90, 150, 90
G	30, 90, 150, 30, 150, 30, 90, 90
H	150, 30, 150, 90, 30, 30, 90, 90

5.1.3 Key Proliferation System: The major goals of the proposed key engendering instrument part are:

- The sub-keys ought to be a cryptographic pseudo irregular and impact-safe.
- Straightforwardness, ease, and effortlessness of execution.

In the proposed framework, the subsidiaries of the sub-keys are finished through URS (128 pieces) which is considered as an underlying example (seed) utilizing a crossover 1D occasional class of CA. The motivation behind utilizing 1D CA is to guarantee effortlessness and rapid of execution time.

5.1.4 Key proliferation steps:

- **Stage 1**: Consider URS as example #0.
- **Stage 2**: Separation design into blocks of 8 pieces (1-byte), for example, the example will be changed over into 16 blocks, 8 pieces for each (8bit *16 block=128-bit absolute example length).
- **Stage 3**: Info current example to the mixture CA machine, the cross-breed CA machine includes 16 rounds of the same rule planning for each block, for example creating an example of 128 pieces. Each piece of the current example addresses the cell's present

status xit of CA. For each piece, one of three change rules, 30, 90, and 150 is applied considering the choice of the rule booking system. The Crossover CA machine refreshes the cell's present status xit to the following state x_i^{t+1} by utilizing the cell's present status xit and two close nearby neighbors (left neighbor cell xti-1 and right neighbor cell x_t^{i+1}.

- **Stage 4**: The result of the half-and-half CA machine characterizes another example.
- **Stage 5**: Think about the new example as another sub-key.
- **Stage 6**: rehash steps (2, 3 4, and 5) until all the sub-keys are produced. This component of key development can produce sub-keys with an enormous period and high populace. **Figures 2**, **3**, and **4** show the key proliferation instrument and sub-keys blocks plan separately.

