SECURED TEXT MESSAGE TRANSMISSION IN A WIRELESS COMMUNICATION SYSTEM WITH THE IMPLEMENTATION OF VIGENERE CIPHER AND RSA CRYPTOGRAPHIC ALGORITHMS

Md. Firoz Ahmed[1], Md. Rimon Islam [1] and Abu Zafor Md. Touhidul Islam[2]

[1]Department of Information and Communication Engineering,
University of Rajshahi, Rajshahi 6205, Bangladesh
[2]Department of Electrical and Electronic Engineering,
University of Rajshahi, Rajshahi 6205, Bangladesh

ABSTRACT

A broad variety of wireless data applications and services depend on security. This paper presents a simulation-based study of a wireless communication system using a secured Vigenere cipher and the RSA cryptographic algorithms on text message transmission. The system under consideration uses 1/2-rated CRC channel coding and BPSK digital modulation over an Additive White Gaussian noise (AWGN) channel. To address security concerns, a text message is encrypted at the transmitter with the Vigenere cipher and RSA before being decrypted and compared for different levels of SNR at the receiver end. To carry out the computer simulation, the Matlab 2016a programming language has been used. The transmitted text message is successfully retrieved at the receiver end after the Vigenere cipher and the RSA cryptographic algorithm are implemented. It is also anticipated that as noise power increases, the effectiveness of a wireless communication system based on the Vigenere cipher and RSA security will decrease.

KEYWORDS

Vigenere Cipher, RSA, AWGN, CRC, BPSK, Text Message.

1. INTRODUCTION

Cellular communication is becoming an immensely useful part of everyday. In addition to being widely used for voice communication, cellular phones can now be used to send text messages, access the internet, conduct financial transactions, and so on. However, since network access is open to all and there is no physical barrier preventing an attacker from accessing the network, ensuring security is a key problem for the transmission of such sensitive information over the wireless medium [1,2]. Although different methods are used to enhance the security of high-speed data transmission, the most efficient technique used to provide confidentiality is data encryption and decryption strategies. Encryption standards such as Data Encryption Standard (DES) [3], Advanced Encryption Standard (AES) [4], and Escrowed Encryption Standard (EES) [5] are used in the government and public domains. These standards appear to be less secure and faster than desired with today's advanced technologies. In the field of high-speed networking, high-throughput encryption and decryption are becoming increasingly important [6].

Wireless data communication can be secured by applying security protocols to different layers of the protocol stack or within the application itself. Cryptographic algorithms (symmetric or

DOI: 10.5121/caij.2021.8201

private-key ciphers, asymmetric or public-key ciphers, hashing functions, and so on) are used as building blocks in security protocols to achieve goals such as peer authentication, privacy, data integrity, and so on. To ensure confidentiality and data integrity, public key algorithms (such as RSA, DSA, Diffie-Hellman key exchange, ECC, and so on), symmetric algorithms (such as DES, 3DES, IDEA, RC4, AES, and so on), and message authentication algorithms (such as MD2, MD5, SHA, and so on) are typically used for authentication and key exchange, respectively.

In recent times, the use of cryptography to secure wireless data through the development of public-key algorithms [7] has emerged as a hot topic. A pair of different keys is used in public-key cryptography for data encryption and decryption, respectively. The attraction of this scheme is that each communicating party only needs a key pair to communicate with an unlimited number of other communicating parties. Once a key pair is obtained, a person can communicate with anyone else. In 1977, MIT Professors Ronal L. Rivest, Adi Shamir, and Leonard M. Adleman developed the asymmetric RSA algorithm [8]. The factorization problem provides the foundation for RSA's security. The security architecture of RSA is based on the difficulty of factoring large numbers.

Cryptography employing the Vigenere Cipher Algorithm and the Cipher Block Chaining (CBC) operation mode is one of many data security methods. This application was created with Borland Delphi 6.0 and includes encryption and data decryption. An extension will be added to the encrypted data. The Vigenere Chiper algorithm and the CBC mode of operation will be combined to create a new method called Vigenere Chiper +, which will improve the Vigenere Chiper algorithm's weaknesses. Because it converts 26 letters of the alphabet into 256 ASCII characters [9].

In this paper, the actual message to be transmitted is encrypted and decrypted using the Vigenere cipher and the RSA block cipher algorithm, and the effect on secured message transmission over wireless noisy channels is investigated.

