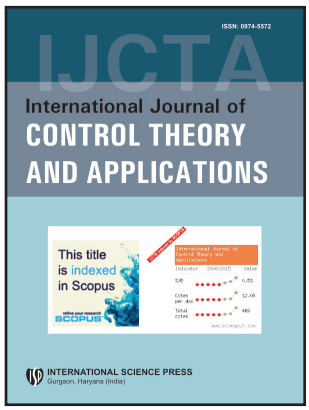

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 9 • Number 43 • 2016

DNA-based Approach of AES with Key Dependent Shift Rows

Nidhinraj P.P.[a] and Joby George[b]

[a-b]Department of Computer Science and Engineering, M.A College of Engineering, Kothamangalam, Kerala, India. Email: [a]nidhinsaikripa@gmail.com; [b]jobygeo@hotmail.com

Abstract: The DNA-based design and implementation of "Advanced Encryption Standard"[AES], is an algorithm with all its specifications on DNA basis which includes data, operations, algorithms, and used functions. This aims at proving the possibility of building a complex DNA-based encryption system which will be a fine candidate for implementation in a biological environment or on DNA computers. The Shift-Rows phase of standard AES algorithm is changed from basic transposition to a dynamic transformation phase depending on derived keys. The parameters of the proposed Shift-Rows similar characteristics as that of the original algorithm AES besides increasing its resistance against attack. The use of key-dependent Shift-Rows can be considered as one of the applied methods for improving the quality of a cryptographic algorithm.

Keyword: DNA Cryptography, Advanced Encryption Standard, Data Encryption, Data Decryption.

1. INTRODUCTION

With the immense advances in the field of DNA computing in which DNA is used as the information carrier and the modern biological technologies are used as an implementation tool multiple theories for implementing DNA computers have evolved. DNA cryptography is inspired by developments in the field of DNA computing. The high level of parallelism, extraordinary energy efficiency and very high information density inherent in DNA molecules are exploited for cryptographic purposes such as encryption, authentication, signature, and so on. In fact, the tremendous storage capacity of DNA, as well as the ability to synthesize DNA sequences in any desirable length makes DNA a perfect medium for cryptography and steganography.

Traditional security systems built on a strong mathematical and theoretical basis (like RSA, DES, and NTRU) have a long legacy and are also found in real time operations. The DNA cryptography is not to negate the tradition, but to create a bridge between existing and new technology. DNA cryptography should use biological hard problems as main security basis and modern biological techniques as tools for building complex systems. Designing new hybrid cryptographic systems using the power of DNA computing will strengthen the existing security systems.

The objective of our work is to facilitate the link and interaction between the fields of DNA computing and digital computing by presenting a DNA-based implementation of "Advanced encryption Standard" (AES). Only

a few works have proposed or suggested a Shift-Rows that is designed on a DNA basis. This paper proposes a novel technique for creating a dynamic key-dependent Shift-Rows based on operations that have been inspired by the biological DNA structure and processes.

2. RELATED WORKS

The Advanced Encryption Standard (AES) specifies a cryptographic standard to protect electronic data and is approved by Federal Information Processing Standards (FIPS). The AES algorithm is a symmetric block cipher to encrypt and decrypt information. AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmened. Rijndael cipher is a family of ciphers with different key and block sizes [1]. AES was first and foremost developed for U.S government but now it is one of the most widely adopted security standards. AES algorithm is based on symmetric key encryption.

Few studies simulating the process of central dogma in cryptographic applications were conducted from proposed DNA-based encryption algorithms. There is a simple cryptographic method based on the same idea and there is a symmetric encryption DNA-based algorithm called YAEA that was proposed by Amin et. al., in [2] [3]. In this research, the binary form of data, such as plaintext messages, and images are transformed into sequences of DNA nucleotides. Then locate multiple positions of a sequence of four DNA nucleotides that represent binary octet plaintext character within a Canis Familiaris genomic chromosome, using efficient searching algorithms. Pointers of randomly selected DNA words for plaintext characters are assembled and send as plaintext [4]. This technique can be used to enforce other conventional cryptographic algorithms.

Another work led by [5] presents a symmetric encryption algorithm simulating mechanisms of the central dogma of biology designed according to the recommendations of experts in cryptography. This contains a DNA module part that simulates critical processes of biological DNA in order to enhance its security [6].

