23. Cryptography on Digital Implementation with Steganography Techniques

Harsh Sahay, Assistant Professor ,Department of Computer Science and Engineering

DAV Institute of Engineering and Technology,Betla Road Palamau,Daltonganj,

822126,India sahayharsh53@gmail.com

ABSTRACT

Cryptography can be implemented by digital circuits. The messages those are sent are passed through digital circuits. Digital design generates cipher text. This cipher text is hidden by steganography techniques and are sent to the networks. To the receiver side by the reverse process of steganography generates cipher text and by the process of decryption original message is received to the receiver side.

Keywords— *Cryptography, Steganography, Digital Design*

INTRODUCTION

In recent trends internet provides communication between peoples, defense personals, gives facility to electronic payment and many others. This is reason behind much concern of privacy, identifying theft, security etc. Recently, due to the large losses from illegal data access, data security has become an important issue for public, private and defense organizations.

In order to protect valuable data or information from unauthorized access, illegal modifications and reproduction, various types of cryptographic techniques are used. [1]There are two kinds of cryptography symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography same key is used between the sender and receiver. While in asymmetric key cryptography two different keys (public key and private key) are used between sender and receiver for encryption and decryption.RSA is most famous asymmetric cryptography algorithm. Some security services can be implemented using cryptography. Cryptography, a word with greek origin, means secret writing. To the science and art of transforming messages to make them secure and immune to attacks. Cryptography is the art of achieving security by encoding messages to make them non readable.[1] Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

The word cryptography has Greek origin it is combination of two,"Kryptos" which means hidden and "logos" which means word and graph, means secret and writing. Cryptography is a science of converting a stream of text into coded form in such a way that only the sender and receiver of the coded text can decode the text. Cryptography plays a very important role in internet based commercial activities as many secret documents which include payment details, money transfer, contract documents, and business plans and other confidential information are to be transferred from one computer to another computer. Cryptography is a technique that allows a piece of information to be converted into cyptic form before being stored in a computer database or transmit over the secure channel. Encryption of message is done to provide extra protection in order to maintain confidentiality of documents. For example, if an unauthorized person succeeds in tapping the channel then information he has copied may not be of his use, if it is encrypted. Cryptography is primarily used to protect the confidentiality of information from intruders. There are two kinds of cryptography Asynchronous Key Cryptography Synchronous Key Cryptography In synchronous key cryptography one key is shared between sender and receiver. While in Asynchronous key cryptography two key is shared between sender and receiver. One is called public key which is publically available while another is called private key, which is kept secret. Steganography is the process of hiding data into a medium such that medium appears to be unsuspicious.

Combination between cryptography and Steganography is done by first encrypting data using encryption techniques and hiding it into transportation medium using an Steganography techniques (Atito et. al. 2012).

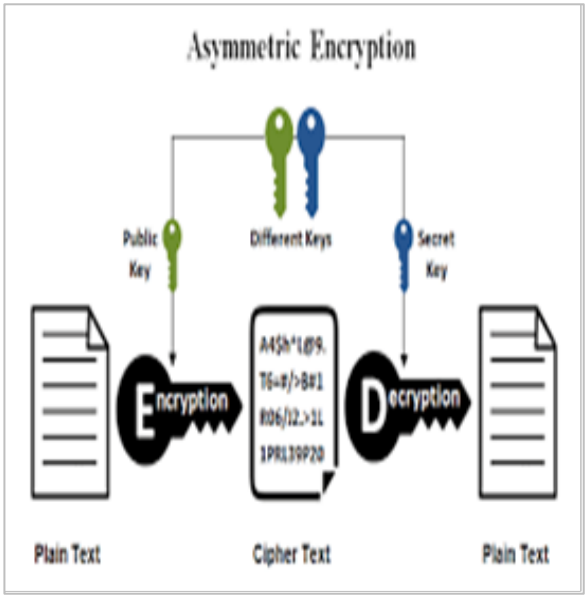

Figure 23-1 Cryptography concept

RELATED WORK

Rivest, Adi Shamir and Adelman has invented RSA algorithm which it is widely most used public key cryptosystem, this algorithm used to encrypt the data to provide security [3]. Vivek Choudhary and Mr. N. Praveen have proposed modification of RSA algorithm by the use of third prime number in their work, which increases security of RSA algorithm.[4]. Samiha Marwan, Ahmed Sawish, Khaled Nagaty developed DNA based cryptographic methods for data hiding in DNA Media. [5]. Alaa Hussein, Al-Hamami and Ibrahem Abdallah Aldariseh proposed enhancing the RSA algorithm; in this RSA algorithm they used additional third prime number in the composition of the private and public key. Because of additional prime number the factoring complexity of variable (n) is also increase. [6].