2. RELATED WORKS

The following is a brief review of the literature in the area relevant to this paper. M. Haque [10] investigated text message transmission using the Vigenere Cipher and the RSA cryptographic algorithms in a 4G compatible MIMO MC-CDMA system. According to the findings of this study, system performance degrades as noise power increases in comparison to signal power.

M. M. Rahman and F. Enam [11] provided an overview of mobile wireless network evolution from 1G to 4G. They also developed a wireless communication system for sending text messages over an AWGN noisy channel. To ensure data security, Playfair encryption/decryption algorithms were implemented. A set of cipher text was obtained and compared for various SNR values. They observed that increasing the SNR improved the text message reproducing performance.

M. Haque et al. [12] presented a comprehensive investigation into text message transmission in an MC-CDMA wireless communication system using STBC and MIMO beamforming schemes, and also the Vigenere Cipher and RSA cryptographic algorithms. The studies found that as the signal-to-noise ratio (SNR) decreases in additive white Gaussian noise (AWGN) noisy and Rayleigh fading channels, the performance of the wireless communication systems text message retrieval degrades.

M.A. Islam and A.Z.M.T. Islam [13] presented secure wireless text message transmission using the RSA cryptographic algorithm. According to the study, as noise power increases, the performance of RSA security-based wireless communication systems degrades.

3. Cryptographic Algorithm

The utilization of the cryptographic algorithm(s)/method(s) is basically related to allowing two people to communicate with each other over an insecure and hostile channel in such a way that an attacker cannot understand what is communicated. Plaintext refers to information that one person wishes to send to another and can take the form of English text, numerical data, or other data. The person encrypts the plaintext with a predetermined key and sends the resulting ciphertext over the channel. No other unauthorized person can determine the true feature of the plaintext by eavesdropping on the channel and seeing the ciphertext. Knowing the encryption key, the person concerned can decrypt the ciphertext and reconstruct the plaintext.

3.1. Vigenere Cipher

A well-known monoalphabetic Cipher is the Vigenere Cipher, named after Blaise de Vigenere. Once a key is selected, each alphabetic character is mapped to a unique alphabetic character in other monoalphabetic cryptosystems (Shift Cipher and Substitution Cipher). The Vigenere Cipher encrypts *m* alphabetic characters at a time, with each plaintext element corresponding to *m* alphabetic characters. The plaintext is divided into groups of *m* elements each. The plaintext elements are converted to residues modulo 26 for each group, with a key consisting of *m* integer values to encrypt added. In the paper, such a Key is represented by the keyword:

$$K= [1\ 2\ 3\ 4\ 5\ 6\ 7\ 8].$$

We can use the same keyword to decrypt, but instead of adding it, we will subtract it modulo 26. The Vigenere Cipher is a polyalphabetic cryptosystem with m keywords that means an alphabetic character can be mapped to one of m possible alphabetic characters if the keyword contains m distinct characters. [10], [14].

3.2. RSA

RSA (Rivest-Shamir-Adleman) was created in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. This RSA cryptographic scheme is a block cipher with plaintext and ciphertext integers ranging from 0 to 2^{1024}. This cryptographic scheme employs an exponential expression. The plaintext is encrypted in blocks, each of which has a binary value less than a common number n, i.e., each block size must be less than or equal to $\log_2(n)$. For some plaintext block M and ciphertext block C, encryption and decryption in RSA take the following form:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (1)$$

Both the sender and the receiver must be aware of the value of n in the RSA scheme. The sender knows the value of e, but only the receiver knows the value of d. As a result, this is a public-key encryption algorithm with the public key PU = {e, n}, and the private key PU = {d, n}.

In order for this algorithm to be suitable for public-key encryption, the following conditions must be met in consideration of two prime numbers, p, q [15].

