Mehran University Research Journal of Engineering & Technology
Vol. 38, No. 3, 609-618 July 2019
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.1903.07

Routine of Encryption in Cognitive Radio Network

ASIF RAZA*, MUHAMMAD TANVEER MEERAN*, AND MUIZZUD-DIN**

RECEIVED ON 03.08.2017 ACCEPTED ON 17.08.2018

ABSTRACT

Today data transmission is very important through different channels. Need of network security comes to secure data transformation from one network to another network. As the complexity of the systems and the networks increases, weakness expands and the task of securing the networks is becomes more convoluted. Duty of securing is done by Cryptography techniques. A colossal amount of data is exchanged over public networks like the internet due to immense accommodation. This includes personal details and confidential information. It is important to prevent the data from falling into the wrong hands. So, due to this factor we use cryptography. Encryption and decryption are the basic terms that are used in cryptography. There are few algorithms which used including, AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) and BLOWFISH. The main contribution of this paper is to provide an algorithm that is useful for data transformation in cognitive radio networks. In this research, we have drawn a new symmetric key technique that is for the usage of cryptography which is helpful to make the data saved from others.

Key Words: Network Security, Cognitive Radio Network Cryptography, Encryption, Decryption, Data Encryption Standard.

1. INTRODUCTION

Technology now-a-days is common in our surroundings. With the passage of time, the transformation of data is increasing day by day and maintaining an old data in a system has gradually increases. Security is an important factor in transmission and saving the data. One important and essential aspect of communications is cryptography. Cryptography is the study of hiding information by converting the sensitive information into an unintelligible text using a suitable encryption technique so that it cannot be understood by any unintended individual, and then converting it back to its original form for the intended receiver using some decryption technique [1].

The cryptography has been used since ancient Roman and Egyptian empires. “Caesar Cipher” invented by

Authors E-Mail: (asifraza.raza14@gmail.com, tanveer_miran@yahoo.com, muizzud_din@hotmail.com)
* Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan.
** Department of Computer Science, Khawaja Fareed University, Rahim Yar Khan, Pakistan.

Julius Caesar is one such example. Now, the cryptography has been digitalized. Computer algorithms have modernized the art of cryptography. Cryptography has become an essential tool in protecting the sensitive information from unauthorized access and to provide information security. This technique has discovered its uses in defence and also in business field. Companies and firms use cryptography techniques to protect their data and information from their adversaries. It is also used to protect individual data and has extensive application in our daily lives [2].

Now-a-days there are four basic objectives of cryptography as mentioned in [3]. Confidentiality, Integrity, Non-Repudiation and Authentication. Sometimes cryptography is referred to as encryption. The basic part of encryption is to provide an irregular scrambled key and concealing the first information by making key and encode this with key and spare from gatecrasher. Encryption part is useful for securing the electronic transmission over unprotected systems.

Fig. 1 describes the encryption, decryption process. By using some specific algorithm between 'plaintext and key' the cipher text is obtained, and this cipher text is transferred to the receiver. To get plain text again on the receiving end, some specific operation are performed between cipher text and key. This is known as decryption process.

A CR (Cognitive Radio) is a system or radio that senses and make us aware of its operational environment and can dynamically and autonomously adjust its radio operating parameters accordingly [4-5].The CR technology works on the principle of dynamic spectrum access where secondary user utilizes spectrum hole [6-7]. The objectives of CR networks are to determine the spectrum holes, select the best spectrum opportunities to meet the user communication requirements and avoid from any harmful interference for a primary user. Transmission has its own importance in this network. This study explores the new technique of encryption and data transmission in network.

The rest of the paper is organized as follows: Section 2 briefly describes the Cryptography types and some popular algorithms that being used in the recent days. Section 3 outlines some issues found in old algorithms. Our proposed, new technique is presented in Section 4. Section 5 detailes implementation and Section 6 provides the performance evaluation of the proposed algorithm. The conclusion is included in Section 7.

