International Journal of Computer Networks and Communications Security

VOL. 2, NO. 5, MAY 2014, 146–151
Available online at: www.ijcncs.org
ISSN 2308-9830

# Secure Wireless Text Message Transmission with the Implementation of RSA Cryptographic Algorithm

**Md. Ashraful Islam[1], A. Z. M. Touhidul Islam[2]**

[1] Lecturer, Department of ICE, University of Rajshahi, Rajshahi-6205, Bangladesh

[2] Associate Professor, Department of ICE, University of Rajshahi, Rajshahi-6205, Bangladesh

*E-mail: [1]ras5615@gmail.com, [2]touhid_ice@ru.ac.bd.com*

**ABSTRACT**

Security is crucial to a wide range of wireless data applications and services. This paper presents a simulation based study of a wireless communication system with the implementation of secured asymmetric RSA cryptographic encryption/decryption algorithm on text message transmission. The system under investigation incorporates 2/3-rated CRC channel coding and QPSK digital modulation over an additive white Gaussian noise (AWGN) channel. For tackling the security problems a text message is first RSA encrypted at the transmitter while it is decrypted at the receiver end and compared for different levels of SNR. The Computer simulation has been performed using Matlab 2009b programming language. The transmitted text message is found to have retrieved effectively at the receiver end under the implementation of RSA cryptographic algorithm. It has also been anticipated that the performance of RSA security based wireless communication system degrades with the increase of noise power.

**Keywords:** *RSA, AWGN, CRC, QPSK, Test Message.*

## 1 INTRODUCTION

Wireless cellular communication has become an important part in our daily life. Besides the large scale adoption of cellular phones for voice communication, it can now also be used to send text messages, access the internet, conduct money transactions and so on. However, for the transmission of such sensitive information over the wireless medium, ensuring security is a critical issue [1,2] since the network access is open to all and there is no physical barrier that can separate an attacker from accessing the network. Although various techniques are employed for the improvement in security of the high-speed data being transmitted, the most important method used to provide the confidentiality is the data encryption and decryption techniques. The encryption standards such as Data Encryption Standard (DES) [3], Advanced Encryption Standard (AES) [4], and Escrowed Encryption Standard (EES) [5] are used in government and public domains. With today's advanced technologies, these standards are seem not to be as secure and fast as one would like. High throughput encryption and decryption are becoming increasingly important in the area of high-speed networking [6].

Communication of wireless data can be secured under the employment of security protocols to various layers of the protocol stack, or within the application itself. Security protocols use cryptographic algorithms (symmetric or private-key ciphers, asymmetric or public-keyciphers, hashing functions, etc.) as building blocks to achieve the desired objectives like peer authentication, privacy, data integrity, and so on. Public key algorithms, (such as RSA, DSA, Diffie-Hellman key exchange, ECC, etc.), symmetric algorithms (such as DES, 3DES, IDEA, RC4, AES, etc.) and message authentication algorithms (such as MD2, MD5, SHA, etc.) are typically used for authentication and key exchange, to ensure confidentiality, and to implement data integrity, respectively.

In recent years, the use of cryptography in wireless data security through the development of public key algorithm [7] has emerged as a topic of significant interest. In public key cryptography, a pair of different keys is used for data encryption

and decryption purposes, respectively. The attractiveness of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he/she can communicate with anyone else. The asymmetric RSA algorithm is developed by MIT Professors: Ronal L. Rivest, Adi Shamir, and Leonard M. Adleman in 1977 [8]. RSA gets its security from factorization problem. Difficulty of factoring large numbers is the basis of security of RSA. In this paper, the actual message to be sent is encrypted and decrypted using the RSA block cipher algorithm and its impact on secured message transmission over wireless noisy channel was observed.

This paper is organized as follows. Section 1 is an introduction. A brief overview of recent relevant works is presented in Section 2. The RSA encryption/decryption algorithm used for safe wirelss communication is discussed in Section 3. Section 4 explains the simulation model to be used to study the performance of the communication system under consideration. Model parameters and assumptions made in simulation study are clearly explained. The simulation results are presented and discussed in Section 5. Section 6 describes the conclusion of the study.

