ENCRYPTION METHOD FOR SECURE DATA TRANSMISSION USING DNA BASED CRYPTOGRAPHY

Sathish.V [1*], Subash Kumar.V [2], Thirumalaivasan.R [3], Pavithra.S [4], SitaDevi Bharatula [5]

Abstract- In today's world, security is very fundamental and significant issues of data transmission. Technology advancement is occurring daily in order to find a new cryptographic algorithm. Data security is concerned with the areas of data transmission. Recent advancements in cryptography has led to new techniques called DNA based cryptography. Here idea of molecular biology is applied and an efficient way is proposed. In existed AES method is well suited for security applications. In our proposed system we improve the performance of the system we propose Triple AES based DNA key cryptography. In our new proposed implementation provides better and faster results in environment, hence data security is high.

1 INTRODUCTION

Nowadays technology is developing at a rate faster than speed of light and the amount of redundant digital multimedia signals has increased more in the internet. The security of a system is essential nowadays. The number of threats a user is supposed to deal grows exponentially, with the growth of Information Technology power. Cryptographic systems have been in use for many years from now on. That is cryptography consists in processing plain information by applying a cipher and obtaining encoded output, which would seem meaningless to a third party who does not know anything about the key involves one or more keys. In secret key cryptography, secure key exchange through public channel is difficult.

Hence in this paper concept of triple AES algorithm and also DNA based cryptography is used. DNA based cryptography is used to generate key for encrypting and decrypting message. Biological issues and cryptography computing troubles provide a double security safeguards for the two schemes and makes it difficult for breaking in.

The word cryptography comes from two Greek words meaning “secret writing” and is the art and science of concealing meaning. The basic component of Cryptography is cryptosystem. Basically transmitting key using a secure channel by both encrypting and decrypting. In this we use a currently emerging area of cryptography is the uncertainty principle of cryptography. In conventional information theory and cryptography, the information or data fed is always monitored or can undergo threats easily as there is no safety. But by using triple AES for authentication, a quantum channel is established instead of an ordinary channel and it permits secure distribution of random keys or information between parties. This is the main advantage of using Triple AES . Message encryption is done using the DNA based algorithm. Cryptography is about the avoidance and recognition of fraud and other cruel activities. Symmetric-key cryptography, also called secret key cryptography. It involves the use of a secret key known only to the users. It is considered by the use of a single key to perform both the encrypting and decrypting of data. On October, 2, 2000, The National Institute of Standards and Technology (NIST) announced Rijndael as the new Advanced Encryption Standard (AES).The Predecessor to the AES was Data Encryption Standard (DES) which was considered to be unsecure because of its weakness to brute force attacks. DES was a standard from 1977 and stayed until the mid1990’s To overcome the situation, the National Institute of Standards and Technology (NIST) created a new encryption standard. The methods were proposed by Joan Daemon and Vincent Rijman, which are called Rijndael.

The National Institute of Standards and Technology (NIST) have published the specifications of this encryption standard in the Federal Information Processing Standards (FIPS) Publication 197. Different versions of AES algorithm exist today (AES128) depending on the size of the encryption key. Three architectural optimization approaches can be employed to speed up the hardware implementations: Pipelining, Sub Pipelining, and Loop-Unrolling. Among these approaches, the sub pipelined architecture can achieve maximum speed up and optimum speed–area ratio in non-feedback modes. The Rijndael algorithm, the Advanced Encryption Standard (AES) provides a symmetric key cryptography that allows for the encryption and decryption of blocks of data. As a symmetric system, the secret key must be shared between the sender and receiver in order for communication to be possible.

AES algorithm is generally applied in the financial field in domestic, such as realizing legal encryption in ATM, magnetism card and intelligence card.