$$ed \equiv 1 \bmod \phi\ (n) \text{ and } d \equiv e^1 \bmod \phi(n) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (2)$$

$$\text{where, } n = pq \text{ and } \phi\ (n) = (p- 1)(q -1)$$

4. Simulation Model

This section goes over the steps that were taken to create the simulation model of the wireless communication system. The presented simulation method is able of assessing the performance of encrypted message transmission over a BPSK modulation technique and an AWGN communication channel. Simulation is being selected as the primary tool for our research, and the simulator has been created using the Matlab 2016a programming language. To begin, we define the parameters used to create the wireless communication simulator. Figure 1 depicts a simulation model of a wireless communication system using the Vigenere cipher and the RSA encryption/decryption algorithms for text message transmission. For channel coding, cyclic redundancy check (CRC) coding with a code rate of 1/2 has been used. The text message is converted into an integer and then encrypted using the Vigenere cipher and the RSA encryption algorithms in such a communication system. CRC is used to channel encode the encrypted data after it has been converted into binary bits and interleaved for minimization of burst errors. The interleaved bits are then digitally modulated with BPSK modulation scheme and transmitted through the AWGN noisy channel. The received complex digitally modulated symbols are demodulated, deinterleaved, and fed to the CRC channel decoder in the receiving section. The decoded binary data is converted to an integer and decrypted using the Vigenere cipher and the RSA decryption algorithms. Finally, the decrypted data is converted into a text message. The following parameters are used, as listed in Table 1.

Table 1. Simulation parameters.

Parameters	Values
Transmitted data	Text message
Channel Coding	CRC
CRC rate	½
Modulation	BPSK
Encryption/Decryption algorithm	Vigenere Cipher and RSA
Channel	AWGN
Signal to noise ratio, SNR	0 to 10dB

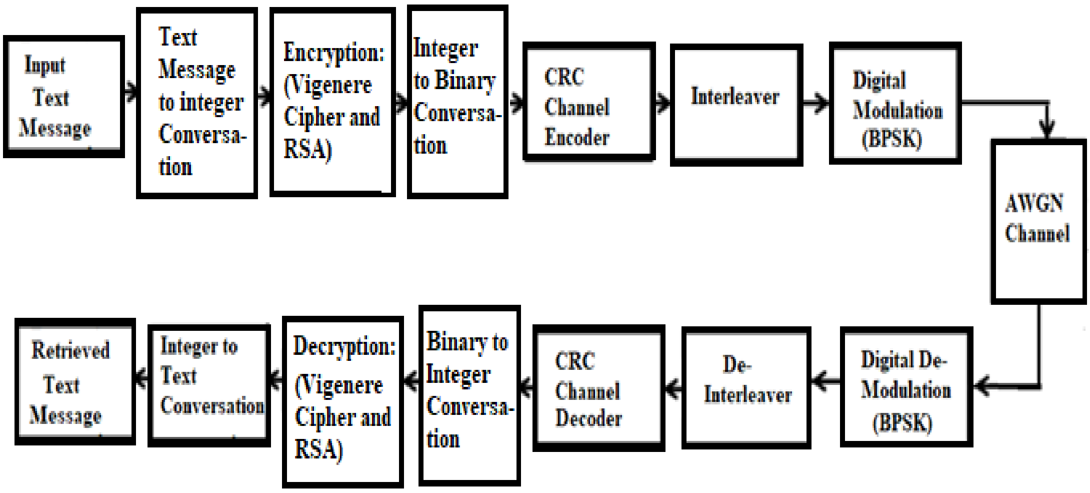
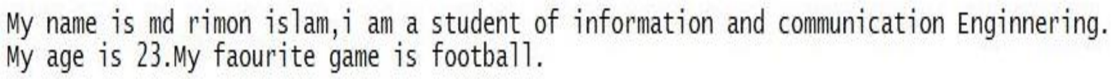

Input Text Message
Text Message to integer Conversa-tion
Encryption: (Vigenere Cipher and RSA)
Integer to Binary Conversa-tion
CRC Channel Encoder
Interleaver
Digital Modulation (BPSK)
AWGN Channel
Digital De-Modulation (BPSK)
De-Interleaver
CRC Channel Decoder
Binary to Integer Conversa-tion
Decryption: (Vigenere Cipher and RSA)
Integer to Text Conversation
Retrieved Text Message

Figure 1: Block Diagram of Wireless Communication with Vigenere cipher and RSA Encryption/Decryption

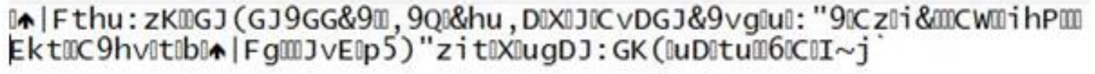
5. SIMULATION RESULTS AND DISCUSSION

A computer program designed for simulation study has been written using Matlab 2016a. The developed program generates different plain text by decrypting various cipher text for various signal-to-noise ratio values. Figure 2 depicts the plaintext message (original text message) to be used for transmission, which is encrypted with a shared secret key. Before sending the messages, the secret key must be shared. Figure 3 depicts the cipher text produced by the shared secret key.



```
My name is md rimon islam,i am a student of information and communication Enginnering.
My age is 23.My faourite game is football.
```