A. STEGANOGRAPHY

Steganography is a technique that facilitating of a message that is to kept secret inside other messages. This result is the concealment of the secret messages itself! Historically, the sender used methods such as invisible ink, tiny pin punctures on specific characters, minute variation between handwritten characters, pencil marks on handwritten characters etc.Of late, people hide secret message within graphic images. For instance, suppose that we have secret message to send. We can take another image file and we can replace the last two right most bits of each of that image with (the next) two bits of our secret message. The resulting image would not look too different, and yet carry a secret message inside! The receiver would perform the opposite trick. [1]

B. DIGITAL DESIGN

The term digital is derived from the way computer perform operations, by counting digits. For many Years applications of digital electronics were confined to computer systems. Today the digital technology is applied in a wide range of areas in addition to computers. Such application as television, Communication systems, radar, navigations and guidance systems, military systems, medical instrumentation, industrial process control and consumer electronics uses digital techniques. Digital technology has progressed from vacuum tube circuits to discrete transistors to complex integrated circuits, some of which contain millions of transistors. [2] Digital

electronics is a field of electronics involving the study of digital signals and the engineering of devices that use or produce them.

Electronics is the science and technology concerned with the controlled flow of electrons and other carriers of electric charge. It covers theory, design, and construction of electronic devices, circuits, instruments, or systems. [7]In digital electronics digital outputs are generated from digital inputs. If the output of the logic circuit depends only on the present input values, we refer to the system as not having memory. Systems without memory are also known as combinatorial logic circuits because they combine inputs to produce the output. Combinatorial circuits can be constructed with gates alone. If, on the other hand, the output of the logic circuit depends on present as well as past input values, we then refer to such a circuit as having memory, because such circuits remember past input values. Systems with memory are also known as sequential logic circuits. Such circuits are more complicated and require some form of memory (flip-flops) and the presence of a clock signal to regulate the response of the circuit to new inputs, ensuring that the necessary operations occur in proper sequence–hence the name sequential logic circuit. We will first consider combinatorial circuits and then proceed to sequential ones.

Digital electronics is about designing and analyzing circuits and although this could be done using only the mathematical language of Boolean algebra introduced.

