ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

A single, triple chaotic cryptography using chaos in digital filter and its own comparison to DES and AES

G.Neelavathi[1], A.Prasanna[2]

Assistant Professor[1]/ VLSI Design PG scholar[2]

Department of ECE, Knowledge Institute of Technology, Salem.

ABSTRACT

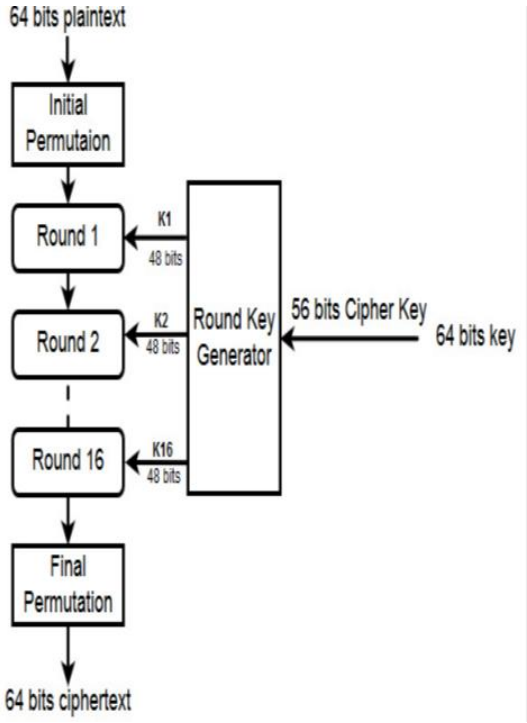
The Data Encryption Standard (DES) of the multimedia cryptography possesses the weak point of key conducting that is why it reaches to the triple form of DES. However, the triple DES obtains the better characteristic to secure the protection of data to against the attacks, it still contains an extremely inappropriate performance (speed) and efficiency in doing so. This paper provides the effective performance and the results of a single and triple chaotic cryptography using chaos in digital filter, compare to DES and triple DES. Finally the implementation aspects of a single chaotic cryptography using chaos in digital filter can stand efficiently as better performance with the small complexity algorithm, points out the resemblances to DES and triple DES with the similar security confirmation results without reaching to the triple form of the structure.

INTRODUCTION

Digital image information has been widely communicated over the Internet and wireless networks owing to the rapid advancements in the multimedia and communication technology. Meanwhile, the protection of digital image information against illegal usage has become an important issue. A direct and obvious way to protect image data from unauthorized eavesdropping is to employ an encryption algorithm. Unfortunately, the renowned block ciphers, such as Triple-DES, AES, and IDEA, are not suitable for practical image encryption. This is because the security of these algorithms is mainly ensured by their high computational cost, making them hard to meet the demand for online communications when dealing with digital images characterized by bulk data capacity. To meet this challenge, many different encryption technologies have been proposed. Among them, the chaos-based algorithms provide an optimal trade-off between security and efficiency. The permutation-substitution network, introduced the communication theory of secrecy systems, and now a guiding principle for the design of a secure cipher, is adopted in her approach. In each round of the cipher, the data positions are firstly scrambled in a secret way, which leads to a great reduction in the correlation among neighboring data. Then, the bit values are altered sequentially and the influence of each bit is diffused to all its succeeding ones during the modification process. With such a structure, a minor change in one bit of the plain-image may result in a totally different cipher-text with several overall rounds of encryption. Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The technique of concealing plaintext in order to hide its particular material is called encryption. The impression of encryption is to make a message incomprehensible, except to the receiver. Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text.

Author for correspondence:
Department of ECE, Knowledge Institute of Technology, Salem.

Encryption is used to guarantee the hidden information from anyone of concern not intended to,even those who can comprehend the encrypted data. The procedure of backsliding cipher text toits original plaintext is considered as decryption.