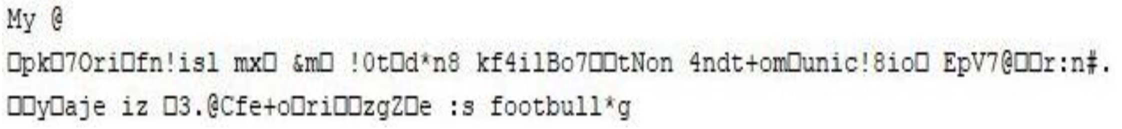
Figure 2. Original text message



```
□↑|Fthu:zK□□GJ(GJ9GG&9□□,9Q□&hu,D□X□J□CvDGJ&9vg□u□:"9□Cz□i&□□CW□□ihP□□
Ekt□□C9hv□t□b□↑|Fg□□□JvE□p5)"zit□X□ugDJ:GK(□uD□tu□□6□C□I~j`
```

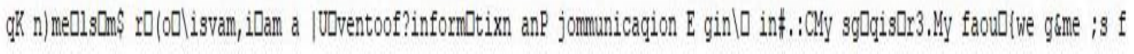
Figure 3. Encrypted Message

The encrypted message is then sent over the AWGN channel in a wireless system. The various cipher text is discovered at the receiver end for different values of signal to noise ratio (SNR). After that, the cipher texts are decrypted using the shared secret key. Figures 4 to14 show the plaintext messages (retrieved text messages) retrieved at the receiver end for SNR values of 0dB to 10dB.



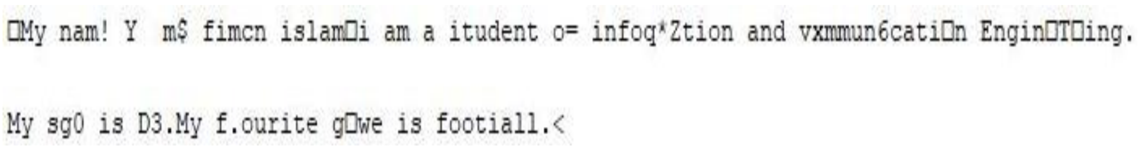
```
My @
□pk□7Ori□fn!isl mx□ &m□ !0t□d*n8 kf4ilBo7□□tNon 4ndt+om□unic!8io□ EpV7@□□r:n#.
□□y□aje iz □3.@Cfe+o□ri□□zgZ□e :s footbull*g
```

Figure 4. Retrieved text message at SNR = 0dB



```
gK n)me□ls□m$ r□(o□\isvam,i□am a |U□ventoof?inform□tixn anP jommunicaqion E gin\□ in#.:CMy sg□qis□r3.My faou□{we g&me ;s f
```

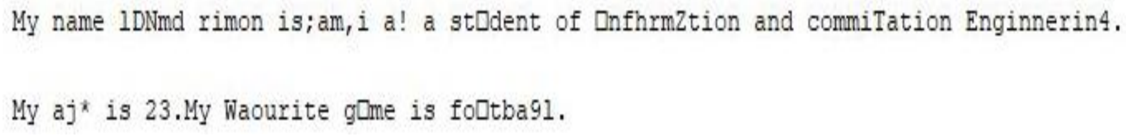
Figure 5. Retrieved text message at SNR = 1dB



```
□My nam! Y  m$ fimcn islam□i am a itudent o= infoq*Ztion and vxmmun6cati□n Engin□T□ing.

My sg0 is D3.My f.ourite g□we is footiall.<
```

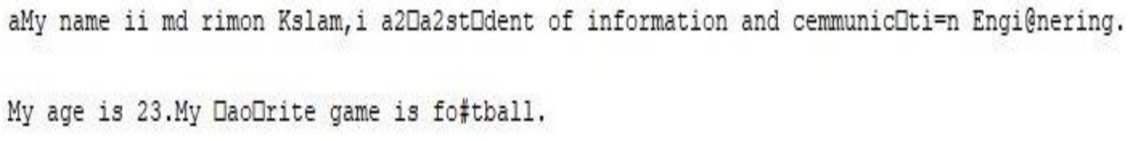
Figure 6. Retrieved text message at SNR = 2dB



```
My name lDNmd rimon is;am,i a! a st□dent of □nfhrmZtion and commiTation Enginnerin4.

My aj* is 23.My Waourite g□me is fo□tba91.
```

