Developing a Cryptosystem for Multimedia Data

Abdelsalam Almarimi¹, Ibrahim Almerhaq², Faraj Abdulaziz³

Accepted 22nd November 2015 DOI: 10.18100/ijamec.09139

Abstract: Announcement The multimedia information is not secure in the wireless systems compared to that of wired systems. So, there is a necessity to encrypt the information and transmit over wireless medium and then receive the encrypted information from the wireless medium to recover the original information using a decryption method. In this paper, we propose a new method of cryptographic algorithm by combining both the symmetric key mono alphabetic shift ciphering and the RSA (Rivest, Shamir, and Adleman) algorithm which can be more applicable to the future generation of wireless systems. We have developed an algorithm for generating the RSA secret keys. The simulation is implemented in MATLAB. The security performance is studied for multimedia data files such as text, audio and image. Since, RSA is based on modular exponentiation, our experimental results show that the proposed algorithm is very efficient and secure for practical implementation as a multimedia cryptosystem.

Keywords: Cryptography, Encryption, Decryption, RSA.

1. Introduction

In the world of Internet, security of information is a must. The cryptography has become more important and critical issue in wireless communications [1]. Unless the system is able to provide some mechanisms to ensure security requirements, the system will have problems to be accepted. The wireless medium is an open air radio environment where any hacker can receive the information. But the multimedia information is not secured in the wireless environment compared to that of wired environment. The hacker has to get the information from wired system by physically attacking the medium. Since the wireless medium is open for access to any intruder or interceptor who can receive the information just with a radio receiver, the wireless information must be encrypted so that the information is secured [2]. Therefore, cryptographic techniques are always employed to protect critical and confidential information against malicious attack from the intruders. So that we can create a privacy to encrypt our message as the sender site and decrypt it at the receiver site. Specifically, the security of information can be applied at the ISO-OSI model of Internet, either at the application layer (Software) or at the data link layer (Hardware) [3].

As the number of hackers (code breakers) increasing, we need to find a more sophisticated secured cryptosystem for our information such that we can spend less time to encrypt/decrypt our information, and managing the keys used for cryptosystems. At the same time we must make the hackers not to get our information. The cryptosystem gives a support to the VoIP (Voice over Internet Protocol) and in turn it finds an application in DAB (Digital Audio Broadcasting) and DVB (Digital Video Broadcasting) [4]. These days, more expert cryptosystems have developed from the two basic classifications: the Symmetric Key Cryptography (SKC) and the Public Key Cryptography (PKC). In this paper, we propose an efficient cryptosystem by combining both the symmetric key mono alphabetic shift ciphering and the public key key RSA (Rivest, Shamir, and Adleman) ciphering which can be more appropriate to the upcoming generation of multimedia wireless systems. We have considered the advantages of both SKC and PKC and eliminated the drawbacks of both SKC and PKC [5],[6]. Cryptography algorithms for multimedia (that is images and video) is not so simple. The DES, AES, RES algorithms are not proper for color images and video, which are 3D arrays of data [7].

The paper is organized as following: next section introduces our proposed cryptosystem (SHIFT/RSA), then we give a detailed report of the of our experimental work and the related results. Finally, we conclude the paper.

2. THE PROPOSED CRYPTOSYSTEM

The basic idea of our proposed cryptosystem is using the combination of both RSA and Shift cipher algorithms. The shift ciphering is a symmetric key cryptography algorithm using a shared key for both encryption (converting plain text to cipher text) and decryption (converting cipher text to plain text) and here the ASCII characters are substituted as numbers from 0 to 127 and they are shifted according to a key and the shifted numbers are transmitted. At the receiver the original numbers are obtained again by shifting using a key which is shared along with the transmitter key.

The RSA algorithm is a common public-key cryptography algorithm. RSA uses two exponents, e and d, where e is public and d is private. Encryption and decryption use modular exponentiation which is feasible in polynomial time using fast exponentiation algorithm. However, modular logarithm is as hard as factoring the modulus, for which there is no polynomial time yet. The general idea behind the procedure used in RSA Here:

- First, we choose two large prime numbers p and q such that n= p × q.
- Compute phi = (p – 1) × (q – 1).
- Choose e (less than n) such that e and phi are relatively prime (having no common factor other than 1).
Choose \( d \) such that \( (e \times d) \mod \phi = 1 \).