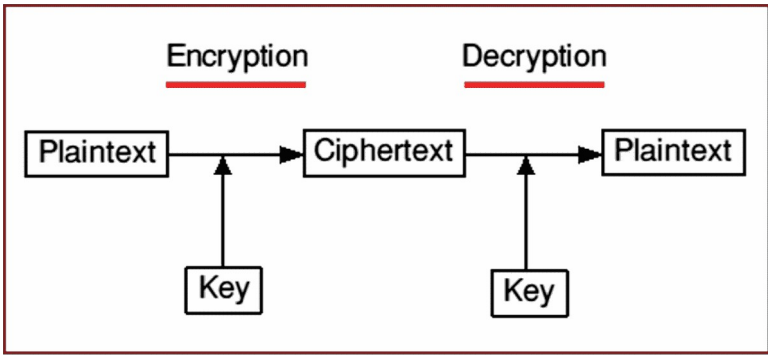

FIG. 1. MODEL FOR CRYPTOGRAPHY

2. CRYPTOGRAPHY TYPES

Basically Encryption has three types [8]

- Symmetric encryption
- Asymmetric Encryption
- Hashing

2.1 Symmetric Encryption

A sort of encryption that has just single key is often known as symmetric encryption [4]. It is one of the most widely used method of cryptography. There are different points of interest in this approach. Execution is decently high. This encryption technique is resonably secure (Fig. 2).

2.2 Asymmetric Encryption

Asymmetric encryption [9] utilizes two distinctive keys for encryption and decoding. The private key can just decode the encoded message [10]. No key, other than private key can be utilized for unscrambling (Fig. 3).

2.3 Hashing

Hash function is the one-way encryption method. Moreover, no key is required for encryption and decryption.

2.4 Related Work and Popular Algorithms

Almost 4000 years ago Cryptography [11-12] Concepts came in Egypt. Around in 2000 BC Hieroglyphics was