## 2 RELATED WORKS

A brief survey of literature in the area relevant to this paper is as follows. M.G. Rashed et al. [9] made a comprehensive study on text message transmission in a quasi-orthogonal space time block coded (QO-STBC) multiple-input single-output (MISO) system under the employment of merely low complexity maximum-likelyhood (ML) decoding based channel estimation and RSA cryptographic encoding/decoding algorithms. They noticed that the text message retrieving performance of the wireless communication system degrades with the lowering of the signal to noise ratio (SNR) over the additive white Gaussian noise (AWGN) noisy and Rayleigh fading channels. M. M. Rahman and F. Enam [10] presented an overview of the evolution of mobile wireless networks from 1G to 4G. They also implemented a wireless communication system for text message transmission over AWGN noisy channel. Playfair encryption/decryption algorithms were implemented for ensuring data security. For various values of SNR, a set of cipher text were obtained and compared. They noticed that the text message reproducing performance was improved with the increase of SNR.

## 3 RSA CRYPTOGRAPHIC ALGORITHM

The Rivest-Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key encryption [11]. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than $2^{1024}$. The RSA scheme makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

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

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

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d, n}. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate mod $M^e$ mod n and $C^d$ for all values of $M < n$.
3. It is infeasible to determine d given e and n.

For now, we focus on the first requirement and consider the other questions later. We need to find a relationship of the form $M^{ed} \bmod n = M$. The preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function. It is shown in that for p, q prime, $\phi(pq) = (p-1)(q-1)$. The relationship between e and d can be expressed as

$$ed \bmod \varphi(n) = 1$$

This is equivalent to saying

$$ed \equiv 1 \bmod \phi(n)$$

$$d \equiv e^1 \bmod \phi(n)$$

That is, e and d are multiplicative inverses mod $\phi n$). Note that, according to the rules of modular

arithmetic, this is true only if d (and therefore e) is relatively prime to ϕ (n). Equivalently, gcd(ϕ (n),d) = 1.

We are now ready to state the RSA scheme. The ingredients are the following:

| | |
|---|---|
| p,q, two prime numbers | (private, chosen) |
| n = pq | (public, calculated) |
| e, with gcd(ϕ (n),e) = 1;1 < e < ϕ (n) | (public, chosen) |
| d≡e-1(mod ϕ (n)) | (private, calculated) |

| **Key Generation** | |
|---|---|
| **Select p, q** | P & q both prime, p≠q |
| **Calculate n = p×q** | |
| **Calculate φ(n) = (p-1)(q-1)** | |
| **Select integer e** | gcd (φ(n),e)= 1;1<e<φ(n) |
| **Calculate d** | $d \equiv e^{-1} \pmod{\varphi(n)}$ |
| **Public Key** | PU = {e,n} |
| **Private Key** | PR= {d,n} |
| | |
| **Encryption** | |
| **Plaintext** | M<n |
| **Ciphertext** | $C=M^e \bmod n$ |
| | |
| **Decryption** | |
| **Ciphertext** | C |
| **Plaintext** | $M= C^d \bmod n$ |