LITERATURE SURVEY

Leon.Chua (2006), [2] describe the second-order digital filter, when implemented using a 2's complement arithmetic for the addition operation, can exhibit chaotic behavior for certain region in the parameter space. The overflow nonlinearity of the adder results in a rather complex dynamics whose phase portrait is self-similar and has a fractal geometry. The intricate chaotic dynamics of this "nonlinear" digital filter is analyzed in symbolic dynamics involving symbols**.**

William Stallings (2007) describes in different Part at his book: Part One: Provides a survey of symmetric encryption, including classical and modern algorithms at. The emphasis is on the two most important algorithms, the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). This part also covers the most important stream encryption algorithm, RC4, and the important topic of pseudorandom number generation. Part Two: Provides a survey of Asymmetric Ciphers including RSA (Rivest-Shamir-Adelman) and elliptic curve. Part Three: Begins with a survey of cryptographic hash functions. This part then covers two approaches to data integrity that rely on cryptographic hash functions: message authentication codes and digital signatures.

S. Lian et al (2008), The Data Encryption Standard (DES) of the multimedia cryptography possesses the weak point of key conducting that is why it reaches to the triple form of DES. However, the triple DES obtains the better characteristic to secure the protection of data to against the attacks, it still contains an extremely inappropriate performance (speed) and efficiency in doing so. This paper provides the effective performance and the results of a single and triple chaotic cryptography using chaos in digital filter, compare to DES and triple DES. This comparison has been made pair-to-pair of single structure respectively to the triple form. Finally the implementation aspects of a single chaotic cryptography using chaos in digital filter can stand efficiently as better performance speed with the small complexity

algorithm, points out the resemblances to DES and triple DES with the similar security .

PROPOSED METHODOLOGY

Data encryption standard (des)

DES is a 64 bits block cipher which work with 64 bits of data per time. It uses 64 bits key input, but only 56 bits of the key will be used inside the operation. In this technique it is used as iteration process that is known as Round. The whole process consist of 16 rounds. For the structure of triple DES is the combination of three time of single DES by using the key bundle in order to generate K1, K2 and K3.

The detail of encryptor is show as below:
Cipher-Image = EK3 (DK2(EK1(Plain-Image)))

For the decryptor is the inverse form of the encryptor only by exchanging the Encrypted process to Decrypted process and Decrypted process to Encrypted process. DES is based on a cipher known as the Feistel block cipher.

Des algorithm

DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and Ri which are then passed into what is known as a round(see figure 3.2), of which there are 16 (the subscript i in Li and Ri indicates the current round).

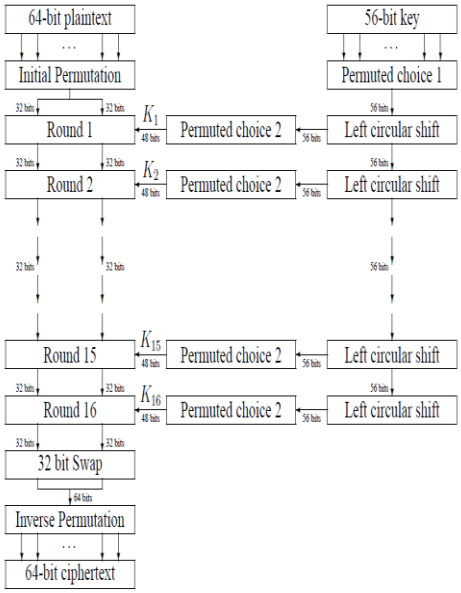


Figure Flow diagram of DES algorithm

Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. Clearly these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the cipher text and either the plaintext or key6. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text.