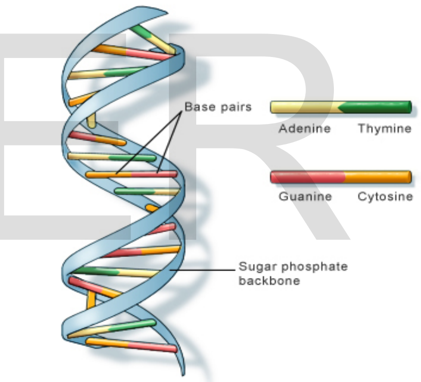
A cryptographic system uses 2 main blocks i.e. is encryption and decryption. Encryption is basically protecting information, i.e. data is transferred into unreadable form in order to ensure privacy and also keeps the information hidden. Decryption, being the reverse process of encryption uses the encrypted form of data and transforms this data into readable form. A key is transmitted between encryption and decryption modules which provide a secure channel for transferring information. This includes a basic block diagram of a cryptographic system, which has an encryption block a secret key and a decryption block, and these are the main components of a cryptographic system.

2. EXPERIMENTAL SECTION

In our project we propose Triple AES algorithm using DNA cryptography. Triple AES is based on the AES steps but In a Encryption side we encrypt two times and decrypt one time to change data plain text to cipher text. In a decryption side, we decrypt two times and encrypt one time to change data cipher text in to plain text. In this system secret key is needed for encryption and decryption process. This secret key is generated using DNA key algorithm. Here since we are using DNA concept, we use DNA based encryption process to generate a DNA coded sequence and this sequence is used as the key and is given to the Triple AES algorithm.

DNA

One of the most essential components required for the functioning of all living organisms is DNA. DNA stands for Deoxyribonucleic acid and it has many properties like vast parallelism, exceptional energy storage capability. There are four classes of nucleotides, Adenine, Guanine, Cytosine, Thymine (A,C,G,T). These nucleotides are strung into polymer chains (DNA strands). DNA is basically used to store genetic information. This information cannot be duplicated or copied.



U.S. National Library of Medicine

Fig. The basic structure of a DNA molecule.

The concepts of biotechnology, where DNA strands are used as a carrier for conveying message from the sender to receiver are used in DNA cryptography.

The existing cryptographic schemes like RSA and DES is pronto many attacks in the near future and has been broken. This is one of the main reason for using DNA concept.

This concept is still in the early stages and further developments are going on in this area. One end orientation of DNA is 5′ and the other end is 3′. DNA which usually exists in the form of double helix structure and these structures are

Formed with the help of hydrogen bonds between them. This structure is called as Watson – Crick.

2.1. Software development:

- *Sathish.V, Subash Kumar.V, Thirumalaivasan.R are currently pursuing Bachelor degree program in Electronics and Communication engineering in Saveetha School of Engineering, India, PH-09094942090. E-mail: sathishtamilsathi@gmail.com , jrthirumalai@gmail.com, subashkumar2910@gmail.com*
- *Ms.Pavithra.S,Ms. SitaDevi Bharatula Assistant Professors, Electronics and Communication engineering in Saveetha School of Engineering, India.E-mail: pavithra1286@gmail.com, sita_bharatula@gmail.com*