*Fig. 1. The RSA Algorithm*

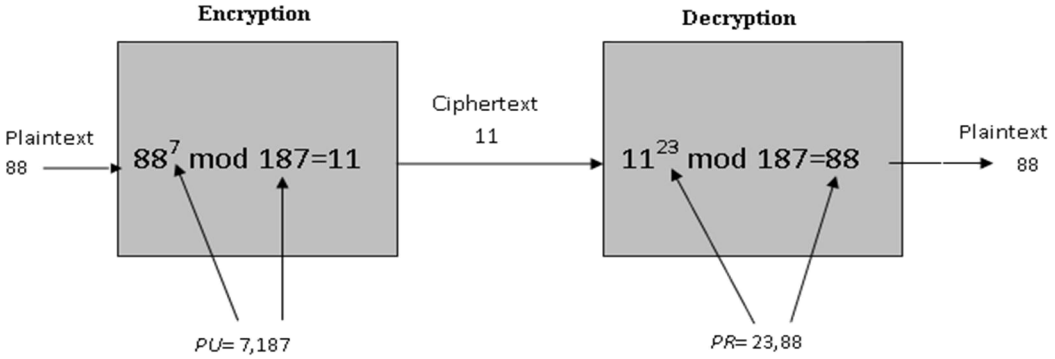


*Fig. 2. Example of RSA Algorithm*

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates C = $M^e$ mod n and transmits C. On receipt of this ciphertext, user A decrypts by calculating M = $C^d$ mod n.

Figure 1 summarizes the RSA algorithm. An example of the RSA algorithm is shown in Fig. 2. For this example, the keys were generated as follows:

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = pq = 17 x 11 = 187.
3. Calculate ϕ (n) = (p-1)(q-1) = 16 x 10 = 160.
4. Select e such that e is relatively prime to ϕ (n) = 160 and less than ϕ (n) we choose e = 7.

Determine d such that de ≡1 (mod 160) and d < 160. The correct value is d = 23, because 23 x 7 = 161 = 10 x 160 + 1; d can be calculated using the extended Euclid's algorithm.

## 4 SIMULATION MODEL

This section discusses the steps that have been followed to develop the simulation model of the wireless communication system. The implemented simulation model is capable of evaluating the performance of encrypted message transmission under different modulation techniques and communication channels. Simulation was chosen to be the primary tool for our study and we have employed Matlab 2009b programming language to develop the simulator. At first, we define the parameters that were used to develop the wireless communication simulator. Fig. 3 shows the

simulation model of a wireless communication system with the implementation of asymmetric RSA encryption/decryption algorithm for text message transmission. Cyclic Redundancy Check (CRC) coding with code rate 2/3 were employed for channel coding purposes. In such a communication system, the text message is converted into integer and then encrypted using RSA encryption algorithm. The encrypted data is converted into binary bits and channel encoded using CRC. The encoded bits are subsequently digitally modulated using QPSK The used parameters are listed in Table 1 as follows:

*Table 1. Simulation Parameters*

| Parameters | Values |
|---|---|
| Transmitted data | Text message |
| Coding | CRC |
| Encryption Algorithm | RSA |
| Key | Student |
| CRC rate | 2/3 |
| SNR | 0-15 |
| Modulation | QPSK |
| Channel | AWGN |

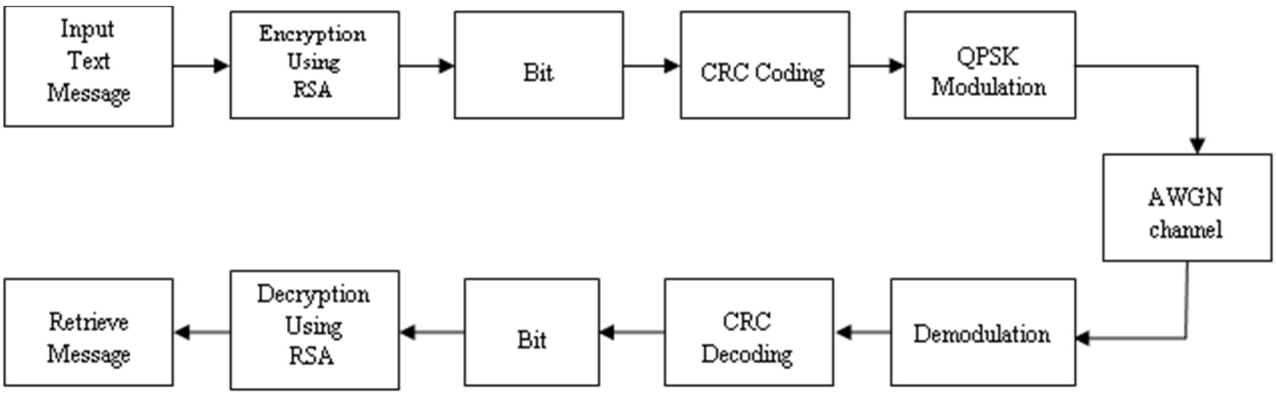


*Fig. 3. Block Diagram of Wireless Communication with RSA Encryption/Decryption.*

modulation scheme and transmitted through the AWGN noisy channel. At the receiving section, the received complex digitally modulated symbols are first demodulated and then fed to the CRC channel decoder. The decoded binary data are converted into integer and decrypted with RSA decryption algorithm. The decrypted data are finally converted into text message.