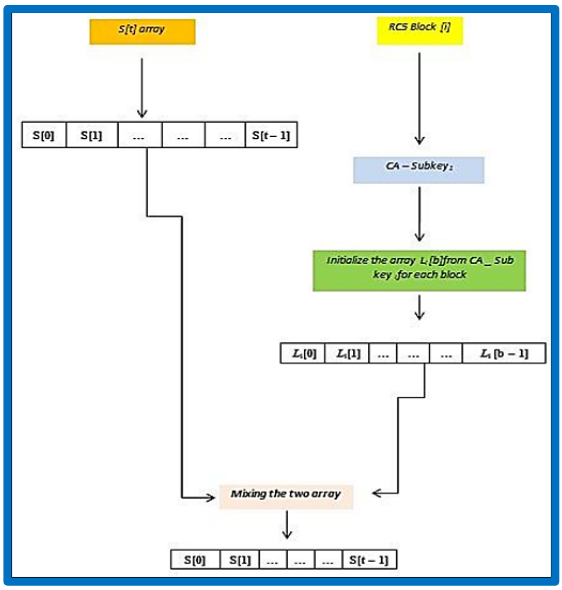


Figure 2: Block diagram of ERC5KS

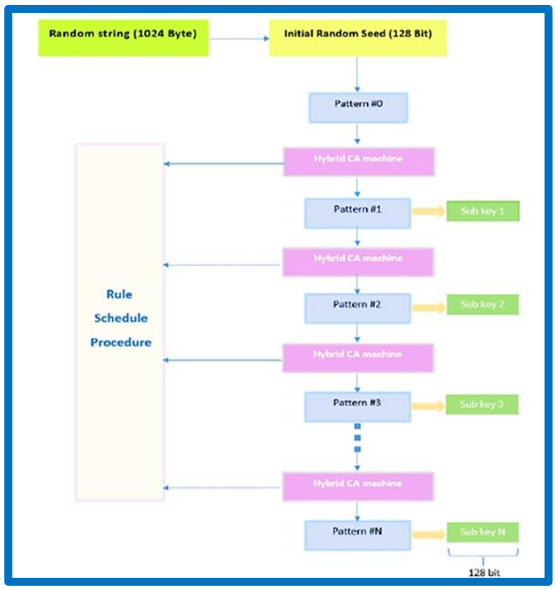


Figure 3: Key propagation mechanism

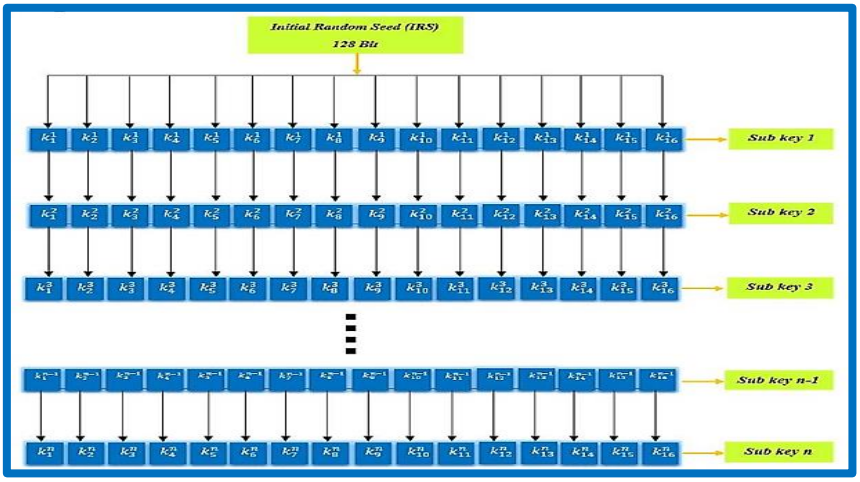


Figure 4: Sub-Keys Blocks Schedule

5.2 Stage Two: Upgrade of RC5 Encryption algorithm The first RC5 has frail keys and to supplant it with solid keys, a proposed Upgrade of RC5 encryption has been carried out as

follows: Improved RC5 Key Timetable 5.2.1: The calculation of Upgraded RC5 Key Timetable (ERC5KS) can be separated into 3 sections: the initial segment is introducing S cluster, the subsequent part is introducing L exhibit and the latter is the blending part, individually, as displayed in **Figure 5**.

- Instating S cluster: The S exhibit is introduced by the same method as the first RC5 key timetable.
- Instating L cluster: L exhibit of the proposed conspire is introduced with each block in the encryption cycle through various sub-keys which got from CA as examined in the past segment. The sub-keys size which produces L exhibit is 128-digit (16 bytes) for each.

5.2.1 Blending S and L exhibits: The two clusters S and L are blending by equivalent to the first RC5 blend capability, the main distinction is that the L exhibit is introduced with various sub-keys for each RC5 encryption and decoding block. Note that, as a unique RC5 calculation, due to the likelihood of getting various sizes of S and L clusters, the bigger exhibit is handled multiple times though the more modest exhibit might be handled more times.

5.2.2 Upgraded RC5 algorithm: The block size of the Enhanced RC5 (ERC5) is made of two words (identicalness to eight bytes), S exhibit is introduced exclusively toward the start of the encryption cycle. Though the L cluster is instated for each block of the wave information by CA sub-keys as referenced in the before segments, the remainder of the encryption calculation is equivalent to the first RC5. Encoding each block of information with various sub-keys reinforces the first RC5 frail keys making cryptanalysis more troublesome. *Note* that on the off chance that the information size isn't equivalent to 64-byte or to its products (block size is equivalent to 2 words, 32 bytes for each=64 byte), an important cushioning is added to the information cluster.