2.1.1 AES:

AES is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128 bits.
Cipher Key and the number of rounds The Cipher Key is similarly pictured as a rectangular array with four rows. The number of columns of the Cipher Key is denoted by Nk and is equal to the key length divided by 32.These representations are illustrated in Figure .In some instances, these blocks are also considered as one-dimensional arrays of 4-byte vectors, where each vector consists of the corresponding column in the rectangular array representation. These arrays hence have lengths of 4, 6 or 8 respectively and indices in the ranges 0..3, 0..5 or 0..7. 4-byte vectors will sometimes be referred to as words. Where it is necessary to specify the four individual bytes within a 4-byte vector or word the notation (a, b, c, d) will be used where a, b, c and d are the bytes at positions 0, 1, 2 and 3 respectively within the column, vector or word being considered.
The input and output used by Rijndael at its external interface are considered to be one dimensional arrays of 8-bit bytes numbered upwards from 0 to the 4***Nb**-1. These blocks hence have lengths of 16, 24 or 32 bytes and array indices in the ranges 0..15, 0..23 or 0..31. The Cipher Key is considered to be a one-dimensional arrays of 8-bit bytes numbered upwards from 0 to the 4***Nk**-1. These blocks hence have lengths of 16, 24 or 32 bytes and array indices in the ranges 0.15, 0.23 or 0.31.
The cipher input bytes (the "plaintext" if the mode of use is ECB encryption) are mapped onto the state bytes in the order a0,0, a1,0, a2,0, a3,0, a0,1, a1,1, a2,1, a3,1, a4,1 ... , and the bytes of the Cipher Key are mapped onto the array in the order k0,0, k1,0, k2,0, k3,0, k0,1, k1,1, k2,1, k3,1, k4,1 ...
At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. Hence if the one-dimensional index of a byte within a block is n and the two dimensional index is (i ,j), we have:
i = n mod 4 ; j = ën / 4û ; n = i + 4 * j
Moreover, the index i is also the byte number within a 4-byte vector or word and j is the index for the vector or word within the enclosing block. The number of rounds is denoted by Nr and depends on the values Nb and Nk. It is given in Table.

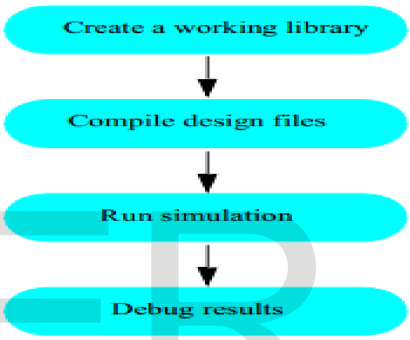
Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

TABLE : NUMBER OF ROUNDS (NR) AS A FUNCTION OF THE BLOCK AND KEY LENGTH.

2.1.2 MODEL SIM

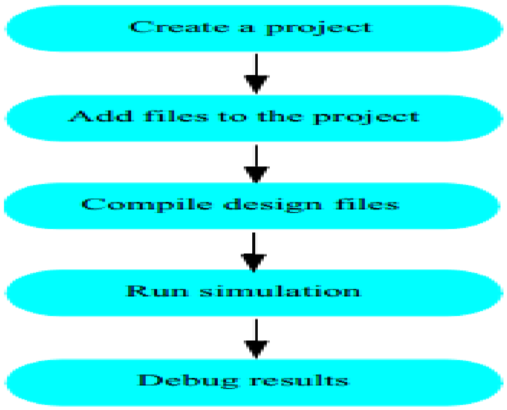
ModelSim is a very powerful simulation environment, and as such can be difficult to master. Thankfully with the advent of Xilinx Project Navigator 6.2i, the Xilinx tools can take care of launching ModelSim to simulate most projects. However, a rather large flaw in Xilinx Project Navigator 6.2i is its inability to correctly handle test benches which instantiate multiple modules. To correctly simulate a test bench which instantiates multiple modules, you will need to create and use a ModelSim project manually. Model Sim is a simulation and debugging tool for VHDL, Verilog, and mixed-language designs.

Basic simulation flow



Project flow

A project is a collection mechanism for an HDL design under specification or test. Even though you don't have to use projects in ModelSim, they may ease interaction with the tool and are useful for organizing files and specifying simulation settings. The following diagram shows the basic steps for simulating a design within a ModelSim project



2.1.4 VERILOG

Verilog, standardized as IEEE 1364, is a hardware description language (HDL) used to model electronic systems. It is most commonly used in the design and verification of digital circuits at the register-transfer level of abstraction. It is also used in the verification of analog circuits and mixed-signal circuits.