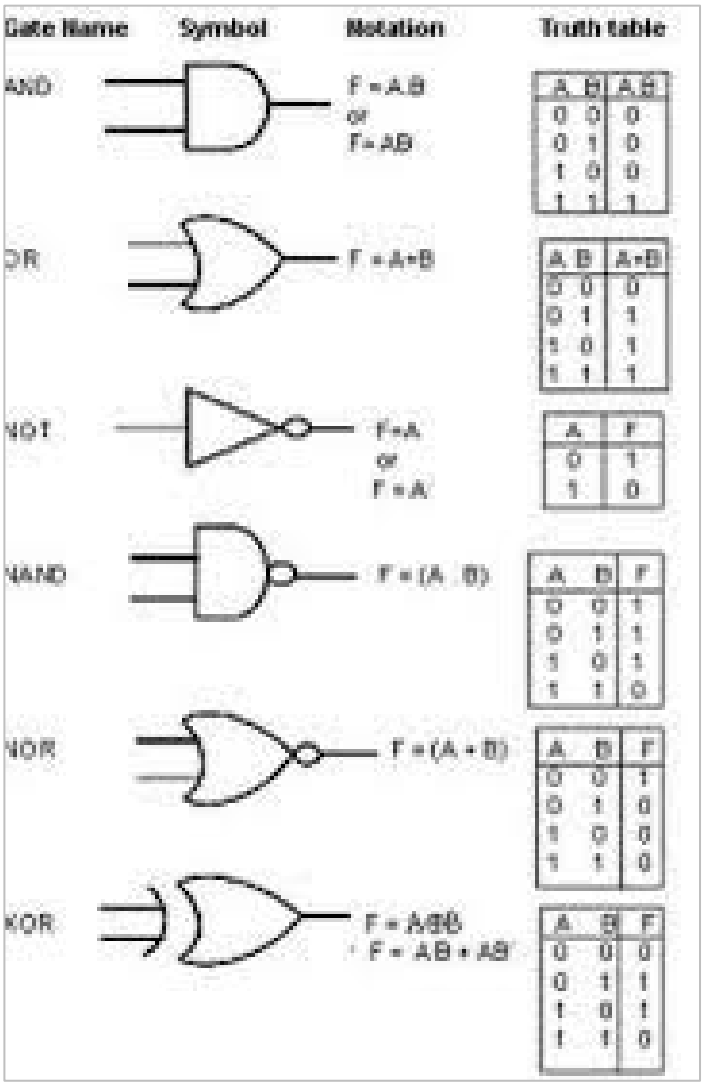

Figure 23-2 Full-Adder

C. HOW TO DESIGN

As we see the massages are sent in the form of bits, after going through digital circuit, it generates cipher text. In the receiver side by the reverse process of these digital circuits generates plain text to the receiver side. The cipher text can be hided by the technique of Steganography.

```
#include<stdio.h>
Int main()
{
Unsigned long long char b=0x32;
Unsigned long long int B;
Unsigned long long int  D;
//Encryption
B=b^0x0C;
printf (“\n%02x”,b);
D=B;
//Steganography
D=D<<2;
D=D>>2;
B=D;
//Decryption
B=B^0x0C
printf(“\n%02x”,b);
return 0;
}
```

As shown above we have initialize an unsigned integer b=0x32.It is exclusive ored with 0x0C, the result is stored at B.By two times left shift operation it is the case of Steganography. Now hidden data is sent to receiver. At the receiver side by the reverse process of Steganography technique, we are getting actual cipher text. In addition, by the process of decryption we are getting actual plaintext.

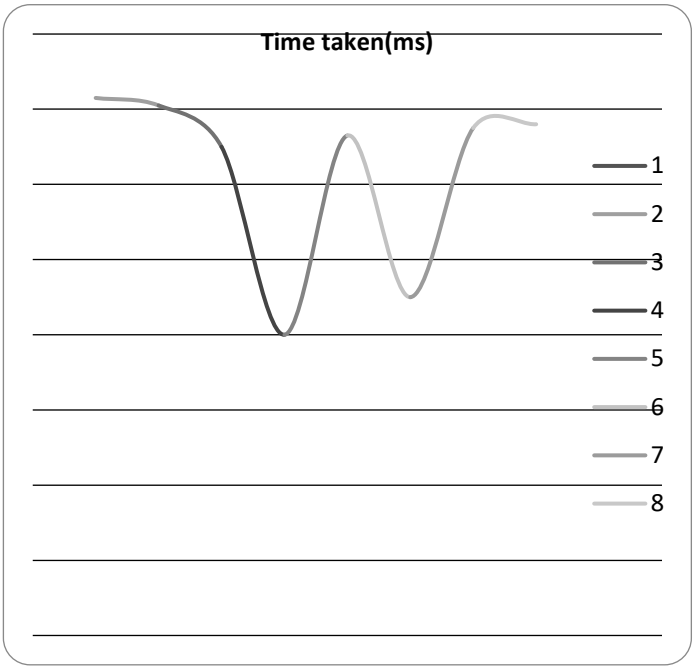

Figure 23-3 Obtained Result

CONCLUSION

Experimentally it is found that digital circuit design of plain text hides data efficiently in the form of cipher text, for hiding cipher text DNA steganography is used. So, it is very difficult for unauthorized parties to get a real plain text.

REFERENCES:

[1] Cryptography and Network security (Book), Atul Kahate, Cryptography Techniques, Introduction.

[2] Digital Fundamentals (Book), Floyd & Jain, Introductory Digital Concepts.

[3] R. L. Rivest, A. Shamir, L. Adelman, "On Digital Signatures and Public Key Cryptosystems," MI Laboratory for Computer Science Technical Memorandum 82, April 1977.

[4] Vivek Choudhary1 and Mr. N. Praveen2 "Enhanced RSA Cryptosystem Based on Three Prime Numbers" 1 Post Graduate Scholar, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India 2 Assistant Professor, Department of Computer Science & Engineering, SRM University, Chennai, Tamilnadu, India

[5] DNA based cryptographic technique for data hiding in DNA media Samiha Marwan, Ahmed Shawish, Khaled Nagaty.

[6] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE

[7] The University of Waikato Electronics 2020