Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage: www.akademiabaru.com/arca.html
ISSN: 2462-1927

Design and Simulation of New One Time Pad (OTP) Stream Cipher Encryption Algorithm

Open Access

Mohammed Nabil[1,*], Mohamed Helmy Megahed[2], Mohamed Hassan Abdel Azeem[1]

[1] Arab Academy for Science and Technology and Maritime Transport Cairo, Egypt
[2] Canadian International College, Cairo, Egypt

ARTICLE INFO

Article history:
Received 18 October 2017
Received in revised form 12 December 2017
Accepted 3 March 2017
Available online 3 April 2018

ABSTRACT

One Time Pad (OTP) is unconditionally secure cryptosystem. The one time pad is a long sequence of random bits. These bits are combined with the plaintext message to produce the ciphertext. One time pad key should be used only once. OTP is the only encryption algorithm that has been proven to be unbreakable. In this paper, the design, design principals, analysis and simulation of new OTP stream cipher algorithm is introduced based on the unpredictability concept which was introduced earlier. The unpredictability concept is based on the randomness of the used encryption algorithm where instead of using one encryption algorithm to secure data, multiple encryption algorithms are used at the same time. Also, instead of using one input, multiple inputs are used at the same time. Pseudo Random Number Generator (PRNG) is used to choose which input entered the selected encryption algorithm. The Linear Complexity (LC) for the designed algorithm is measured on 1 Tera Bytes where no repetition is detected. The proof of security for the designed algorithm is given to show the high security level of the OTP proposed algorithm. The proposed algorithm passed all NIST tests. The designed algorithm can easily resist different attacks such as linear, differential and algebraic cryptanalysis; also it resists other cryptanalysis attacks.

Keywords:

One Time Pad (OTP), unpredictability, Pseudo Random Number Generator (PRNG),

1. Introduction

One time pad (OTP) [1] encryption is a binary additive stream cipher, where a stream of randomness keys is generated and then combined with the plaintext for encryption or with the ciphertext for decryption by an 'exclusive OR' (XOR). One time pad (OTP) encryption algorithm is unbreakable encryption due to that the key must be as long as the plaintext, the key must be random and the key must only be used once. It will be impossible to decipher one time pad encrypted data without having the proper key, regardless any existing or future cryptanalytic attack or technology. Our designed OTP encryption algorithm is based on the unpredictability concept.

* *Corresponding author.*
E-mail address: mohammednabel5050@gmail.com (Mohammed Nabil)

The unpredictability concept depends on the randomness of the used encryption algorithm. Instead of using one encryption algorithm to secure data, multiple encryption algorithms are used at the same time. Also, instead of using one input, multiple inputs are used at the same time. Pseudo Random Number Generator (PRNG) is used to select which input entered the selected encryption algorithm. In one time pad encryption scheme, random key is equal in length to the plaintext message to be encrypted, with no repetition is used. In this paper, we propose a new OTP stream cipher encryption algorithm with the followings as:

1- Two RC4 algorithms as inputs with key size of 256 bits for each which are noted $RC4_1$ and $RC4_2$ and the output of each RC4 is 256 bits.
2- Two Double AES-256 algorithms with only three rounds and each output of 256 bits which are noted DBAES1 and DBAES2. The Double AES-256 has 512 bits key length
3- One RC4 algorithm to select which input entered the selected Double AES-256 algorithm which is noted $RC4_3$ with key size of 512 bits and output of the RC4 is 1 bit.
4- The total key size of the cryptosystem is 2048 bits.
5- XOR between the outputs of the two Double AES-256 which is DBout which is the key stream that is 256 bits.
6- XOR between DBout and Plaintext of 256 bits to produce the ciphertext.

The key stream of 256 bits of the designed algorithm Linear Complexity is measured over 1 Tera Bytes and no repetitions is detected. The key stream of 256 bits of the designed algorithm passed all the NIST tests. RC4 has period of 10^{100} [2] with total period for the two RC4 algorithms of 10^{200}. The total period of the three RC4 algorithms is 10^{300} which is the period of the designed new OTP stream cipher encryption algorithm. Therefore, our proposed designed OTP algorithm has long period which is resulted from the unpredictability concept [3]. The designed OTP stream cipher encryption algorithm is secure against different attacks such as linear cryptanalysis [4,6], differential cryptanalysis [5,6,9,11], algebraic attack [6,7,11], correlation attack [11], divide and conquer attack [11], related key attack [6,8], sliding attack [6,12] and binary decision diagram (BDD) attack [12] due to the unpredictability concept where the attacker is confused and the attacker cannot decide which algorithm is operating with a defined input from the two RC4 algorithms.