DES round function

DES uses 16 rounds. Each round of DES is a Feistel cipher, as shown in Figure

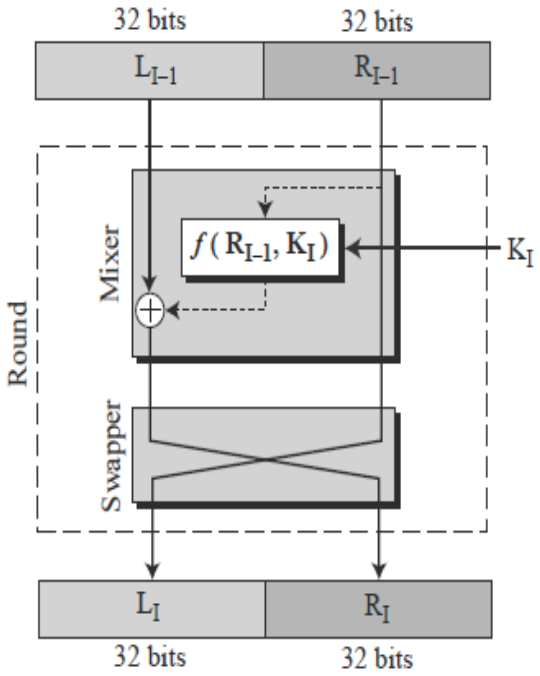


Figure Round in DES (encryption site)

The round takes LI−1 and RI−1 from previous round (or the initial permutation box) and creates LI and RI, which go to the next round (or final permutation box). Assume that each round has two cipher elements (mixer and swapper). Each of these elements is invertible. The swapper is obviously invertible. It swaps the left half of the text with the right half. The mixer is invertible because of the XOR operation. All noninvertible elements are collected inside the function ***f*** (RI−1, KI).

Description

Advanced encrypted system

The proposed structure for data encryption using chaos in digital filter is composed by two main parts. First is the key generator which is made up with the input of 16 characters (128 bits). Second is the encryption engine which uses only one all-pole digital filter to perform the process.

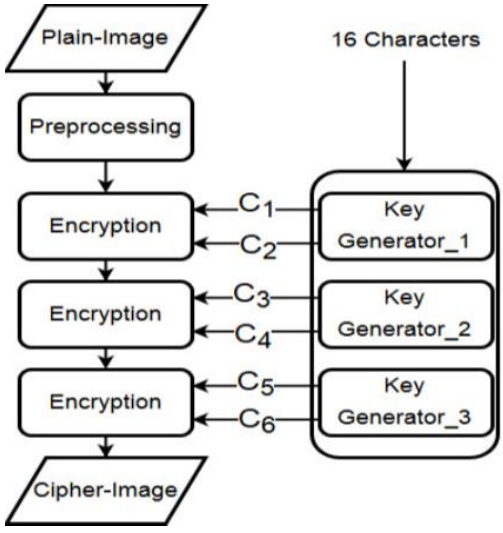


Figure Block diagram of AES

The system provides the value as key sensitivity and high security confirmation. The concept of triple DES and followed the structure of single chaotic cryptography. But for the coefficients of each filters of encryption engine are produced by different sub key generators which have different made up coefficients but the same input of 16 characters. The strong security over the single form is it has more initialed values than the single. For its triple form is made as the concept of triple DES and followed the structure of single chaotic cryptography. But for the coefficients of each filters of encryption engine are produced by different sub key generators which have different made up coefficients but the same input of 16 characters. The strong security over the single form is it has more initialed values than the single.

Software description

Model sim

Modelsim is a hardware simulation and debug environment primarily targeted at smaller ASIC and FPGA design. Modelsim combines simulation performance and capacity with the code coverage and debugging capabilities required to simulate multiple blocks and systems and attain ASIC gate-level sign-off. Comprehensive support of Verilog, System Verilog for Design, VHDL, and SystemC provide a solid foundation for single and multi-language design verification environments. Modelsim easy to use and unified debug and simulation environment provide today's FPGA designers both the advanced capabilities that they are growing to need and the environment that makes their work productive. Modelsim is a verification and simulation tool for VHDL, Verilog, System Verilog, and mixed language designs.

Basic simulation flow

The following diagram shows the basic steps for simulating a design in ModelSim.