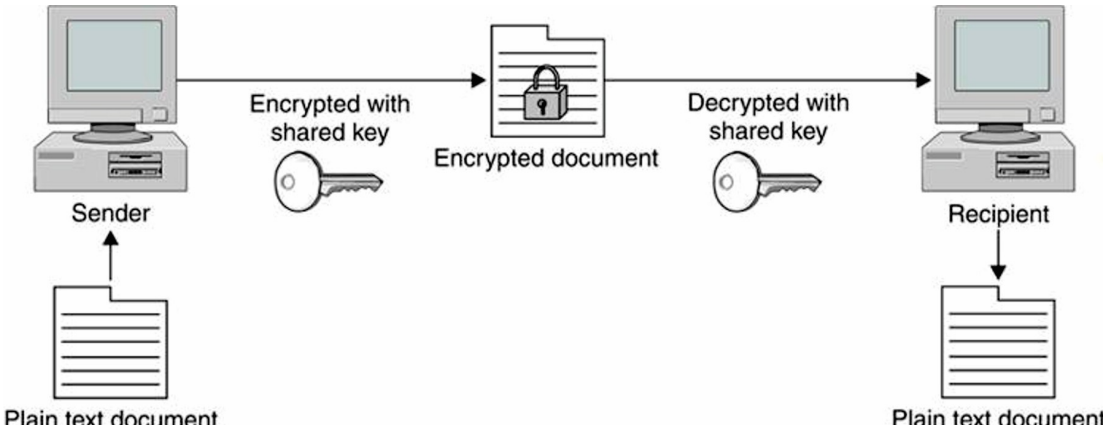

FIG. 2. SYMMETRIC ENCRYPTION

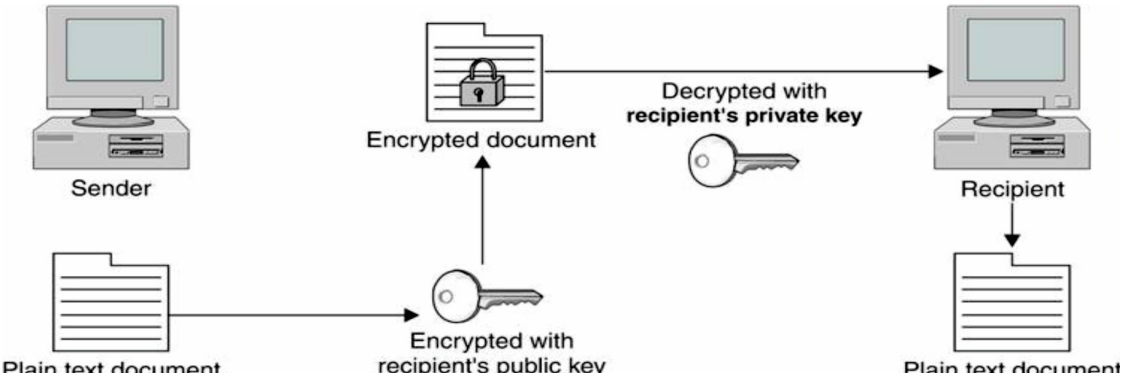

FIG. 3. ASYMMETRIC ENCRYPTION

used for the tombs decoration of deceased rulers and kings. Those symbols describeed the story of Kings and rulers lifestyle. Those symbols were cryptic in special meaning to describe the words. With the passage of time, deciphering the symbols has become more complicated and there is less interest in this approach.

The Arabs were the first that worked in this field. QALQASHANDI is an Arabic author who was the first to introduce the technique for solving the ciphers [13]. His method was based on writing the cipher text letters and after writing, the frequency of each symbol could be counted. By using the average frequency of each letter of language, the plain text could be written by using this technique. A Frenchman named ANTOINE ROSSIGNOL, had also worked on this. In 1628, he helped his army force to defeat the Huguenots by decrypting the captured message. His style for solving ciphers was based on methods of two lists.

Decius Wadsworth was the one who developed a cipher system in 1817. His cipher system was very helpful and used at the end of World War-II. His cipher system was consisted of two disks. The outer disk and the inner disk. The outer disk contained the 26 alphabets and 2-4 numbers and the inner disk had only 26 letters of alphabet. The disks were adapted to each other at the ratio of 26:33. To encipher a message, the internal plate was turned until the desired letter was at the top position with the quantity/number of turns required for this outcome as the ciphers. Because of adapting discs together, a cipher for a character could not be repeated till the all thirty-three characters were used for plaintext [14].

Tomography cipher was developed in 1859 by PLINY EARLE CHASE. His method of ciphering indicates that two-digit numbers can be allocated to every single character of text by method for table and these numbers were written at the end first numbers to form a row on the top of second numbers. A row that is on bottom side should be multiplied by 9 and correspondingly pairs are stored into table to make a cipher text.

Othere popular encryptions methods that exist in the cryptography are:

Punita and Sitender [15] AES is symmetric 128-bit block length and 128,192 and 256-bits key length data encryption technique to encrypt sensitive data which is used by US governments to protect important information. AES is included in the ISO/IEC 18033-3 standard [16].

Shah and Bhavika [17] DES introduced the DES algorithm [18]. The DES takes maximum of 2^{56} attempts to find the correct key. One of the main draw back in working with the DES is data vomiting due to lack of security for the data.

Stallings [19] 3DES is an extension of DES which involves repeating the basic DES algorithm three times using either two or three unique keys for a size of 112 or 168 bits [18].

3. ISSUES FOUND IN ALGORITHMS

There are number of issues found in the existing algorithms:

- Complex structure, and predictable due to short key length.

- The more complex structure of algorithm increases the time of execution. Therefore, the structure of algorithm must be simple to operate algorithm faster.
- The longer the length of the key, the higher the security. However, it affects the spped of execution of the algorithm [14].
- The overall performance of any algorithm depends upon the selection of mathematical and/or logical operations applied on plain text, key and cipher text.

In network security, there are two types of attacks. The former one is Active attack. Active attack tries to modify the systems resources and it affects operations performed on the system. The on the other hand, the passive attack is a try, which monitors the data transmission without affecting the operation performed in the system [20]. It is categorized as Eavesdropping, Collecting private data.