The speed of the proposed designed OTP algorithm is measured which is 75 M bits /Sec on Laptop Dell Inspiron 15R and the operating system is Windows 7 of 64-bit, Processor Intel® Core™ i7-5400U CPU @ 1.80 GHz and RAM of 8 GB. Our proposed designed OTP encryption algorithm achieves high security level.

1.1 Contributions

1- The design and simulation of new OTP stream cipher algorithm is proposed that is based on the unpredictability concept which is immune to different cryptanalysis attacks.
2- High speed encryption and decryption.

1.2 Outline of the Paper

Section 2 introduces the related work. Section 3 introduces the design principales. Section 4 presents the algorithm architecture. Section 5 presents software implementation. Section 6 introduces the Linear Complexity. Section 7 presents the NIST tests. Section 8 presents the performance analysis. Section 9 concludes the paper.

2. Related Work

In this section, we present a brief overview of the related works which we will employ to our proposed design of the new One Time Pad (OTP) stream cipher encryption algorithm as the following:

2.1 The Vernam Cipher

There is only one completely secure cryptosystem known as Vernam Cipher [1, 13]. In modern terminology, a Vernam cipher is a symmetrical stream cipher in which the plaintext is combined with random or pseudorandom stream of data (key stream) of the same length to generate ciphertext output using XOR function. The key stream is random and it is used only once. Vernam Cipher uses a random key that is as long as the message. The key stream needs not to be repeated. In additional, the key must be use once for encryption and decryption of a single message and then that key is discarded. So, this technique is called the One Time Pad and it is unbreakable.

2.2 SSEA3

The Spread Spectrum Encryption Architecture (SSEA3) [3] is computationally secure cryptosystem. Spread Spectrum Encryption Architecture is a family of symmetric key cipher systems. It consists of Two AES-256 encryption algorithms with only 3 rounds to achieve unpredictability in its design at subkeys level, output level and algorithm level. SSEA3 architecture is based on the unpredictability concept. The unpredictability concept concerned with selecting one algorithm from multiple algorithms, selecting one subkey from multiple subkeys at each round of the block cipher algorithm in addition to masking the output ciphertext with encrypted stream of bits. SSEA3 has two AES-256 encryption algorithms with two different S-Boxes to solve the synchronization problem between the two algorithms used. Each algorithm has only 3 rounds of AES-256. Different S-Boxes is used to ensure different algorithms output with the same key. The encryption algorithm will keep changing from algorithm one to algorithm two. Each round has 16 subkeys of the 3 rounds. The subkeys are dynamic (not fixed). The output of the two AES-256 encryption algorithms is XORED to produce ciphertext output. SSEA3 is highly secure and highly speed encryption algorithm which can resist Quantum Computer (QC) [14, 15] attacks. As shown in Figure 1, the SSEA3 architecture has two AES-256 encryption algorithms and two session keys for the cryptosystem. The RC4 stream cipher algorithm selects which subkey is used to encrypt the plaintext. One subkey of the 16 subkeys is chosen at each round based on RC4 stream cipher algorithm as Pseudo Random Number Generator (PRNG). The PRNG chooses where the plaintext goes to algorithm 1 or algorithm 2. The output from RC4 stream cipher algorithm is used to enter the algorithm that is not used by the plaintext. The outputs from the two encryption algorithms are XORed to produce ciphertext output as shown in Figure 1.

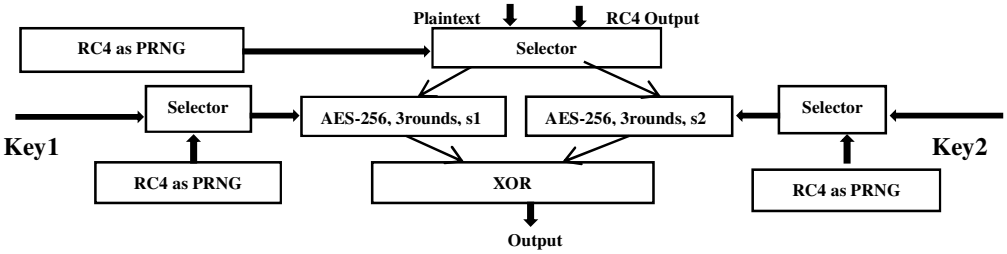

Fig. 1. SSEA3 Encryption Architecture

3. Design Principles

The proposed design of a new One Time Pad (OTP) stream cipher encryption algorithm is based on the unpredictability concept. The unpredictability concept is based on the randomness of the used encryption algorithm. Instead of using one encryption algorithm to secure data, multiple encryption algorithms are used at the same time. Also, instead of using one input, multiple inputs are used at the same time. Pseudo Random Number Generator (PRNG) is used to choose which input entered the selected encryption algorithm. The proposed structure of OTP algorithm is resembling SSEA3. In this paper, we propose the design and simulation a new OTP stream cipher encryption algorithm with the following design principles:

a) The unpredictability concept.
1- Using multiple encryption algorithms at the same time based on PRNG instead of using one encryption algorithm.
2- Using multiple inputs at the same time instead of using one input.
3- XOR between the outputs of the encryption algorithms.
b) High security level through resisting different cryptanalysis attacks.
c) High speed of generating the bits stream of the OTP stream cipher and high speed of the proposed encryption algorithm.

4. Algorithm Architecture

4.1 System Components

4.1.1 Two Double AES-256 encryption algorithms with only three Rounds

We proposed to use two Double AES-256 encryption algorithms with two different S-Boxes. Two different S-Boxes are used to solve the synchronization problem between the two algorithms. Each algorithm has Double AES-256 with only three rounds. The encryption algorithm will keep changing from algorithm 1 to algorithm 2 based on RC4. The proposed architecture is dynamic due to the unpredictability concept. The attacker cannot perform any cryptanalysis attack over the ciphertext output because of the unpredictability concept.

4.1.2 Key schedule

There are four keys each of 256 bits length. We select the key schedule of AES-256 to generate sub keys at each round for the three rounds for each algorithm used. The key schedule of AES-256 generates the 256 bits seed for the RC4 stream cipher algorithm.

4.1.3 RC4 Stream Cipher Algorithm as Pseudo Random Number Generators (PRNG)

The proposed designed encryption algorithm has three RC4 stream cipher algorithm as PRNG. The RC4 is used to select where the inputs goes to algorithm 1 or algorithm 2. The output from the two RC4 stream cipher algorithm is used to enter the two algorithms. The outputs from the two encryption algorithms are XORed to generate the key stream of 256 bits.

4.2 Encryption Process

Figure 2 shows that the proposed algorithm architecture has Two Double AES-256 encryption algorithm and one session key for each algorithm (K_1, K_2). $RC4_3$ stream cipher algorithm chooses which output from $RC4_1$ and $RC4_2$ will enter the two Double AES-256 algorithms. The output of the

two algorithms are XORed to generate the key stream and the key stream is XORed with plaintext to generate the encrypted ciphertext output.

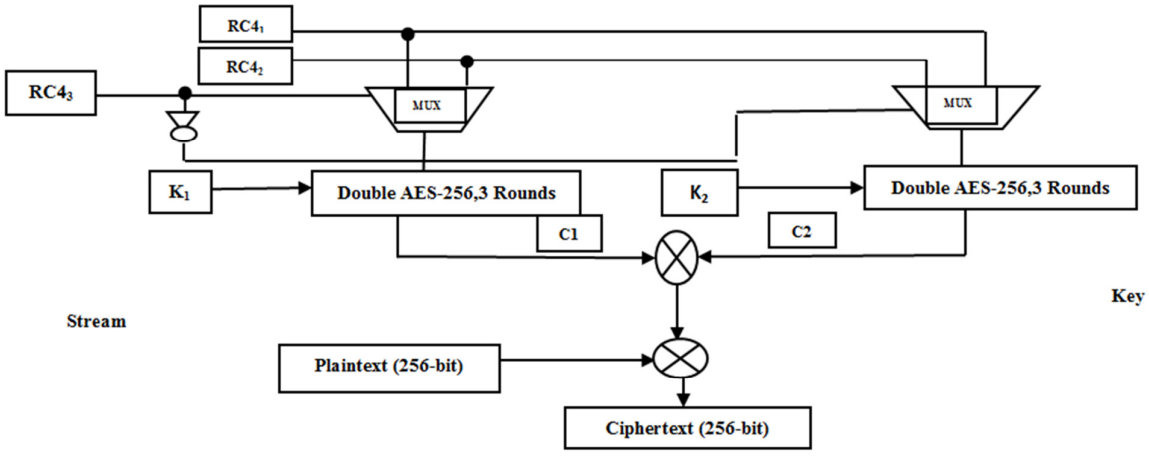

Fig. 2. Encryption Process

4.3 Decryption Process

The Decryption Process of the proposed algorithm is done by the same process of encryption in addition to perform XORing between ciphertext and key stream as shown in Figure 3.