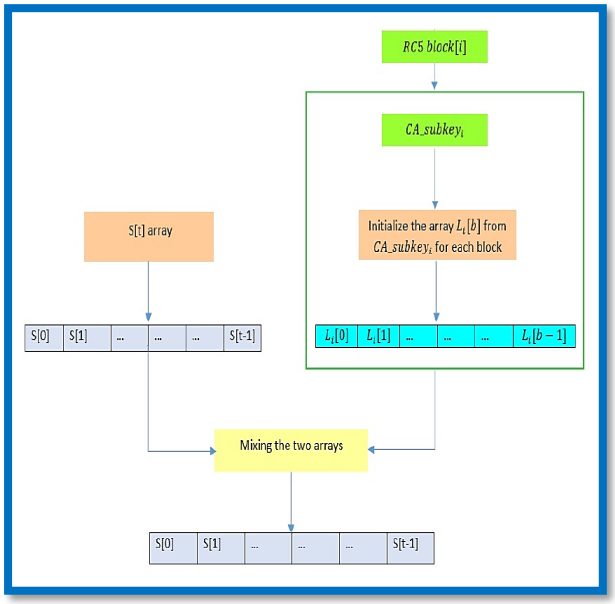


Figure 5: ERC5KS Scheme

6. Assessment Of the Proposed System:

The assessments of the proposed system have been run under Windows 10 Ace. Intel(R) Core(TM) i5-5200U computer chip @ 2.20GHz 2.20 GHz, 8 GB Arbitrary Access Memory (Slam), the framework type is 64-cycle Working Framework, 64x-based processor. C# programming language is used to foster the recommended framework (Visual Studio 2013).

6.1 Tracking down the Rules: to find the proficient standards that produce great PRNS to the proposed PRNGs, the framework tried the accompanying principles: 30, 45, 51, 60, 90, 102, 105, 150, 153, 165 and 195. In certain circumstances, a uniform cross-section was tried, while different reenactments assess non-uniform (half and half) CAs. All the previously mentioned rules were tried as uniform CAs thinking about the three most significant NIST tests. The framework additionally inspected numerous non-uniform principle sets like 30, 90,105 with 150 and 30, 45 with 150, and numerous others. That's what the outcomes show, for the most part, non-uniform CAs are preferable RNGs over uniform ones since a portion of these mixes finish some of NIST assessments and could produce RNS with an enormous intermittently. At long last, delivering an RNS with great quality and a wonderful period was the test of this paper, subsequently, the plan recognized that in more than 100 examinations, and three standards which gave the best outcomes would in general oversee the finishing up created grids: 30, 90, and 150. Notwithstanding the low effect of rule 90 on uniform CAs, it affects non-uniform CAs.

6.2 Consequences of Period and Factual Tests: The eight CAs rules set of the proposed conspire to show roughly the same execution level. The tests were applied to various ages, for example, numbers of produced sub keys (10,000, 32,000, 50,000, 75,000, and 100,000 ages were tried), and utilized similar starting worth to each of the tried standards set and measure of age. They all finished the three NIST measurable assessments. Likewise, they all created sub-keys with practically no duplication, and that implies that the proposed framework found an extremely enormous periodicity with p-values. This additionally implies that their age of arbitrary succession gives something to be searched for, wanted, and commendable. Accordingly; the outcomes show that the top-notch of the created RNS is adequate for some applications. **Table 2** sums up the normal p-upsides of the standard sets applied with various measures of age (note that if the p-esteem is more noteworthy than 0.01, it is considered fruitful). The table additionally shows the execution time for these ages. In this way, the applied rudimentary, non-reversible, crossbreeds, occasional, and programmable CAs give great and quick RNGs.