Verilog HDL is one of the two most common Hardware Description Languages (HDL) used by integrated circuit (IC) designers. The other one is VHDL. HDL's allows the design to be simulated earlier in the design cycle in order to correct errors or experiment with different architectures. Designs described in HDL are technology-independent, easy to design and debug, and are usually more readable than schematics, particularly for large circuits.

Verilog can be used to describe designs at four levels of abstraction:

(i) Algorithmic level (much like c code with if, case and loop statements).

(ii) Register transfer level (RTL uses registers connected by Boolean equations).

(iii) Gate level (interconnected AND, NOR etc.).

(iv) Switch level (the switches are MOS transistors inside gates).

3. RESULTS AND DISCUSSION :

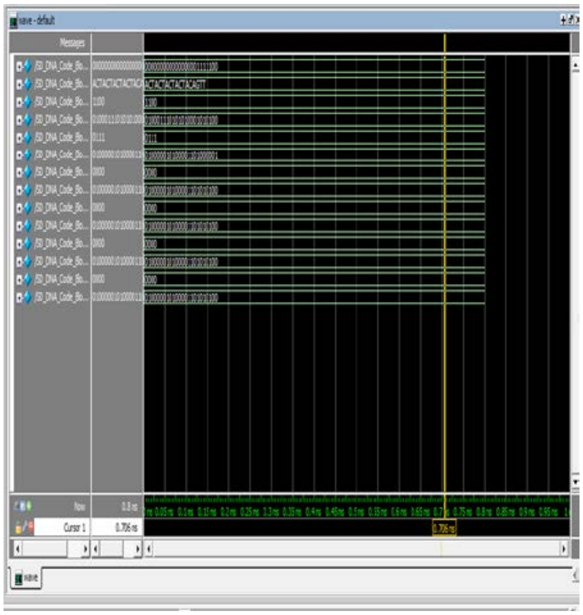


Fig. Key to DNA key encode operation

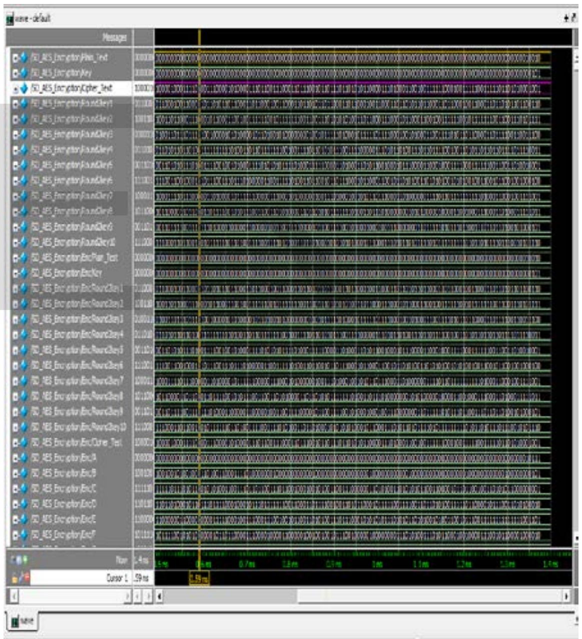


Fig. AES encryption

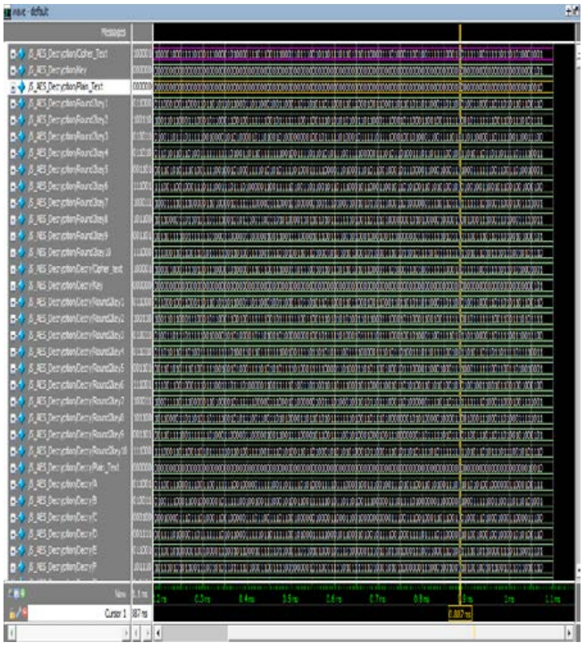


Fig. AES decryption

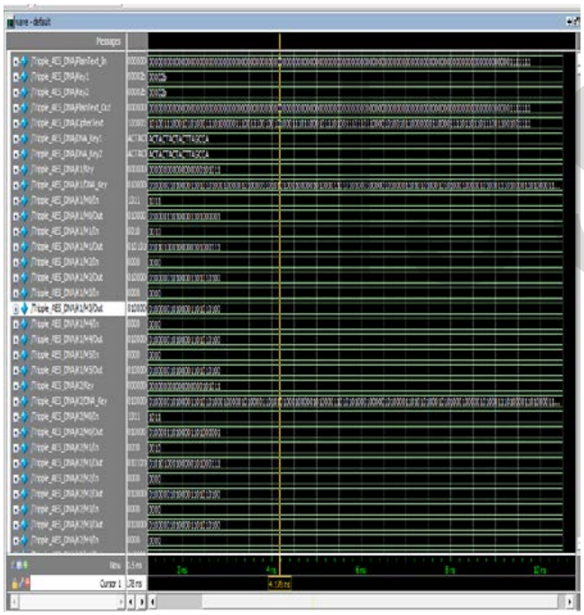


Fig. Triple AES with DNA key snap shot

ADVANTAGES

- Triple AES is more secure (it is less susceptible to cryptanalysis than 3DES).
- Triple AES supports larger key sizes than 3DES's 112 bytes.
- Triple AES is faster in both hardware and software.
- Triple AES's 128-bit block size makes it less open to attacks via the birthday problem than 3DES with its 64-bit block size.
- AES is required by the latest U.S. and international standards.
- High efficiency of gray code key
- High reliability

3. CONCLUSION