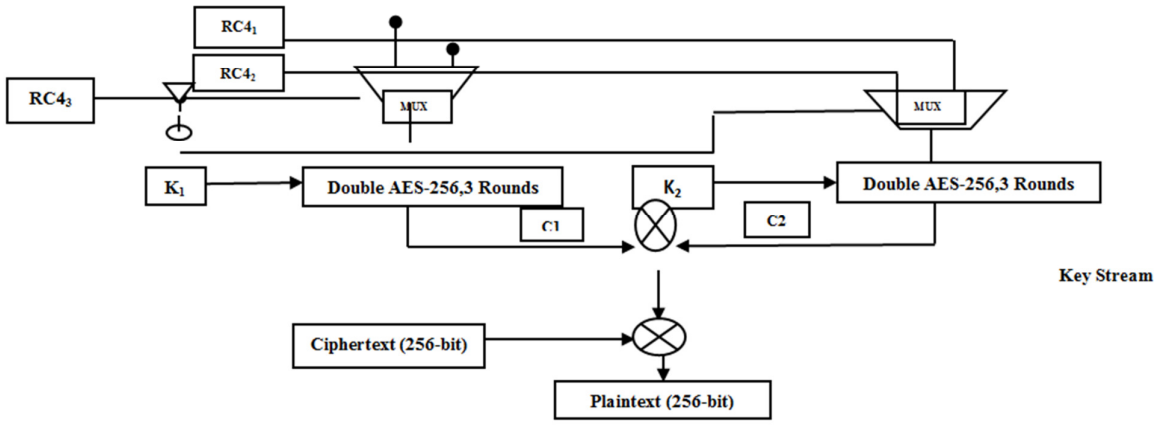

Fig. 3. Decryption Process

4.4 Mathematical Model

4.4.1 Encryption

$RC4_3$ Selects $ENC_{DB1AES-256}$ OR $ENC_{DB2AES-256}$

$ENC_{DB1AES-256}(RC4_1) = C_1$, the first double AES-256 encrypts the output from first RC4

$ENC_{DB2AES-256}(RC4_2) = C_2$, the second double AES-256 encrypts the output from second RC4

Key Stream (DBout) $= C_1 \oplus C_2$

Ciphertext=DBout $\oplus$ Plaintext

4.4.2 Decryption

$RC4_3$ Selects $ENC_{DB1AES-256}$ OR $ENC_{DB2AES-256}$
$DEC_{DB1AES-256}(RC4_1) = C_1$, the first double AES-256 encrypts the output from first RC4
$DEC_{DB2AES-256}(RC4_2) = C_2$, the second double AES-256 encrypts the output from second RC4
Key Stream (DBout) $= C_1 \oplus C_2$
Plaintext=DBout $\oplus$ Ciphertext

4.5 System Analysis

The attacker needs to know which algorithm is operating to encrypt $RC4_1$ and $RC4_2$. The designed algorithm architecture stops the linear and differential cryptanalysis due to that the attacker does not know which algorithm is used to encrypt $RC4_1$ and $RC4_2$.

4.6 Proof of Security according to Cryptanalysis Attacks

The Designed Algorithm is immune to Linear Cryptanalysis, Differential Cryptanalysis, Algebraic Attack, Correlation attacks, Divide and Conquer attack, Related Key attack, Sliding attack and BDD attack (Binary Decision Diagram attack).

The cryptanalysis attacks are based on the fact that the algorithm is fixed and the algorithm in the new designed OTP keep changing for every $RC4_1$ and $RC4_2$ blocks; therefore, the cryptanalysis attacks are not applicable.

5. Results and Software Implementation

We developed software for the proposed encryption algorithm. This software can encrypt and decrypt files in addition to measuring the Linear Complexity (LC) for the designed algorithm that is measured on 1 Tera Bytes where no repetition is detected. The output file from the designed system is immune to different cryptanalysis attacks where unpredictability is the barrier between the proposed system and the attacks. Also, proposed system is faster than [1].

6. Linear Complexity

The LC is a technique that is used to determine the period of output that can be repeated and to determine whether or not the sequence is complex enough to be considered random. The possibility of using the linear complexity characteristic for testing randomness is based on the Berlekamp-Massey [16] algorithm, which provides an efficient way to evaluate finite strings. The Berlekamp-Massey is an algorithm that is used to determine the LC. The LC for the designed algorithm is measured on 1 Tera Bytes where no repetition is detected. The LC test is the most important test for stream cipher encryption algorithms.