Table 2: Average (*P*-Value) and Execution Time of The Proposed System

No. of generated sub-keys	Execution time(Sec)	Average *P*-value			Status
		Frequency	Block	Run	Successful
10000	0.076	0.7480	0.5812	0.5797	Successful
32000	0.240	0.5410	0.3986	0.4841	Successful
50000	0.376	0.4832	0.4645	0.5173	Successful
75000	0.540	0.5672	0.6182	0.4264	Successful
100000	0.747	0.6562	0.4460	0.3115	Successful

6.3 Assessment of the Upgraded RC5 Algorithm: to make the RC5 calculation more grounded, it needs to remove its feeble keys and replace them with more grounded keys. While trying to do this assignment, the ERC5 calculation has been presented. The submitted conspire encodes each block of RC5 with an alternate key which was produced given CA as examined before. This calculation was embraced to mend the shortcomings of RC5 keys and to ensure progressed security notwithstanding present superior encryption. With the end goal of checking the strength of the proposed work, a few investigations have been preceded as follows:

1. Data Entropy Analysis: **Table 3** shows the entropies of the first record, RC5 and ERC5.

Table 3 :(1st and 2nd) Entropy of Original files, RC5 and ERC5

No	1st Entropy			2nd Entropy			
1	Name	Original Computer Test	Original RC5	ERC5	Original Computer Test	Original RC5	ERC5
2	Cmp1	6.1100	7.8440	7.9851	12.2032	15.6757	15.9662
3	Cmp2	7.0400	7.8440	7.9958	12.2032	15.6757	15.9890
4	Cmp3	4.9278	7.9933	7.9959	14.0678	15.9804	15.9891
5	Cmp4	7.6814	7.5664	7.9964	9.8500	15.1307	15.9906
6	Cmp5	5.3865	7.9957	7.9977	15.3592	15.9890	15.9935
7	Cmp6	2.9016	7.9973	7.9980	10.7175	15.9923	15.9945
8	Cmp7	6.3162	7.2883	7.9982	5.8009	14.5644	15.9953
9	Cmp8	6.5813	7.9982	7.9987	12.6156	15.9951	15.9965
10	Cmp9	6.8635	7.9985	7.9986	13.0806	15.9962	15.9966

From the above Table, the fruitful result of the ERC5 is clear through the upgraded consequences of entropy examination. At the point when the documents are enciphered, their first entropy ought to impeccably be 8 and the second entropy ought to be 16. On the off chance that the result of such a code produces figures with first entropy under 8 or potentially second entropy under 16, there exists a certain level of expectedness, which dangers its security. The higher the pace of entropy of enciphered, the better the security. **Table 3** explains that the outcomes accomplished from the proposed framework are exceptionally near the hypothetical worth of entropy contrasted with the first RC5. This implies that the data spillage in the encryption methodology is infeasible, and the encryption framework is secure against the entropy assault.

2. Irregularity Tests: to guarantee the nature of the proposed ERC5 over unique RC5, NIST tests were made, and the outcomes are displayed in **Table 4**. Likewise, **Figure 6** determines the achievement pace of each, the proposed ERC5 generally wins.

Table 4: NIST Tests Results of RC5 vs. ERC5

No	Name	Frequency		Block		Run	
		Original RC5	SRC5	Original RC5	SRC5	Original RC5	SRC5
1	Cmp1	0.0029	0.7732	0.8810	0.8361	0.0434	0.2168
2	Cmp1	0.0830	0.9971	0.1502	0.4969	0.7583	0.6603
3	Cmp2	0	0.6314	0	0.4069	0.3230	0.2911
4	Cmp3	0.3212	0.816	0.3719	0.3596	0.9565	0.5432
5	Cmp4	0.6776	0.9333	0.0056	0.3021	0.0391	0.9634
6	Cmp5	0	0.3880	0.8780	0.4393	0	0.6971
7	Cmp6	0.0736	0.3774	0.3571	0.2390	0.6038	0.8048
8	Cmp7	0.3080	0.5287	0.2287	0.959	0.5538	0.9564
9	Cmp8	0.0693	0.1284	0.99999	0.1481	0.000003	0.9712
10	**Success Rate**	1/9	8/9	4/9	5/9	3/9	6/9