4. PROPOSED ALGORITHM

This section elaborates the security which we implemented for the plain text. Plain text and key are generated by using the ASCII (American Standard Code for Information Interchange) code. Proposed algorithm applies on plain text and obtained required cipher text, is more secure than prior algorithms. This algorithm is shown in Fig. 4.

5. IMPLEMENTATION OF ENCRYPTION

(1) Read the user file and Generate Corresponding ASCII value of each character in the file. Let us suppose user file has a word **Hi**, the ASCII of **H** is **072** and ASCII of **i** is **105**.

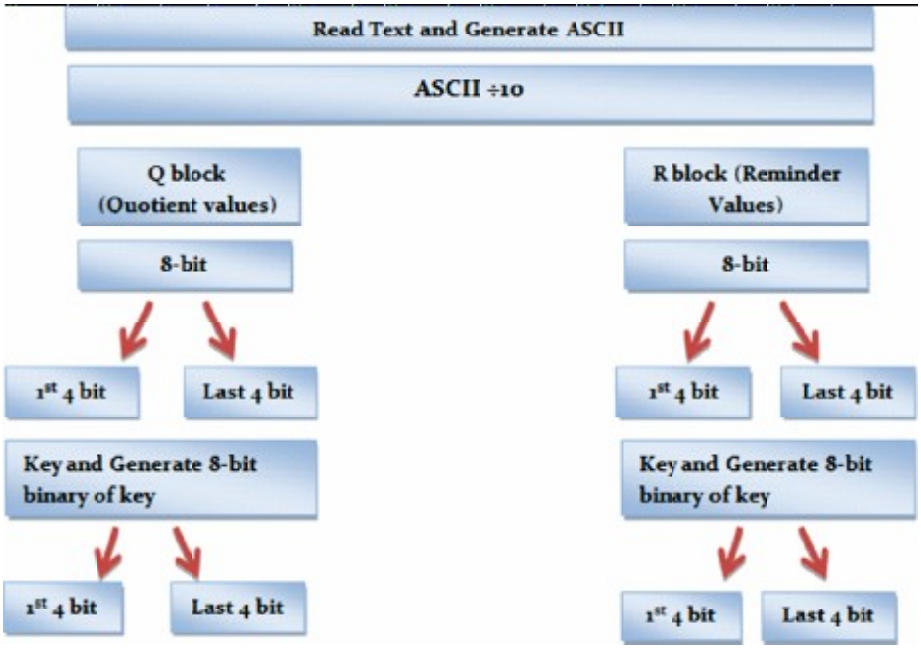

FIG. 4. PROPPSED ALGORITHM FOR ENCRYPTION

(2) Divide every character ASCII value by 10. Calculate Quotient. The Quotient values are stored in Q block and Reminder values are stored in R block e.g.

Q[7,10], R[2,5]

(3) Calculate 8-bit binary value for each value that is in R block and Q block correspondingly.

Q[00000111, 00001010], R[00000010, 00000101]

(4) Take key from user. Key should be set of one or more special character. Calculate ASCII value of sequence correspondingly and convert it into 8-bit binary. Let us suppose that user entered $$. ASCII is 3636 and binary is 00100100 00100100.

(5) Every 8-bit binary key is divided into 4 4 bits also Every 8-bit binary value in Q block and R block is divided in 4 4 bits correspondingly.

Key[key1	key2	key3	key4]
Key[0010	0100	0010	0100]
Q[Q1	A2	Q3	Q4]
Q[0000	0111	0000	1010]
R[R1	R2	R3	R4]
R[0000	0011	0000	0101]

(6) Take XORs of Q1 with Key2, Q2 with key1, and Q3 with key4 and Q4 with key3 also take XORs of R1 with key2 and R2 with key1, R3 with key4 and R4 with key3.

Q[Q1⊕key2 Q2⊕key1 Q3⊕key4 Q4⊕key3]
R[R1⊕key2 R2⊕key1 R3⊕key4 R4⊕key3]

(7) Obtain cipher blocks as Q¢ and R¢from pervious step. The result will be in this form.