7. National Institute of Standards and Technology (NIST) Tests [17]

The proposed algorithm passed all NIST tests which is a freeware package for statistical tests as the following:

1. The Frequency (Monobit) Test.
2. Frequency Test within a Block.
3. The Runs Test.
4. Longest-Run-of-Ones in a Block.

5. The Binary Matrix Rank Test.
6. The Discrete Fourier Transform (Spectral) Test.
7. The Non-overlapping Template Matching Test.
8. The Overlapping Template Matching Test.
9. Maurer's “Universal Statistical” Test.
10. The Linear Complexity Test.
11. The Serial Test.
12. The Approximate Entropy Test.
13. The Cumulative Sums (Cusums) Test.
14. The Random Excursions Test.
15. The Random Excursions Variant Test.

8. Performance Analysis

The proposed algorithm is characterized by high security level through resisting different cryptanalysis attacks, high speed of generating the bits stream of the OTP stream cipher and high speed of the proposed encryption algorithm. The speed of the proposed designed OTP algorithm is measured which is 75 M bits /Sec on Laptop Dell Inspiron 15R and the operating system is Windows 7 of 64-bit, Processor Intel® Core™ i7-5400U CPU @ 1.80 GHz and RAM of 8 GB.

9. Conclusion

We proposed to design and simulate a new OTP stream cipher encryption algorithm which is suitable for applications that needs high security such as UAV Data Link. The proposed design algorithm resists different cryptanalysis attacks such as Linear, Differential cryptanalysis and algebraic attacks. It has high speed of generating the key stream bits of the OTP stream cipher and high speed of the proposed encryption algorithm of 75 M bits/Sec.

References

[1] Dhull, Sonia, and Vinod Saroha. "Enhancing Security of One Time Pad Cipher by Double Columnar Transposition Method." *International Journal of Advanced Research in Computer Science and Software Engineering* 3, no. 3 (2013).
[2] Chefranov, A. G., and T. A. Mazurova. "Pseudo-random number generator RC4 period improvement." In *Automation, Quality and Testing, Robotics, 2006 IEEE International Conference on*, vol. 2, pp. 38-41. IEEE, 2006.
[3] Megahed, Mohamed Helmy Mostafa. "SurvSec Security Architecture for Reliable Surveillance WSN Recovery from Base Station Failure." PhD diss., Université d'Ottawa/University of Ottawa, 2014.
[4] Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 386-397. Springer, Berlin, Heidelberg, 1993.
[5] Federic Muller, “Differential Attack and Stream Cipher”, eprint, ICAR, 2007.
[6] Hong, Deukjo, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee et al. "HIGHT: A new block cipher suitable for low-resource device." In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 46-59. Springer, Berlin, Heidelberg, 2006.
[7] MARTIN VöRöS, “ALGEBRAIC ATTACKS ON CERTAIN STREAM CIPHERS”, Master’s Thesis, Bratislava, 2007.
[8] Biham, Eli. "New types of cryptanalytic attacks using related keys." *Journal of Cryptology* 7, no. 4 (1994): 229-246.
[9] Biham, Eli, and Adi Shamir. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.
[10] Verdult, Roel. "Introduction to Cryptanalysis: Attacking Stream Ciphers."
[11] Banegas, Gustavo. "Attacks in Stream Ciphers: A Survey." *IACR Cryptology ePrint Archive* 2014 (2014): 677.
[12] Đorđević, Srđan, S. Bojanić, and O. Nieto-Taladriz. "BDD-based Cryptanalysis of LFSR Stream Ciphers."

[13] Srikantaswamy, S. G., and H. D. Phaneendra. "Enhanced OneTime Pad Cipher with MoreArithmetic and Logical Operations with Flexible Key Generation Algorithm." *International Journal of Network Security & Its Applications* 3, no. 6 (2011): 243.
[14] Barreno, Marco A. "The future of cryptography under quantum computers." *Dartmouth College Computer Science Technical Reports* (2002).
[15] Antal Nemes, Viktoria Villanyi and Peter Sziklai, "Quantum Resistant Cryptography", Technical Report from Faculty of Science, Budapest, 2012.
[16] Erin C., "Berlekamp-Massey Algorithm", PhD Thesis, Minnesota University, 2000.
[17] Zaman, J. K. M. S., and Ranjan Ghosh. "Review on fifteen Statistical Tests proposed by NIST." *J. of Theoretical Physics & Cryptography* 1 (2012): 18-31.