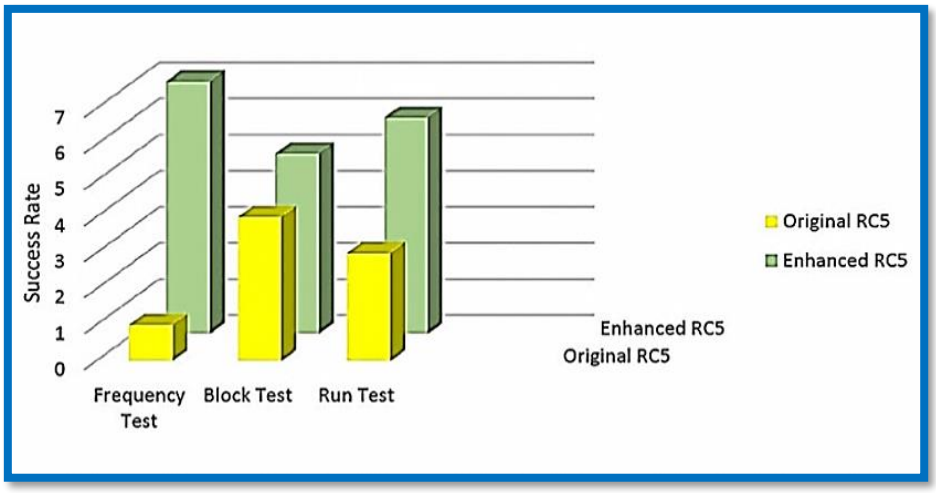


Figure 6: Achievement pace of frequency, block, and run tests for ERC5 versus original RC5

6.4 Execution Time: The accompanying table shows that the proposed framework is quite enough and can be utilized as an encryption framework.

Table 5: ERC5 Execution Time for the Proposed Encryption Framework

No	Name	ERC5 Execution Time (Sec.)
1	Cmp1	0.012
2	Cmp1	0.032
3	Cmp2	0.040
4	Cmp3	0.045
5	Cmp4	0.060
6	Cmp5	0.070
7	Cmp6	0.071
8	Cmp7	0.087

6.5 Key Space Investigation: A decent encryption calculation ought to be delicate to the code keys, and the keyspace ought to be sufficiently huge to make savage power assaults infeasible. For the proposed encryption framework, the key space investigation has been painstakingly examined and can be summed up as follows:

6.5.1 Key Responsiveness Examination: A significant element for a decent crypto-framework is a very key aversion to guarantee the security of the crypto-framework across the best force assault in an action. Key responsiveness of any crypto-framework can be identified in two different ways: First and foremost, the code created by any crypto-framework ought to be delicate to the key, for instance, if two-piece different mystery keys have been utilized to scramble a similar unique plain, then, at that point, the two produced figure keys delivered should be disengaged to one another. Furthermore, the code can't be unscrambled accurately regardless of whether there is only a tad variety among encryption and decoding secret keys. In the proposed encryption calculation, the figure relied upon each digit of the key, this reliance was accomplished by the upgraded RC5 stage, where each block of information relies upon the CA sub keys and each subkey of the CA stage relies upon the past key, significantly this reliance brings about making the framework's critical awareness as displayed in **Figures 7** and **8**. **Figure 8** shows different codes of the same plain encoded with two keys contrasts from one another in only the slightest bit while **Figure 8** shows that assuming the unscrambling keys vary in just a single piece from the encryption key, then the subsequent decoded is unique about the first plain.