### *4.1 Cyclic Redundancy check (CRC)*

Cyclic Redundancy Check (CRC) codes are a subset of then class of linear codes, which satisfy the cyclic shift property such as if C=[$C_{n-1}$ ,$C_{n-2}$ ……,$C_O$] is a codeword of a cyclic code, then [$C_{n-2}$ $C_{n-2}$ ,…,$C_0$,$C_{n-1}$ ], obtained by a cyclic shifts of the elements of C, is also a code word. In other word all cyclic shifts of C are code words. From the cyclic property, the codes possess a great deal of structure which is exploited to greatly simplify the encoding and decoding operation [14].

### *4.2 Additive White Gaussian Noise (AWGN)*

A reasonable assumption for a fixed, LOS wireless channel is the additive white Gaussian noise (AWGN) channel [12], which is flat and not "frequency-selective" as in the case of the fading channel. Particularly fast, deep frequency-selective fading as often observed in mobile communications is not considered in this thesis, since the transmitter and

receiver are both fixed. This type of channel delays the signal and corrupts it with AWGN. The AWGN is assumed to have a constant PSD over the channel bandwidth, and a Gaussian amplitude probability density function. This Gaussian noise is added to the transmitted signal prior to the reception at the receiver [13]. The transmitted signal s(t), white Gaussian noise n(t) and received signal r(t) are expressed by the following equation:

$$r(t)=s(t)+n(t)$$

where n(t) is a sample function of the AWGN process with probability density function (pdf) and power spectral density. It was developed using 'awgn' function available in Matlab.

## 5 SIMULATION RESULTS AND DISCUSSION

Matlab 2009b has been used to write a computer program designed for simulation study. The developed program provides different replain text by decrypting different cipher text for different values of signal to noise ratio. The plaintext message (original text message) to be used for the transmission is shown in Fig. 4 which is encrypted using a shared secret key. The secret key must be shared before transmitting the messages. The cipher text produces by the shared secret key is shown in Fig. 5.

**I am a student, department of Information And Communication Engineering (ICE),University of Rajshahi. My session is 2008-2009**

*Fig. 4. Plaintext Message.*

**Ù¾+bË[ð#BîF¢y´ËïcÁòævßcÒådåL¤ßÀÝW tE¶ï9F{¦äÍûÂÊ3í¸Çl6u;/r[â¢+Hl¦tJYÿ°G-ö ä**
**A VÑvOõL^ûfRp)HMNÜ Ú²# nº**

*Fig. 5. Encrypted plaintext message with shared secret key.*

Then encrypted message is transmitted in a wireless system over the AWGN channel. At the receiver end, for various values of signal to noise ratio (SNR) various ciphertext are found. These ciphertexts are then decrypted using the shared secret key. For 0,1,2,3,5,7,10,13,15 dB values of SNR the replaintext messages (retrieved text messages) retrieved at the receiver end are shown in Figs. 6, 7, 8, 9, 10, 11, 12, 13, and 14, respectively.