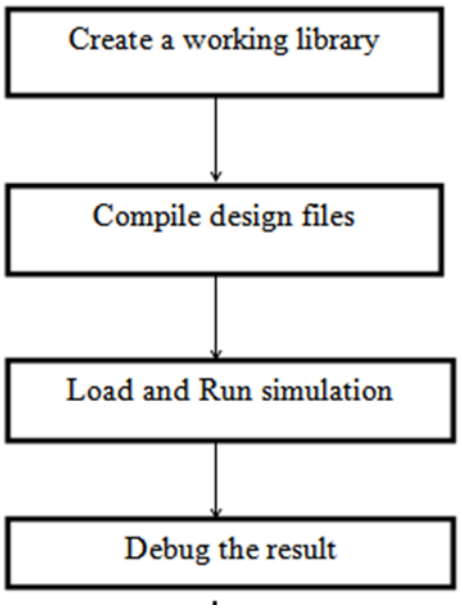


Figure Basic Simulation Flow

Creating the Working Library, in Modelsim, all designs are compiled into a library. Now typically start a new simulation in Modelsim by creating a working library called "work," which is the default library name used by the compiler as the default destination for compiled design units compiling the Design. After creating the working library the Modelsim library format is compatible across all supported platforms. It can simulate the design on any platform without having to recompile the

design. Loading the Simulator with the Design and Running the Simulation. With the design compiled, load the simulator with the design by invoking the simulator on a top-level module (Verilog) or a configuration or entity/architecture pair (VHDL). Assuming the design loads successfully, the simulation time is set to zero, and you enter a run command to begin simulation. Debugging the Result and unable to get the results expect, it can be used with Modelsim robust debugging environment to track down the cause of the problem.

