Implementation of Three Fish Cipher Algorithm to Achieve Secured Communication

Vadthyavath Vijaya¹, Ramavath Anusuria²

¹Department of Electronic Communication Engineering, Sreyas Institute of Engineering and Technology, Hyderabad, Telangana, (India)
²Asst. Professor, Department of Electronic Communication Engineering, TKRCET, Telangana, (India).

ABSTRACT
The prime requirement of everyone is to see the secure communication in our life. Now a day’s the security has became utmost aspect of life. Password can be used like, numbers, letters and biometrics with cryptography technique. In this report various encryption and description algorithms were studied, description standard data is used for data security and implementation of Three-Fish Cipher algorithm with minimum number of overheads and then compile, simulate and test with the help of Xilinx ISE software and compare the proposed work with test bench.

Key Index: Secure communication, Three-Fish Cipher algorithm, Xilinx ISE software.

INTRODUCTION

SECURED COMMUNICATIONS

Secured communication against network is increasing significantly with time. Our communication media should also be secure and confidential. Cryptanalysis is the study used to describe the methods of code-breaking or cracking the code without using the security information, usually used by hackers. For this purpose, the following things can be done by the sender/receiver.

- One can transmit the message secretly, so that it can be saved from hackers.
- The sender ensures that the message arrives to the desired destination.
- The receiver ensures that the received message is in its original form and coming from the authenticate person.

The confidentiality of information that cryptography can provide is useful not only for the legitimate purposes of preventing information crimes e.g. the theft of trade secrets or unauthorized disclosure of sensitive medical records but also for illegitimate purposes e.g., shielding from law enforcement officials a conversation between two terrorists planning to bomb a building. In order to achieve the same one can use two techniques, (i) one can use invisible ink for writing the message or can send the message through the confidential person, and (ii) use of scientific approach called “Cryptography”. The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. It is used in applications present in technologically advanced societies; it includes the security of ATM cards, computer passwords, and electronic commerce.

![Schematic Model diagram of Secured Communication](image)

Fig.1. Schematic Model diagram of Secured Communication

But the most recognized form of cryptography is its use encipher and decipher information, thus keeping its contents guarded against unauthorized disclosure. There are two classes of key-based encryption algorithms: symmetric and asymmetric algorithms. Symmetric algorithms use the same key for encryption and decryption, whereas asymmetric algorithms use different keys for encryption and decryption. Ideally it is infeasible to compute the decryption key from the encryption key.
CRYPTOGRAPHY

It is a technique used to avoid an unauthorized access of data. It helps to provide accountability fairness and accuracy and also provide confidentiality. Broadly, four different kinds of people contributed their efforts in this technique and are: (i) Military, (ii) The Diplomatic Corps, (iii) Diarists, and (iv) Communications System.

Cryptography involves two basic operations and is named as encryption and key management. Information/data can be encrypted using a cryptographic algorithm by various keys. The security of cryptographic system is not only dependent on the encryption algorithm; it also depends upon the keys used for the encryption. These keys are always kept secured from the hacker and are known as secret key. Key plays an important role in encryption process, which is a main part of cryptography. Due to channel impairments sometimes the transmitted data and/or key may get corrupted. If it is slightly changed or corrupted, the data will not be recovered; therefore, key needs to be transported over the secured channel. The frequency of use of a cryptographic key always has a direct correlation to how often the key should be changed. Encryption algorithms can be hacked by utilizing supercomputer which provides fast speed and allows the hacker to use more permutations and combinations in a specified time. Modern era depends upon wireless communication and almost all the electronic funds are being carried out online. In order to protect the same and maintain the privacy of the users; cryptography is the best solution due to their better response even in the presence of advisory. For better security, either more number of keys is used or the length of the existing keys is increased. In both the approaches the overheads are increased, therefore, the best idea is to use sub-keys. Sub-keys are used only for such nodes which are attacked by the hacker.

The sub keys are always derived from the main key which helps in reducing the overheads. The basic cryptographic model has been shown in figure 1.1. It involves encryption and decryption section; initially, the data has been encrypted by the help of key and further transmitted over the web. Finally, it has been received and the encrypted data is decrypted with the help of same or different key. The key is any value and/or word and is used in both the sections for encryption and decryption purpose.

![Fig.2. Schematic diagram of Basic Cryptographic Model](image-url)
RESULTS AND CONCLUSION

Following are simulated results of three fish block cipher algorithm implemented in virtex-5 kit with the help of Xilinx ISE 12.1.

![Block Diagram of Three Fish Cipher In Xilinx](Fig.3)

The figure shows block diagram of encryption decryption and key scheduling blocks with plaintext as input, key K and tweaked input and cipher text as output from encryption block and deciphered text is obtained as output from decryption block.

Key scheduler tweaked input and plain text:

- key = $256'h3663586286256826862927927972576642749794249275223732$;
- tweak = $128'h93448681648614861648618468126486$;
- plain_text = $256'h98567345678342556436856834656836586856564865863564863856$;

Following shows ciphered text as output:
Fig. 4 Ciphered Outputs

Fig. 5. Deciphered Outputs
CONCLUSION

- The information security can easily be achieved by cryptography algorithm techniques a large number of encryption algorithm have been developed for securing confidential data from the cyberpunks. The aim of current Cryptography is to prevent data from hackers. The strength of the system is dependent on the length of the key. But to achieve this a large computational time is required, giving a large delay which can be harmful to us.

- The use of FPGAs can help us to improve this limitation because FPGAs can give enhanced speed. This is due to fact that the hardware implementation of most encryption algorithms can be done on FPGA. The proposed scheme for three fish cipher algorithm has been optimized on the time required to generate the keys or decode data. The algorithm and coding has been implemented on Xilinx ISE software with the help of Verilog HDL language. The synthesis has been done on Xilinx FPGA (Xilinx 12.1c) and the faster clock frequency has been observed in comparison with classical DES.

- It has been observed that it takes 19 nanoseconds for the input data of size 8 bytes while the technique by which the algorithm has been implemented in this thesis using Verilog HDL has reduced the time to 14.2 nanoseconds for 32bytes. The improvement has been observed to be 45.78% as compared to classical DES technique.

REFERENCES