This project gives a concise outline about cryptography, quantum cryptography and DNA based cryptography. Information about technologies used in DNA is also provided here. It also discusses about secure message transfer between two systems. The proposed system is computationally is more efficient, they provide best security and are faster to execute.

5. REFERENCES

[1] AtulKahate: “Cryptography and Network security” Tata McGraw Hill Education Pvt. Ltd (2nd edition 2003).

[2] William Stallings. “Cryptography and Network Security”, Third Edition, Prentice Hall International, 2003.

[3] Behrouz A.Forouzan:” Cryptography and Network security” McGraw Hill companies (special Indian edition, 2007).

[4] G. Cui, L. Qin, Y. Wang and X. Zhang, “Information security technology based on DNA computing”, Proc. of the 2007 IEEE International Workshop on Anti-counterfeiting, Security, Identification, Xiamen, China, pp.288-291, 2007.

[5] K. Tanaka, A. Okamoto and I. Saito, Public - key system using DNA as a one-way function for key distribution, Bios stems, vol.81, no.1, pp.25-29, 2005.

[6] A.Gehani, T.LaBean, and J.Reif, “DNA-based Cryptography”, Lecture notes in Computer Science, Springer, 2004.

[7] Ashish Gehani, Thomas LaBean and John Reif. DNA-Based Cryptography.DIMACS DNA Based Computers V, American Mathematical Society, 2000.

[8] Ashish Gehani, Thomas LaBean and John Reif.DNA-Based Cryptography.DIMACS DNA Based Computers V, American Mathematical Society, 2000.

[9] Gehani Ashish, La Bean, Thomas H. Reif, JohnH, “DNA-Based Cryptography”, Department of Computer Science, Duke University, June 1999.