RESULTS AND DISCUSSION

Simulation test

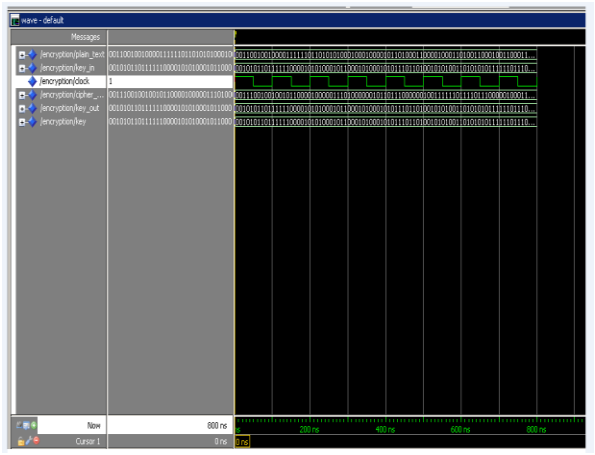


Figure Encryption module

Figure Encryption substitute bytes

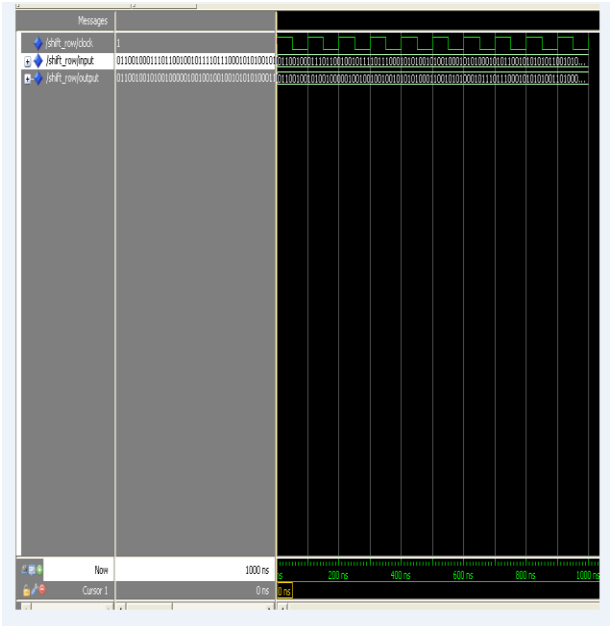


Figure Encryption shift row generation

Figure Encryption mix column

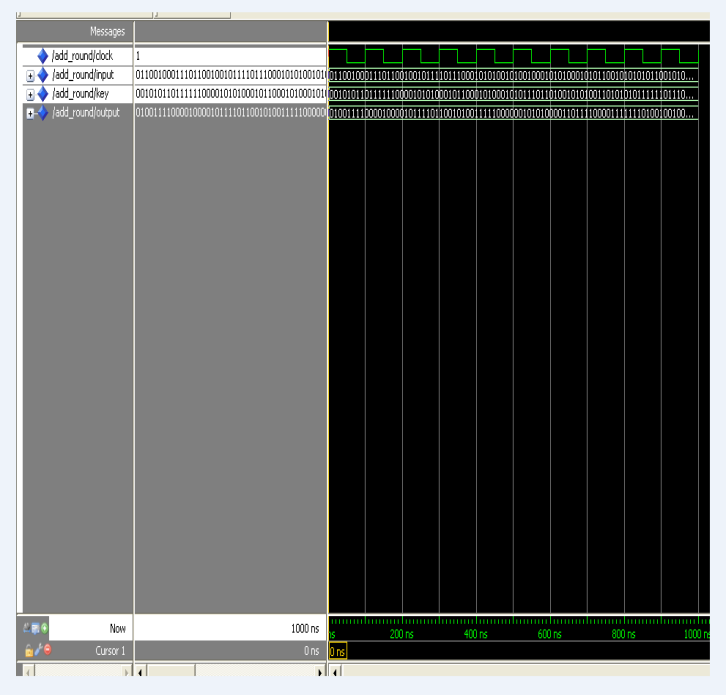


Figure Encryption add round key

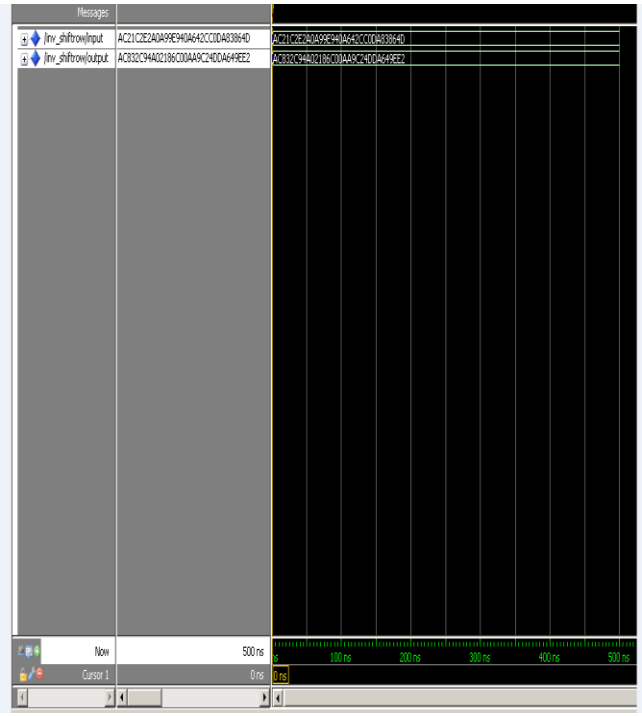


Figure Decryption inverse shift rows

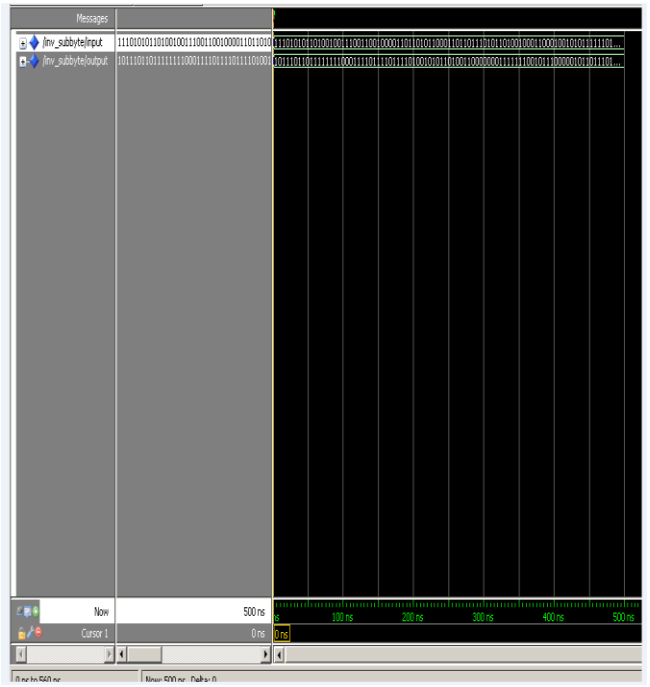


Figure Decryption inverse substitute bytes

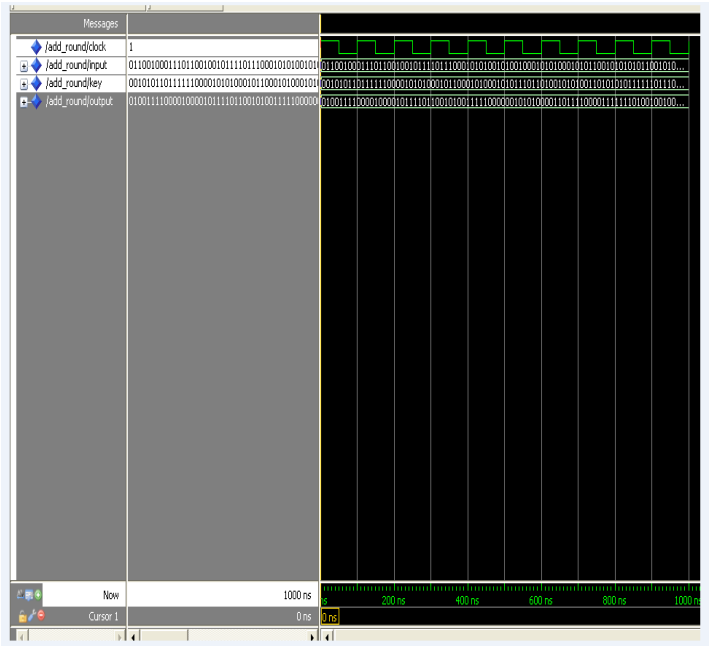


Figure Decryption add round key

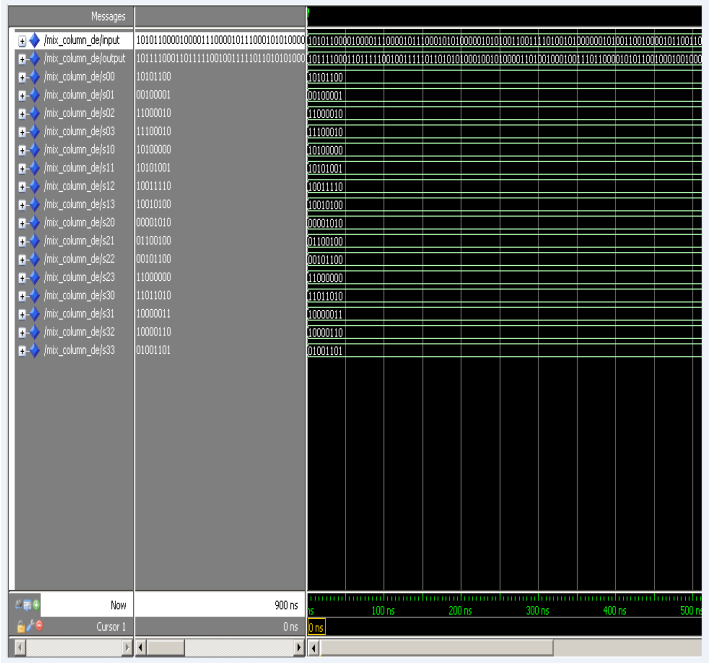


Figure Decryption inverse mix column

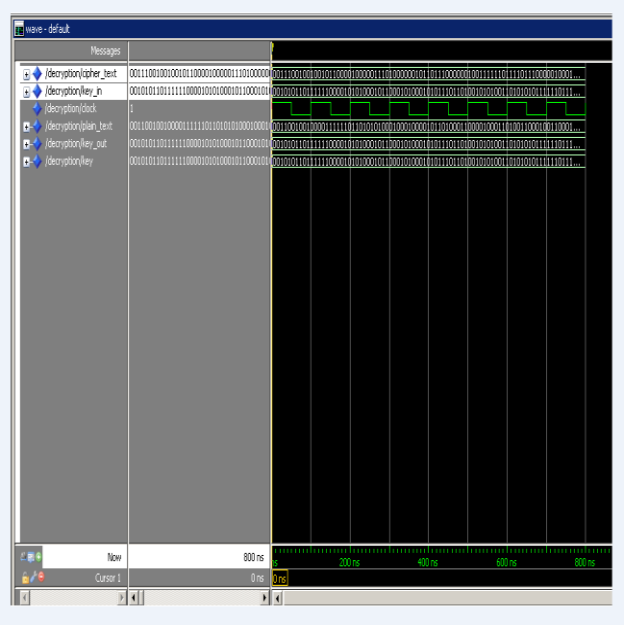


Figure Decrypted module

CONCLUSION

In general, any channel which can carry information from a secure area to the outside should be studied as a potential risk. Implementation-specific timing characteristics provide one such channel and can sometimes be used to compromise secret