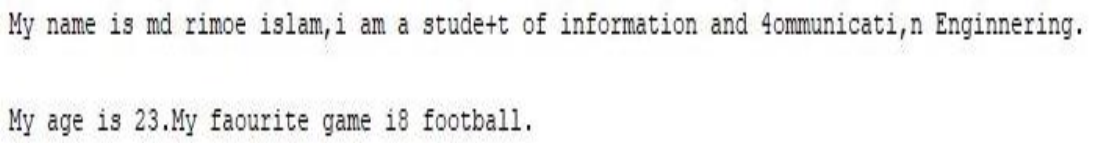
Figure 7. Retrieved text message at SNR = 3dB



```
aMy name ii md rimon Kslam,i a2□a2st□dent of information and cemmunic□ti=n Engi@nering.

My age is 23.My □ao□rite game is fo#tball.
```

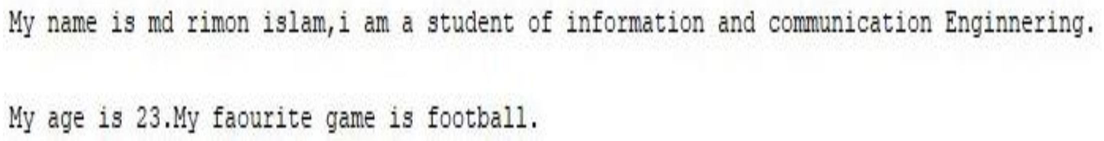
Figure 8. Retrieved text message at SNR= 4dB



```
My name is md rimoe islam,i am a stude+t of information and 4ommunicati,n Enginnering.

My age is 23.My faourite game i8 football.
```

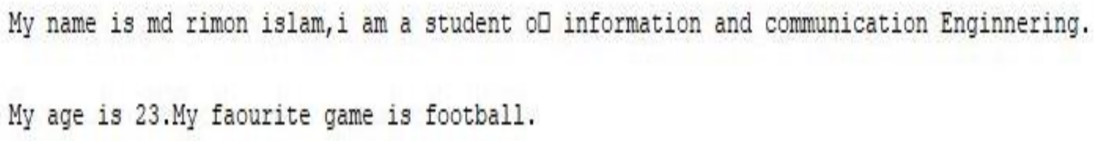
Figure 9. Retrieved text message at SNR= 5dB



```
My name is md rimon islam,i am a student of information and communication Enginnering.

My age is 23.My faourite game is football.
```

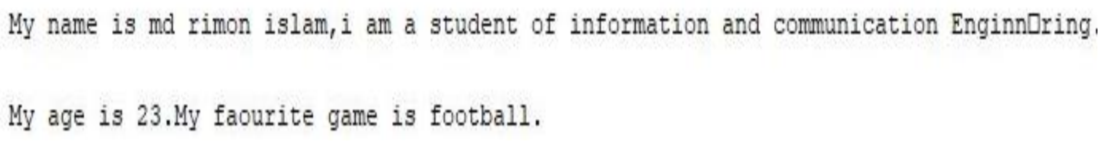
Figure 10. Retrieved text message at SNR= 6dB



```
My name is md rimon islam,i am a student o□ information and communication Enginnering.

My age is 23.My faourite game is football.
```

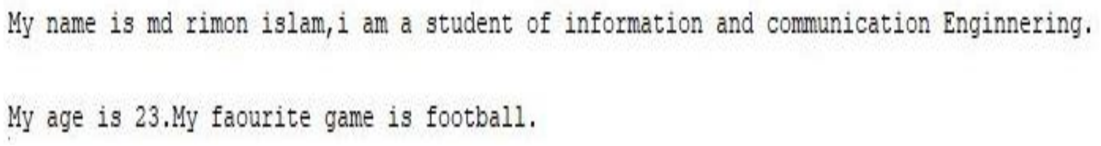
Figure 11. Retrieved text message at SNR = 7dB



```
My name is md rimon islam,i am a student of information and communication Enginn□ring.

My age is 23.My faourite game is football.
```