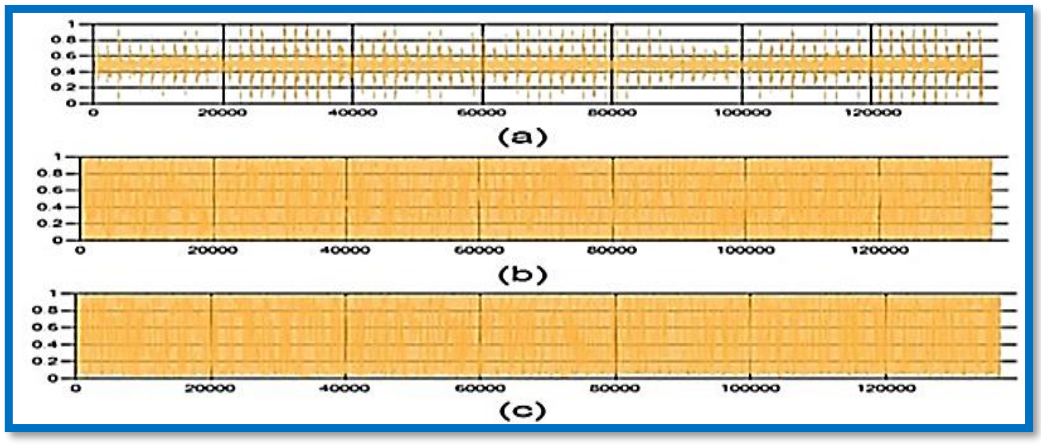


Figure 7: Simulation RC5 Algorithm by Waveforms

Figure 7 simulation RC5 algorithm by waveforms using blank plaintext for known correct cipher output of 0xb7c4b44a-9faa44d8, shown in above different encryption process for same document with two keys contrast from one another in only the slightest bit, (a) shows unique wave record before encryption and (b,c) shows a similar wave document encoded with the two keys.

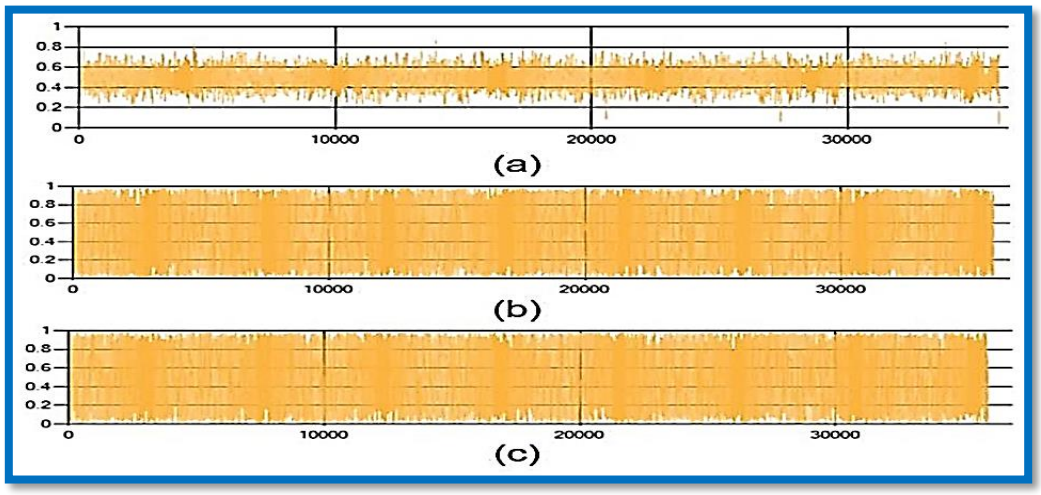


Figure 8: plot of waveform decoded with critical contrasts in just a single piece

Figure 8: At the higher plot of waveform decoded with critical contrasts in just a single piece from the first key. (a) Unique waveform plot. (b) The plot of the waveform is unscrambled with vital contrasts in just a single piece from the first key. (c) The plot of waveform unscrambled with a vital varies in just a single piece from the first key on one more situation from (b).

7. Conclusions:

This paper proposes an encryption framework given cell automata with an improved RC5 encryption algorithm. The primary finishes of this paper can be summarized as follows: The proposed framework found another blend of CA rules to create a strong RNS with a high populace and huge period, notwithstanding a high irregularity. In this way, recommended PRNGs expand the security of the calculation. Likewise, the improvement of RC5 calculation comes to reinforce the first RC5 frail keys and to solidify the first RC5 in terms of safety and irregularity by exploiting the proposed PRNGs given CA; these PRNGs are utilized as a one-time pad key for each block of information. The proposed framework is key touchy. This awareness is accomplished by the reliance of each block of the ERC5 stage on the created PRNGs-CA stage sub-keys. Additionally, the announced consequences of the proposed framework affirmed the positive impact on solidifying the force of unique RC5 in the two terms of the entropy and arbitrariness tests.