keys. Vulnerable algorithms, protocols, and systems need to be revised to incorporate measures to resist timing cryptanalysis and related attacks. The security confirmation of each technique provided the similar exclamation while produced different performance of complexity running. A single form of chaotic cryptography in digital filter can obtain the best outstanding consideration among others.

REFERENCE

[1]. S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.
[2]. L. O. Chua and T. Lin, ‘‘Chaos in digital filters,’’ IEEE Trans. Circuits Systs., vol. 35, no. 6, pp. 648-658, June 2009.
[3]. M-S. Liu, Y. Zhang, J. li, “Research on Improving Security of DES by Chaotic Mapping” IEEE, Proceedings of the 8th International Conference on Machine Learning and Cybernetics, Baoding, pp. 12-15, Jul 2009. K. Elissa, “Title of paper if known,” unpublished.
[4]. Teng, P. Y., Huang, S. I., ―Multilevel Data Encryption & Decryption System and Method Thereof‖, Industrial Technology Research Institute, 2009.
[5]. C. Shannon, “Communication theory of secrecy system”, Bell systemTechnical Journal 28:656-715, 2011.
[6]. M. George and A. Ioannis, “Cryptography with Chaos”, Proceeding 5th Chaotic Modeling and simulation International Conference, June 2012
[7]. M. Ebrahim, S. Khan and U. B. Khalid, “Symmetric Algorithm Survey:A Comparative Analysis”, International Journal of Computer Applications (0975-8887) Volume 61-No. 20, January 2013
[8]. B.J. Saha, Arun, K.K. Kabi and C. “A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color Images” 2014 international Conference on Circuit, Power and Computing Technologies [ICCPCT].
[9]. P. Reatrey, C. Sorawat and P. Jaruwit, “A New Key Generator for DataEncryption Using Chaos in Digital Filter”, 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC 2017), 4-5 August 2017, Shah Aam, Malaysia.
[10]. S. Soni, H. Agrawal and M. Sharma, “Analysis and Comparisonbetween AES and DES Cryptographic Algorithm”, IJEIT 2017.