Q′[Q1′	Q2′	Q3′	Q4′]
Q′[0100	0101	0100	1000]
R′[R1′	R2′	R3′	R4′]
R′[0100	0000	0100	0111]

(8) Combine Q¢ cipher text block and R¢ cipher text block by using sequence key (in bit form) in between Q¢ and R¢

Q′$$R′

0100101 01001000 00100100 00100100 01000000 01000111

(9) Convert each 8-bit into ASCII and Save ASCII value correspondingly. Finally get and save cipher text. Obtained result is EH$$@G. All this process implementation is illustrated in Fig. 5.

6. IMPLEMENTATION OF DECRYPTION

(1) Read cipher text, user entered Sequence key. Convert cipher text and key into binary value.

(2) Identify sequence key and remove. Two blocks obtained are Q' and R'

(3) Divide 8- bits of each block(Q¢ and R¢) in 4 4 bits and make a 4 4 bits of key

Q′[Q1′	Q2′	Q3′	Q4′]
Q′[0100	0101	0100	1000]
R′[R1′	R2′	R3′	R4′]
R′[0100	0000	0100	0111]
Key[ke1	key2	key3	key4]
Key[0010	0100	0010	0100]

(4) Take XORs as like

Q′[Q1′⊕key2 Q2′⊕key1 Q3′⊕key4 Q4′⊕key3]

R′[R1′⊕key2 R2′⊕key1 R3′⊕key4 R4′⊕key3]

(5) Combine the 4-8 bits and result obtained in theform of Q block and R block

Q[00000111 0001010]

R[00000010 00000101]

(6) Calculate ASCII value/symbols for each 8 bit in blocks.

Q[7,10], R[2,5]

(7) Multiply each value in Q block by 10 and after obtaining the result, add value from R block correspondingly. Obtained result is in this form

7x10=70, 10x10=100

70 + 2100 + 5 = 72105

(8) Take value correspondingly from ASCII table. Obtained result is **H** and **i**Cipher text was: **EH$$@G** Original text is **Hi**

7. EXPERIMENTAL FINDINGS OF ALGORITHM

Results are obtained using WINDOWS operating system and software used for implementation is Visual Studio 2010.

There are different bytes which indicate the execution time period of the algorithm. The experimental result are divided into three sections. Every section has different specifications.

7.1 Testing Results by Using HP G3450

Table 1 describes the different plain text of different bytes as an input by using system HP G3450, which is based on 5th generation with 8 GB RAM. Through this system the estimated execution time of encryption and decryption of plaintext can be measured.