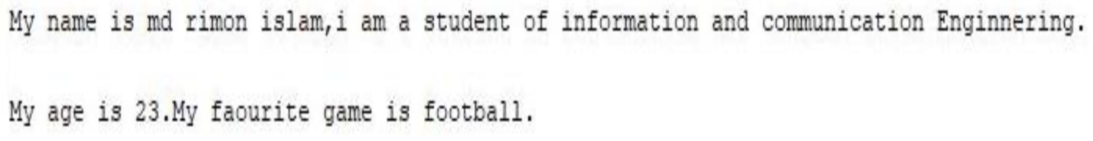
Figure 12. Retrieved text message at SNR= 8dB



```
My name is md rimon islam,i am a student of information and communication Enginnering.

My age is 23.My faourite game is football.
```

Figure 13. Retrieved text message at SNR= 9dB



```
My name is md rimon islam,i am a student of information and communication Enginnering.

My age is 23.My faourite game is football.
```

Figure 14. Retrieved text message at SNR= 10dB

When the transmitted (Figure 2) and retrieved (Figures 4–14) text messages are comparison, it is evident that the simulated wireless communication system using the Vigenere cipher and RSA encryption/decryption algorithms degrades as the SNR value decreases. With increasing SNR levels, the Vigenere cipher and RSA encrypted text message reproducing performance improves, and the original text message is fully reproduced at the receiver end at SNRs of 9 dB or higher.

6. CONCLUSION

In this paper, we applied the Vigenere cipher and the RSA cryptographic encryption/decryption algorithm in a wireless communication system using BPSK modulation over an AWGN channel and assessed the text message transmission performance of the communication system at various SNR levels. Based on the results of this simulation study, it is possible to conclude that employing the Vigenere cipher and the RSA cryptographic algorithm in a 1/2-rated CRC channel encoded wireless communication system with BPSK modulation over an AWGN noisy environment is very useful in retrieving the transmitted text message at the receiver end.

REFERENCES

[1] World Wide Web Consortium, the World Wide Web FAQ. http://www.w3.org/Security/faq/www secutityfaq.html (1998).

[2] U.S. Department of Commerce, the Emerging Digital Economy II. http://www.esa.doc.gov/508/esa/The the Emerging Digital Economy II.html (1999).

[3] Data Encryption Standard. http://csrc. nist.gov/publications/fips/fips46-3/fips-46-3.pdf.

[4] Advanced Encryption Standard. http://csrc.nist.gov/publications/fips/fips197/fip s-197.pdf.

[5] Escrowed Encryption Standard. http://csrc.nist.gov/publications/fips/fips1185/fi ps-185.txt.

[6] Adam J. Elbirt, Christof Paar, "An Instruction Level Distributed Processor for Symmetric Key Cryptography," IEEE Transactions on Parallel and Distributed Systems, Vol. 16, No.5 (2005).

[7] P. Kuppuswamy and C. Chandrasekar, "Enrichment of Security through Cryptographic Public Key Algorithm based on Block Cipher, Indian Journal of Computer Science and Engineering," Vol. 2, No. 3, pp.347-355 (2011).

[8] William Stallings, Network Security Essentials (Applications and Standards), Pearson Education, pp. 2.80 (2004).

[9] EK. Nurnawati, National Appl Science and Tech. IST AKPRIND Yogyakarta (2008).

[10] M. Haque, "Secure text message transmission in a 4G compatible MIMO MC-CDMA system with combined implementation of Vigenere Cipher and RSA cryptographic algorithm," International Journal of Information Technology Convergence and Services (IJITCS) Vol.2, No.5 (October 2012)

[11] M. M. Rahman and F. Enam, "Secure Message Transmission over Wireless Communication," Research Journal of Physical and Applied Sciences, Vol. 2, No. 3, pp. 30-35 (2013).

[12] M. Haque, S. E. Ullah, and J. J. Sadique, "Secure Text Message Transmission in an MC-CDMA Wireless Communication System using STBC and MIMO Beamforming Schemes, "International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.1 (February 2013).

[13] M.A. Islam and A.Z.M.T. Islam, "Secure wireless text message transmission with the implementation of RSA cryptographic algorithm, "International Journal of Computer Networks and Communications Security, Vol. 2, No. 5, May 2014, 146–151.

[14] Douglas R. Stinson" Cryptography: Theory and Practice", CRC Press, CRC Press LLC, USA (1995).

[15] William Stallings" Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice-Hall Publisher (2005).