**SB|P1rUõàáür>8ÌÑÈ»ôðéujT(O.i fnnrm!4IIMCblí&aNee]LCG0'XG%F!-)4)n¦hJD«®WÌÉÖe**
**——————————————iex-**

*Fig. 6. Decrypted Replaintext message for SNR=0.*

**(ie a`sw2"".p, d qbv.näô ï¦` l-5*+gpk`!.$ aIMMLÂepikh¢Çkfieg!0y~s *@D)¬ÄnI VubrItx$kf ZiBS`i`a>0Mi2àó÷á[Í® és0"$ |1l29**

*Fig. 7. Decrypted Replaintext message for SNR=1dB.*

**I`!-bb¢s~ tefp)`!$1as4m%,´"-@\'cTI/. LD amOm÷ìic% Igj(Mfg`oderéî§ ,MGE! 4")> ersiFHNW1VMb[HmDm* My qess)/.**
**ää ¾¼ ÆV²**

*Fig. 8. Decrypted Replaintext message for SNR=2dB.*

**A0qm a stum$.d depavpgib|,cf Infnblation"Idf Cki}a*-#!vilc,Mbgineevmnc ,OaA)(EnivERqi}p of R`jsiahi>0Mi0cerrion IQ 31% (?-**

*Fig. 9. Decrypted Replaintext message for SNR=3dB.*

**É am e$ctudenp(*leparômeNT of Inf matiON And Commuîéãation Enginåçping (HCE), Õnivez{atq*mt"Pqzchahi. My sm{s!on is " 08-**

*Fig. 10. Decrypted Replaintext message for SNR=5dB.*

**I am a student, department of In&/rmadion And CommunicAVéon Angineering(ICE), UnivERsity of Pajshahi. My session is 2°08-2009**

*Fig. 11. Decrypted Replaintext message for SNR=7dB.*

**I am a student, de0!rtment of In&or-!4ion And ComMUnication Ejcineering(ICE), University of Rajshahi. My session is 2008-2009**

*Fig. 12. Decrypted Replaintext message for SNR=10dB.*

**I am a student, department of Information And Communication Engineering (ICE), University of Rajshahi. My session is 2008-2009**

*Fig. 13. Decrypted Replaintext message for SNR=13dB.*

**I am a student, department of Information And Communication Engineering (ICE), University of Rajshahi. My session is 2008-2009**

*Fig. 14. Decrypted Replaintext message for SNR=15dB.*

Comparing the transmitted (Fig.4) and retrieved text messages (Figs. 6 to14), it is observable that the message retrieving performance of the simulated wireless communication system with the employment of RSA encryption/decryption algorithms is degraded with lowering the SNR value. The RSA encrypted text message reproducing performance is improved with increasing SNR level and the original text message is fully reproduced at the receiver end at the SNR of 13dB or more.

## 5 CONCLUSION

In this paper we implemented asymmetric RSA cryptographic encryption/decryption algorithm in a wireless communication system under QPSK modulation over AWGN channel and evaluated the text message transmission performance of the system for different levels of SNR. On the basis of the results obtained in the present simulation study, it can be concluded that the deployment of RSA cryptographic algorithm in CRC channel encoded wireless communication system under QPSK modulation over AWGN noisy environment is very much effective in proper retrieval of transmitted text message at the receiver end.

## 6 REFERENCES

[1] World Wide Web Consortium, The World Wide Web FAQ. http://www.w3.org/Security/faq/www-secutity-faq.html, 1998.

[2] U.S. Department of Commerce, The Emerging Digital Economy II. http://www.esa.doc.gov/508/esa/TheEmergingDigitalEconomyII.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/fips-197.pdf.

[5] Escrowed Encryption Standard. http://csrc.nist.gov/publications/fips/fips1185/fips-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] M. G. Rashed, S. E. Ullah, and M. F. Sharmin, "Encrypted Message Transmission in a QO-STBC encoded MISO Wireless Communication System under Implementation of Low Complexity ML Decoding Algorithm," International Journal of Computers and Technology, Vol. 2, No. 2, pp. 53-57, 2012.

[10] 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.

[11] M. K. Simon and M.-S. Alouini, Digital Communication over Fading Channel, John Wiley and Sons, NY, USA, 2004.

[12] M. A. Hasan, "Performance Evaluation of WiMAX/IEEE 802.16 OFDM Physical Layer," Espoo, June, 2007.

[13] J. G. Proakis, Digital Communications, McGraw-Hill Inc., New York, NY, Third Edition, 1995.

[14] Theodore S. Rapaport, "Wireless Communications Principles and Practice," Prentice-Hall of India Private Limited,2004