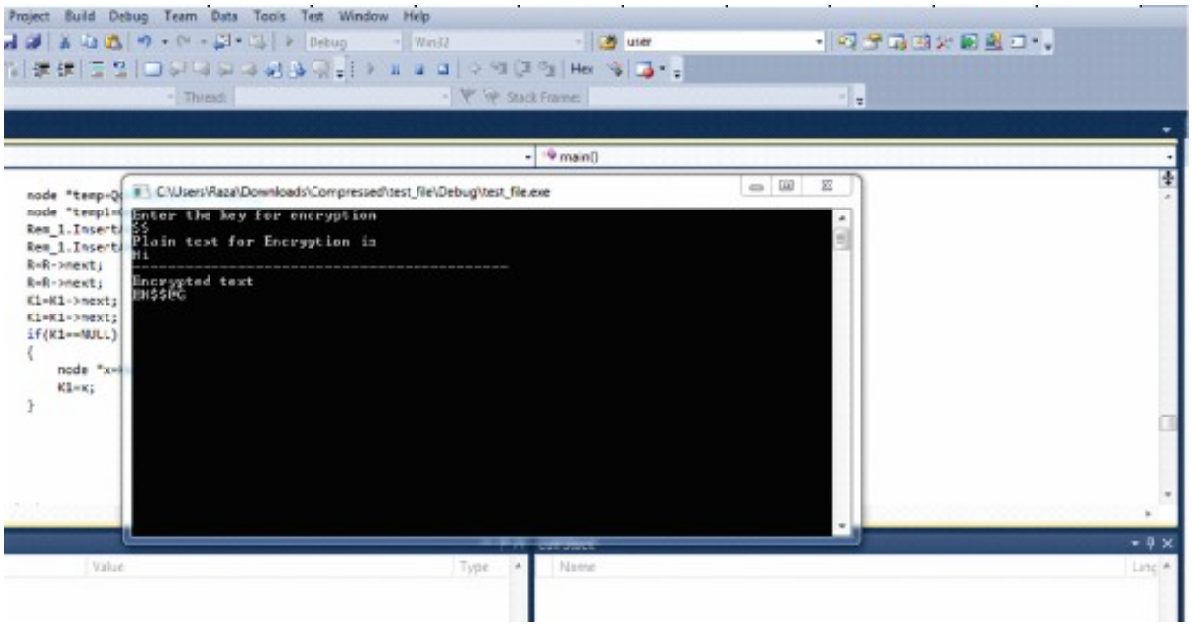

FIG. 5. IMPLEMENTATION OF ENCRTPTION

Fig. 6 shows the Testing results of HP G3450 where blue bars show the encryption time and red bars shows the decryption time whereas x-axis demonstrate the data unit (bytes) and y-axis represents time(seconds).

7.2 Testing Results by using HP1000

Table 2 describes different plain text of different bytes as an input by using system HP1000, which is based on 2nd generation with 2 GB RAM. Through this system the estimated execution time of encryption and decryption of plain text can be measured.

Fig. 7 shows the Testing results of HP 1000 and blue bars show the encryption time and red bars show the decryption time whereas x-axis demonstrates the data unit (bytes) and y-axis represents time(seconds).

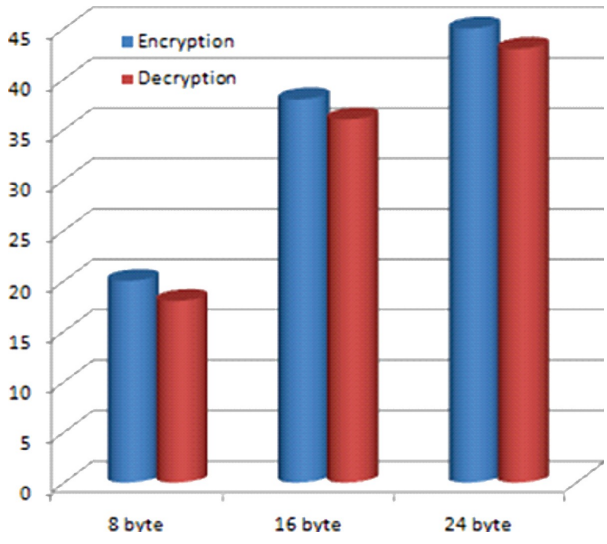

FIG. 6. RESULTS USING HP G3450 (8GB RAM)

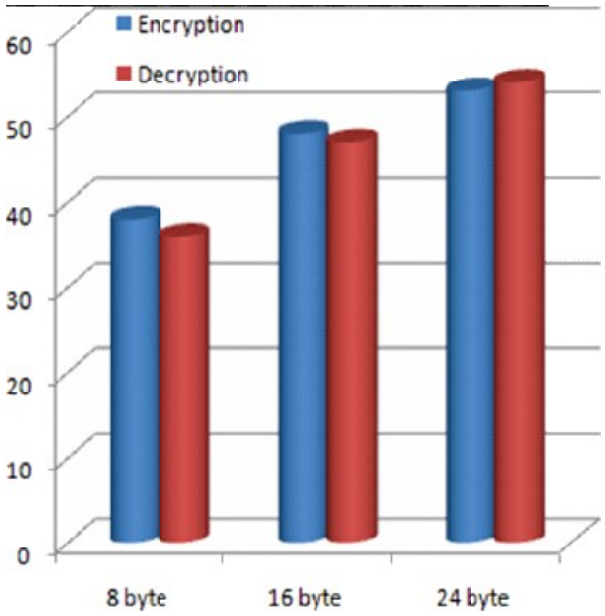

FIG. 7. RESULTS USING HP 1000 (2GB RAM)

