

Information security based on sub-system keys generator by utilizing polynomials method and logic gate

Khalid Kadhim Jabbar *

Hussain A. Hailal [†]

Aysar Thamer Naser [§]

Department of Computer Center

College of Education

University of Mustansiriyah

Baghdad 10046

Iraq

Abstract

Information security is the biggest and most complex problem at present because of its great impact on modern software in all fields. Therefore, many researchers are working to develop modern methods of protecting data from modification, theft or even accessing it in one way or another. As dealing with data is a very sensitive matter in terms of sending this data from one party to another through the internet or social media. The protection of that data requires the use of algorithms to encrypt or conceal the data with the proposed and used algorithms, and these algorithms work based on the proposed key exchange principle, so many of these algorithms need a key generator to work with other than the public key or private for encryption or decryption of the blade. Our proposed solution developed a key generation sub-system, as this system consists of two parts, the first part aimed to generate the first key (the first 64-bit subkey), while the second part (the second subsystem) will generate the second key (the second subkey is 64-bit). As the two sub-systems work to generate keys in different ways, the first system uses the principle of electronic gates to generate the keys randomly, while the second system uses binary text and LFSR. The idea in these sub-systems is that they work together in encrypting and decrypting data, requiring that the sender and receiver have the keys to complete the process. The results obtained from the two sub-systems show the power of protecting data from being read or decoded, as the

* E-mail: khalid_jabbar@yahoo.com;

khaledk.jabbar@uomustansiriya.edu.iq (Corresponding Author)

[†] E-mail: hussainabed342@uomustansiriya.edu.iq

[§] E-mail: acer_era@uomustansiriya.edu.iq

message consists of only a part of the key and the second part is at the receiver, which gives stronger immunity in this encrypted data.

Subject Classification: 68P30, 68U35.

Keywords: Information security, LFSR, Electronic gates, Encryption process, Decryption process.

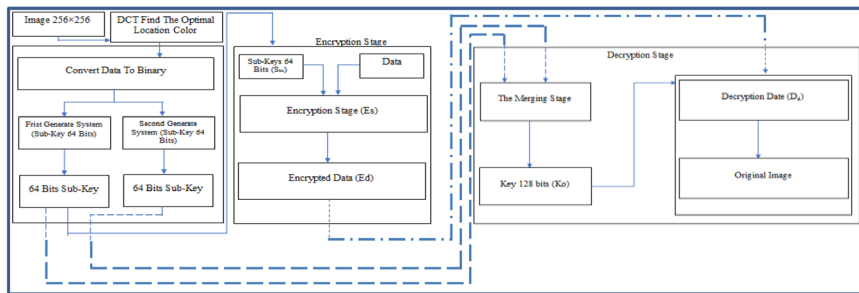
1. Introduction

Information security is the biggest and most complex problem at present because of its great impact on modern software in all fields [1]. Therefore, many researchers are working to develop modern methods of protecting data from modification or theft or even accessing it in one way or another. As dealing with data is a very sensitive matter in terms of sending this data from one party to another through the Internet or social media [2, 3, 4] and the protection of that data requires the use of algorithms to encrypt or conceal the data with the proposed and used algorithms, and these algorithms work based on the proposed key exchange principle, so many of these algorithms need a key generator to work other than the key is public or private for encryption or decryption the blade [5, 6, 7]. Our proposed developed a key generation sub-system, as this system consists of two parts, the first part aimed to generate the first key (the first 64-bit subkey), while the second part (the second subsystem) will generate the second key (the second subkey is 64-bit). As the two sub-systems work to generate keys in different ways, the first system uses the principle of electronic gates to generate the keys randomly, while the second system uses binary text and LFSR [8]. The idea in these sub-systems is that they work together in encrypting and decrypting data, requiring that the sender and receiver have the keys to complete the process. Whereas the encryption process requires the use of the first 64-bit private sub key [9], in decryption, the process requires the combination of the first and second keys to have one 128-bit key to complete the process. The sender and receiver must secretly exchange keys between them to complete the encryption and decoding process, depending on the key switching system.

2. The Proposed Method

Our state of the proposal can show in the figure below:

Figure 1 shows the main states of our proposed sub-system, as the first see that the data covert to binary, and the binary data go through the two subsystem keys, this means the keys are generators from the original



data giving more power to the keys, used the logic gate and the LFSR for permutation the bits also give the big deal when the keys go through the test randomness keys when showing the randomness of the keys.