Recently in 2013 [7] proposed an algorithm with a 192-bit key for encryption by utilizing the hyperchaotic system and combination with DNA complementary rule [8]. The author uses the Arnold cat and then it is encoded into DNA image, this provides a better confusion. After that, by means of the complementary rule and XOR with a hyperchaotic binary sequence, each nucleotide of DNA image is transformed into its corresponding base pair.

In 2014, a combination of DNA computing and round-reduced AES block cipher is proposed by Eman Shehab et. al., [8] The method proved to have high resistance to most of the known attacks such as exhaustive search, statistical analysis, and differential analysis concluding that the method achieves high level of security and fast implementation.

Lately, on 2015, AI-Wattar et. al., proposed an approach for altering the Mix-Columns transformation engaged in the AES algorithm [10]. The approach employed methods inspired from DNA processes and structure, which relied on the key. The analysis of the obtained results showed that this new transformation is more secure, resistance against the attacks, and will increase the stability of AES against linear and differential cryptanalysis.

3. PROPOSED SYSTEM

The proposed system is basically a DNA adaptation of the Advanced Encryption Standard. But shift rows phase of round transformations is modified to provide a new dynamic and key dependent transformation phase instead of the static transposition.

A. AES Round Transformations

AES consists of multiple rounds of transformation to convert plaintext message into ciphertext output. Each round consists of several procedures to transform the intermediates and always involves a relying on the private

cryptographic key. AES has fixed block size (128bit), and a key length is 128, 192 or 256 bits, relating to the number of rounds for the algorithm. The round transformations are performed on a 4x4 matrix of bytes called state. The algorithm calculations are basically achieved on finite fields.

In AES, the Shift-Rows transformation is one of the linear units of symmetric encryption algorithms. It consists of a transposition action where each row of the state cyclically shifted a number of times to scramble the byte order within each 128-bit block. This transformation includes shifting the state rows the first row in the state does not change, the second row is circularly shifted to left by 1 byte, the third row takes a 2 bytes circular left shift, and the fourth row is circularly shifted by 3 bytes to left. Figure 1 shows the AES Shift-Rows transformation.

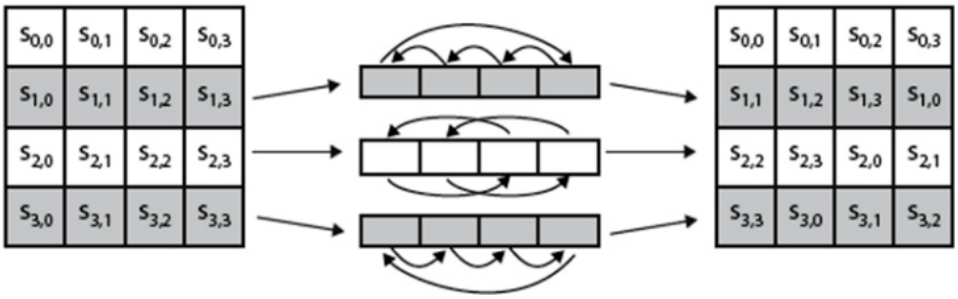

Figure 1: AES Shift Rows transformation

According to [4], AES without Shift-Rows stage are more than that of AES, their values differ very little for different rounds. The most challenging for AES algorithm is the linear and differential cryptanalysis where Rijndael can be an issue to standard techniques of differential and linear cryptanalysis.

From the analysis of resistance against differential and linear cryptanalysis, it was found that, for Enhancing the resistance of block cipher against differential and linear attacks, arbitrary unknown and key-dependent substitution and permutation transformations are considered as a good factor since the differential and linear attacks needs to be known transformations[11][12]. Dynamic and unknown to the cryptanalyst structure and other specific properties of substitution and permutation functions improves the block cipher's resistance against attacks. For the attacker, differential and linear trail over multiple rounds are considered as a vital requirement, and in the existence of key-dependent dynamic transformations, output differences rely on the additional key used. There are unrelated differentials over multiple rounds of transformation in addition to different key values. This toughens attacker's job to utilize the current linear and differential techniques of cryptanalysis.

B. Key Dependent Shift Rows Design

The Shift-Rows transformation will be referred to as a key-dependent dynamic transformation in the proposed work. The static transposition algorithm of Shift-Rows is converted to a dynamic procedure which depends on round key values. The transformation process is inspired by DNA-strands structures including its nature, orientation as well as DNA-bases and operations like reverse-complement.