- Funding: None
- Acknowledgement: None
- Conflicts Of Interest: The Author Declares No Conflict of Interest.
- Availability Of Project and Codes

8. References

[1] Shahzadi R, Anwar SM, Qamar F, Ali M, Rodrigues JJ. Chaos based enhanced RC5 algorithm for security and integrity of clinical images in remote health monitoring. IEEE Access. 2019;7:52858-70.

[2] Alsaffar N, Elmedany W, Ali H. Application of RC5 for IoT devices in smart transportation system. In: 2019 8th International Conference on Modeling Simulation and Applied Optimization (ICMSAO); 2019 Apr; IEEE. p. 1-4.

[3] Vibar JCN, Medina RP, Sison AM. ERC5a–An enhanced RC5 algorithm on bit propagation in the encryption function. In: 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS); 2019 Feb; IEEE. p. 479-82.

[4] Abidi A, Sghaier A, Bakiri M, Guyeux C, Machhout M. Statistical analysis and security evaluation of chaotic RC5-CBC symmetric key block cipher algorithm. Int J Adv Comput Sci Appl. 2019;10.(١٠)

[5] Hossen MS, Islam MA, Khatun T, Hossain S, Rahman MM. A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem. In: 2020 International Conference on Smart Electronics and Communication (ICOSEC); 2020 Sep; IEEE. p. 676-81.

[6] Alenezi MN, Alabdulrazzaq H, Mohammad NQ. Symmetric encryption algorithms: Review and evaluation study. Int J Commun Netw Inf Secur. 2020;12(2):256-72.

[7] Wang Z, Yu B, Pei B, Zhang L. Research on AES encryption algorithm based on timestamp in Wireless Sensor Networks. In: 2020 2nd International Conference on Information Technology and Computer Application (ITCA); 2020 Dec; IEEE. p. 15-8.

[8] Yang C, Wu J, Wang L, Zhang X, Li L, Liu S. Smart grid monitoring systems based on advanced encryption standard and wireless local area network. IOP Conf Ser Mater Sci Eng. 2020;719(1):012056.

[9] Al-Ahdal AH. Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks. Turk J Comput Math Educ. 2021;12(12):133-43.

[10] Sagun A, Khaidurov V, Lakhno V, Opirskyy I, Chubaievskyi V, Desiatko A. Devising a method for improving crypto resistance of the symmetric block cryptosystem RC5 using nonlinear shift functions. East Eur J Enterp Technol. 2021;5(9):113.

[11] Valeriy L, Andrii S, Vladyslav K, Boris G, Petro K, Svitlana K. One method for RC5 algorithm's cryptographic strength improving. In: Soft Computing for Security Applications: Proceedings of ICSCS 2021. Singapore: Springer Singapore; 2021. p. 13-25.

[12] Ngamsert R, Kangrang A. Applying of marine predator's algorithm linked with reservoir simulation model considering sedimentation for reservoir operation. Adv Civ Eng. 2022.

[13] Hussein SN, Obaid AH, Jabbar A. Encryption Symmetric secret Key in Wireless Sensor Network Using AES Algorithm. Iraqi J Sci. 2022;5037-45.

[14] Sumathi M, Narmadha R, Anbarasi Jebaselvi GD. Performance comparison of data security algorithms. In: Human-Assisted Intelligent Computing: Modeling, simulations and applications. Bristol, UK: IOP Publishing; 2023. p. 33-1.

[15] de Carvalho Bertoli G, Suri R, Rizos A, Pereira DP. Open Challenge for Intrusion Detection on Air-Ground Communication: From Data Analysis to Simulation. In: 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC); 2023 Oct; IEEE. p. 1-9.