TABLE 1. RESULTS USING HP G3450 (8GB RAM)

Block Size (Byte)	Encryption Time (sec)	Decryption Time (sec)
8	20	18
16	38	36
24	45	43

TABLE 2. RESULTS USING HP 1000 (2GB RAM)

Block Size (Byte)	Encryption Time (sec)	Decryption Time (sec)
8	38	36
16	48	47
32	53	54

8. CONCLUSION

In this research paper, we have explored a new approach for accomplishing the secured information transmission in an upgraded way. The proposed approach is the symmetric key calculation and will read each plain text one by one and can convert it into cipher text by performing some operations. This proposed algorithm is efficient and easy to implement. From the result, it is proved that this approach is more reliable and faster than others.

ACKNOWLEDGEMENT

Authors acknowledge Department of Computer Science, Bahauddin Zakariya University, Multan, and Department of Computer Science, Khawaja Fareed University, Rahim Yar Khan, Pakistan, for motivating and supporting for the successful completion of this research work.

REFERENCES

[1] Gupta, V., Singh, G., and Gupta, R., "Advance Cryptography Algorithm for Improving Data Security", International Journal of Advanced Research inComputer Science & Software Engineering, Volume 2, No. 1, January, 2012.

[2] Kessler, G.C., "An Overview of Cryptography", April 28, 2017, http://www.garykessler.net/library/crypto.html

[3] Jueneman, R., "Electronic Document Authentication", IEEE Network Magazine, April, 1987.

[4] Bishop, M., "Introduction to Computer Security", Addison-Wesley Professional, New York, 2005.

[5] Poison, J., "Cognitive Radio Applications in Software Defined Radio", Proceedings of SDR Technical Conference and Product Exposition, pp. 1-6, 2004.

[6] Mitola, J., "Cognitive Radio for Flexible Mobile Multimedia Communications", Proceedings of IEEE International Workshop on Mobile Multimedia Communications, pp. 3-10,San Diego, CA, USA, 1999.

[7] Sodagari, S., and Clancy, T.C., "An Anti-Jamming Strategy for Channel Access in Cognitive Radio Networks", International Conference on Decision and Game Theory for Security, pp. 34-43, Springer, 2011.

[8] Trappe, W., "Introduction to Cryptography with Coding Theory", Pearson, 2nd Edition, New York, 2005.

[9] Bishop, M., "Introduction to Computer Security", Addison-Wesley Professional, New York, 2005.

[10] Hellman, M., "An Overview of Public Key Cryptography", IEEE Communications Magazine, November, 1978.

[11] Alexey, C., Bastian, K., et al. "Infrastructure for Remote Instrumentation, Computer Standards & Interfaces", 3rd International Conference on Computing, Communication and Networking, Volume 34, No. 6, November, 2012.

[12] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Lee, J.M., Paillier, P., and Shi, H., "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions", Journal of Cryptology, Volume 42, 2008.

[13] Bellare, M., Kilian, J., and Rogaway, P., "The Security of the Cipher Block Chaining Message Authentication Code", Journal of Computer and System Sciences, December, 2000.

[14] Biham, E., and Shamir, A.,"Differential Cryptanalysis of the Data Encryption Standard", Springer, New York, 1993.

[15] Wadsworth, D., "Decius Wadsworth", December 07, 2016, https://en.wikipedia.org/wiki/DeciusWadsworth.

[16] Stallings, W., "The Advanced Encryption Standard", Cryptologia, July, 2002.

[17] Shah, K., and Bhavika, G., "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering, [ISSN: 2231-2307], Volume 2, No. 1, March, 2012.

[18] Stallings, W., "Data and Computer Communications", Pearson Education, New Jersey, 2005.

[19] Stallings, W., "Cryptography and Network Security Principles and Practice", Prentice Hall, 2007.

[20] Stallings, W., and Brown, L., "Computer Security", Pearson Education, New Jersey, 2015.