The cipher key Kr at round *r* is used as a key for applying the reverse-complement over state bytes (byte level). Byte transposition process used here is dynamic rather than static and it also depends on key values derived from corresponding round keys. Four key values (N1, N2, N3, and N4) are derived from four specific bytes of Kr for each round of Shift-Rows. These key values range from 0 to 3.

The number of bytes that form the DNA-base (candidate for reverse complement operation) will be selected according to the key-value. In this transformation, the DNA-bases will not be two bits as standard algorithms

instead they will be represented by a variable number of bytes. The key value (N1, N2, N3 andN4) would specify the number of nucleotides that form one DNA-base. Individual rows of state STE is separately considered for Shift-Rows. Each row is a DNA strand of length 16, but the number of nucleotides that form DNA base differs depending on key value.

The key derived from round key Kr will have four values, these values represent the number of nucleotides that form a possible candidate for reverse-complement operation (DNA base). The key values and their meanings are shown in Table 1.

Table 1
Transposition key values and their meanings

Value	*Meaning*
0	Each element of state row represents a base
1	No value/state row remains unchanged
2	Every two elements of state row represents a base
3	Entire state row represents a base

The mechanism of byte level reverse-complement of state row elements is defined using these key-values. Here *a*, *b*, *c* and *d* are 4 bytes, representing a single row of stat STE where each row represents a DNA strand consisting of 16 nucleotides. Each DNA base will consist of one, two or four bytes, according to the key values. After each STE row is represented as DNA bases, the reverse-complement method is performed. The reverse-complement is performed in byte by byte level fashion if every DNA-base is formed by one byte. When the key value is two then the DNA bases will be of two bytes and the reverse complement operation will be performed on every separate two bytes in the row. The reverse complement will be achieved on the whole row as one part if the entire row represents a DNA base (key value = 3). Unlike these cases when the key value is 1, then there will be no reverse operation, but the state row is just complemented.

4. CONCLUSION

The implementation of a DNA-based version of the "Advanced Encryption Standard" (DAES) with new dynamic key-dependent permutation transformation was proposed with chosen byte from the key and existing AES state. The new Shift-Rows transformation is not fixed, but changeable at each round according to the round key values. Analyzing the results demonstrates that the characteristics of the new Shift-Rows are more secure and this toughen the job for attackers, on which concluded that it is potential to employ it for an encryption. When analyzing the stability against linear and differential cryptanalysis, the new encryption algorithm shows significant improvement.

REFERENCES

[1] Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa, "Design of DNA-based Advanced Encryption Standard (AES)", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15).

[2] A. Gehani, T.H LaBean, 1.H. Reif, "DNA-based cryptography", In 5th DiMACS Series in Discrete Mathematics and Theoretical Computer Science, MIT, Vol. 54, pp. 233-249, 1999.

[3] A. Leier, C. Richter, and W. Banzhaf. "Cryptography with DNA binary strands", Biosystems. pp. 13- 22, 2000.

[4] S.V. Kartalopoulos, "DNA-inspired cryptographic method in optical communications, authentication, and data mimicking", in Military Communications Conference. pp. 774-779, 2005.

[5] T. Kazuo, O. Akimitsu, S. Isao, "Public-key system using DNA as a one-way function for key distribution", Biosystems, pp. 25-29, 2005.

[6] National Institute of Standards and Technology (NIST). Fips 197: Advanced encryption standard (AES). Technical report, National institute of Standards and Technology (NiST), 2001.

[7] Auday H. A-Wattar, Ramlan Mahmod, Zuriati Ahmad Zukarnain and NurIzura Udzir. "A New DNA-based Approach of Generating Key dependent mix-columns Transformation" International Journal of Computer Networks & Communications (IJCNC) Vol. 7, No. 2, March 2015.

[8] Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA-based Implementation of YAEA Encryption Algorithm," lASTED International Conference on Computational Intelligence (CI 2006), San Francisco, Nov. 20, 2006.

[9] J. Daemen and V. Rijmen, "AES proposal: Rijndael," in First Advanced Encryption Standard (AES) Conference, 1998.

[10] V. Rijmen and J. Daemen, "Advanced Encryption Standard," Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, pp. 19-22, 2001.

[11] G. Krishnamurthy and V. Ramaswamy, "Study of Effect of Removal of Shift-Rows and Mixcolumns Stages of AES and AES-KDS on their Encryption Quality and Hence Security."

[12] M. Zhang, et. al., "A mathematical formulation of DNA computation," NanoBioscience, IEEE Transactions on, Vol. 5, pp. 32-40, 2006.