There are two different systems used for keys generator, where each of these sub-systems are work differently for this purpose, these two systems can be explained below:

3.1 First System (First Sub-Keys 64 Bits)

3.2 The Second the Subsystem

[illegible]

(a): Round One (R0), Generate Random, (b): Round Two (RT), Generate Random, (c): Round Three (RTT), Generate Random

All the figures above stages work based on one system each, and eventually, you collect all those results in one range to get the keys of course all those resulting bits turn into hexadecimal illustrated in the following simple table of keys:

Table 1
Simple Hexadecimal keys with size of 128-Bits

980014 AA	82A0DD 2A	02A1DDD5	FFED1234	FFFCB2F1
BBCCEEDD	123ABFCD	EFEF1234	0000DFEC	ACF13323
FFFF5431	98AAAA76	1983DDDD	8765EFDA	ADCBEDFA
AEBDCFAD	15427938	091234AD	A13D5C7F	FFEDABA
1ACDEFA7	19834DCB	15362DFC	ADCEAF00	11872652
1FDEABA	ABCEDFAE	8AFCBE23	1245ACBD	18976DCE

4. The Results of Randomness Keys Generator

In actuality, only a few distinct forms of pseudo-random number generators have been employed, as shown in the following five experiments. [5]:

4.1 Frequency Experiment:

The purpose of this test is to locate whether the number of 0s and 1s in s is roughly equivalent to what would be predictable from a random sequence. Using n_0 and n_1 to represent the number of 0s and 1s in s , consecutively, the statistic is where the formula reads:

$$X_1 = (n_0 - n_1)^2 / n \quad (1)$$

4.2 Serial Experiment (Two-Bit Test):

As one might expect from a random sequence, the intent of this experiment is to locate whether the number of repeats of 00, 01, 10, and 11 as the suffix of s are nearly equal. Let n_{00} , n_{01} , n_{10} , and n_{11} indicate the digit of iterations of 00, 01, 10, and 11 in s and the number of repeats of 00,

01, 10, and 11 in s , consecutively. Notable is the fact that $n_{00} + n_{01} + n_{10} + n_{11}$ Equals (n_1) .

$$X_2 = 4/n - 1(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - 2/n(n_0^2 + n_1^2) + 1 \quad (2)$$

4.3 Poker Experiment:

Let m as integer with $[n / m] \geq 5$. (2mz. and $k = [n / m]$). Let N_i denote the number of instances of series types of length m , $1 \leq i \leq m$, and partition the series of S into k not overlap parts of length m . The poker test determines if sequences of length m happen in s with roughly the same frequency as random series.

$$X_3 = 2^m / K(\sum_{i=1}^{2m} n_{2i}) - K \quad (3)$$

4.4 Runs Experiment:

The test range is used to determine if the number of runs (of either zeros or ones) of varied lengths in the series S predictable corresponds to what would be expected in a random series of length n . $e_i = (n_i + 3) / 2i + 2$ denotes the predicted number of hiatus (or blocks) of length i . Let k be the greatest integer i such that e_i is smaller than 5. b_i, g_i represents the number of blocks and hiatus of length i in seconds for each $1 \leq i \leq k$.

$$X_4 = \sum_{i=1}^k \frac{(b_i - e_i)^2}{e_i} + \sum_{i=1}^k \frac{(g_i - e_i)^2}{e_i} \quad (4)$$

4.5 Autocorrelation Experiment:

This test aims to determine whether there is a correlation between s and its (non-cyclic) shifted variants. $1 \leq d \leq [n/2]$, let d is a fixed integer:

$$A(d) = \sum_{i=0}^{n-d-1} s_i + s_{i+d} \quad (5)$$

$$X_5 = 2(A(d) - (n - d / 2)) / \sqrt{n - d} \quad (6)$$

Where $+$ denotes the XOR operator. The result of the five tests just (pass or fail) can be seen in the following Table 2:

Table 2
The Result of the Five Randomness Keys Generator

Poly value	Generator	Five Test Randomness keys
11000011	1100001110010100011011110000100010 000101111101111101001000001100100 0111010001011001101010101101101110 1011110110010111000001010.....	<ul style="list-style-type: none"> • Pass frequency test 0.0039 • Pass serial test 5.9915 • Pass poker test 126.4 • Pass run test 6.221 • Pass autocorrelation test 0.002
1110001	1000111101100111110101010010110110 1011000011011100101011110000000100 0100100001011101001101000001110111 1110011001001110001100010000111101 1001111101010.....	<ul style="list-style-type: none"> • Pass frequency test 0.0039 • Pass serial test 764.9 • Pass poker test 126.4 • Pass run test 5.221 • Pass autocorrelation test 1.032
100111	1110011000100111110000110110101011 0010111101110100100000010100011100 1100010011111000011011010101100101 1110111010010000001010001100110001 0011111000011.....	<ul style="list-style-type: none"> • Pass frequency test 0.0039 • Pass serial test 764.9 • Pass poker test 126.4 • Pass run test 4.221 • Pass autocorrelation test 0.032

5. Conclusion

The result from the proposed sub-system key generator presents a huge number of keys, these keys can be used in different algorithms with different domains for encryption and decryption information such as: still images, text, and video. Furthermore; the use of the logic gate and the polynomials give more efficient random keys from the two sub-systems. Our proposed sub-systems are more powerful and difficult to decrypt messages or data because the system can use two different sub-systems at the same time, so the first 46 bits in the sender and the second 46 bits of keys in the receiver, giving more power to the proposed system and key generator. The two keys of 46 bits each first and second, work in different ways by using an algorithm, it can be prime keys for the public keys algorithm or private keys for the private algorithm. The use of the image as the first to generate huge bits by converting the image to binary, which gives more space for using the system to complete the generated keys as random.

References

- [1] Rana Saad Mohammed, Khalid Kadhim Jabbar, and Hussien Abid Hilal Image Encryption Under Spatial Domain Based On Modify 2d Lscm Chaotic Map Via Dynamic Substitution-Permutation Network,

- International Journal of Electrical and Computer Engineering*, Vol. 11, No. 4, pp. 3070~3083, (August 2021).
- [2] Ismail San, Nuray At, Compact Keccak Hardware Architecture for Data Integrity and Authentication on FPGAs, *Information Security Journal: A Global Perspective*, Issue 5, Volume 21, (2012).
 - [3] Lampis Alevizos, Eliana Stavrou, Cyber threat modeling for protecting the crown jewels in the Financial Services Sector (FSS), *Information Security Journal: A Global Perspective*, (29 Jul 2022).
 - [4] Khalid Kadhim Jabbar, hussin Abd Hilal, and Rana Saad Mohammed, Text Cryptography Using Multiple Encryption Algorithms Based On Circular Queue Via Cloud Computing Environment, *Journal of Theoretical and Applied Information Technology*, 30th June (2018).
 - [5] Soundra Pandian, Five-decade evolution of feedback shift register: Algorithms, architectures and applications, Indian Institute of Technology Patna | IIT Patna. Department of Electrical Engineering, (2009).
 - [6] Alaa kadhim, and Hussein Abed, New Random Keys Generator Depend on Multi Techniques, University of Technology-Baghdad, (2015).
 - [7] Raj Jain, Random Testing Random Number Generators Number Generators, Washington University Saint Louis.
 - [8] Daniel Augot and Matthieu Finiasz, wustl.edu, A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem, *INRIA*, (2008).
 - [9] Ayoub Otmani, and Herve Tal' E Kalachi, Polynomial-Time Key Recovery Attack on The Faure-Loidreau Scheme Based on Gabidulin Codes Philippe Gaborit, Cornell University, (14 Apr 2017).
 - [10] Yuan-Dong Cheng, Ji-Dong He & Fa-Gang Hu (2017) Quantitative risk analysis method of information security-Combining fuzzy comprehensive analysis with information entropy, *Journal of Discrete Mathematical Sciences and Cryptography*, 20:1, 149-165, DOI: 10.1080/09720529.2016.1178913
 - [11] Prashant Manuja & Rajveer Singh Shekhawat (2022) Developing information security metrics and measures for risk assessment of an organization, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1195-1202, DOI: 10.1080/09720529.2022.2075092.

Received March, 2022

Revised May, 2022