The public key is the encryption key is \([e, n]\)

The private key is the decryption key is \([d, n]\).

Compute the cipher text: \( C = P^e \mod n \)

Compute the plaintext: \( P = C^d \mod n \).

The encryption/decryption process comprises the following steps:

**Transmitter**
- Step 1: Initialize all network parameters
- Step 2: Generate data

**RSA/SHIFT Encryption**
- Step 3: Encrypt the data
- Step 4: Transmit the signal as frames

**Receiver**
- Step 5: Receive the signal frames

**RSA/SHIFT Decryption**
- Step 6: Receive and decrypt the data
- Step 7: Plot the results.

3. THE SIMULATION AND RESULTS

3.1. Text Encryption/Decryption Example

The input text file shown below is the plain text (text information in a file) and the characters are converted into numbers and then they are encrypted using our proposed algorithm to get the cipher text and then the cipher text is transmitted over the medium.

*Input Text File:*

Hello Sir,
Good Morning!
How are you?
I will come at 10 AM!

The cipher text file shown below is the cipher text (text information in a file) which was transmitted over the medium. Since the encryption/decryption method is based on modular exponentiation, it is very hard for the hacker to get the information from this cipher file as factoring the modulus for which there is no polynomial algorithm yet [1].

*Cipher Text File:*

Hello Sir,
Good Morning!
How are you?
I will come at 10 AM!

The above text files:
- Input: Transmitter
- Output: Receiver
- Cipher: Wireless medium represent the results of RSA/SHIFT secured wireless system.

Since our encryption algorithm is based on modular exponentiation, and there no polynomial algorithm to factor the used modulus, we believe that the results are practical and secure in wireless systems.

3.2. Voice Encryption/Decryption Example

In figure 2 below, the speech signal waveforms shown. The top waveform indicates the plain text and the middle waveform is the cipher text. The decrypted output speech waveform is shown in the bottom. The input speech signal is sampled, compressed, and then they are quantized. The quantized samples are encrypted using our algorithm. It is very hard for the hacker to get the original speech signal from the ciphered speech signal. The cipher speech is decrypted to get the plain speech signal after proper decompression and Digital-to-Analog Conversion.

![Figure 1. Input/Output Speech (.wav format)](image)

The above voice waveforms in figure 1 are:
- Input (top waveform): Transmitter
- Output (bottom waveform): Receiver
- Cipher (middle waveform): Wireless medium represent the results of RSA/SHIFT

So, since our cryptosystem is based on RSA algorithm which relies on the difficulty of factoring large integers and there no polynomial algorithm to factor the used modulus, we believe the results are practical and secure in wireless systems.

3.3. Image Encryption/Decryption Example

Figure 2 shows a plain image (original) of a bitmap file (*.bmp).

The above waveforms in figure 1 are:
- Input (top waveform): Transmitter
- Output (bottom waveform): Receiver
- Cipher (middle waveform): Wireless medium represent the results of RSA/SHIFT

So, since our cryptosystem is based on RSA algorithm which relies on the difficulty of factoring large integers and there no polynomial algorithm to factor the used modulus, we believe the results are practical and secure in wireless systems.
Figure 2. Input Image (*.bmp file).

Figure 3 shows the cipher image (original) of a bitmap file (*.bmp) and it is very difficult for the hacker to find the image which is being secretly transmitted on the medium.

Figure 3. Cipher Image (*.bmp file).

Figure 4 shows a plain image (original) of a bitmap file (*.bmp) after the decryption process. It is same as the figure 3. We get the decrypted pixels of the image and assemble the pixels back to an image.

Figure 4. Output Image (*.bmp file).

The above image files in figures 3 to 5 are:
- Input: Transmitter,
- Output: Receiver
- Cipher: Wireless Medium) represent the results of RSA/SHIFT.

So, also as we have mentioned above, the results are practical and secured in wireless systems.

4. Conclusion

In this paper, we have proposed a new cryptosystem for encrypting/decrypting multimedia information such as text, audio, and image in less time and at the same time it is very hard for the hackers to get the information which is being transmitted in the wireless medium. The results are extremely convincing and are coincident with the practical existing multimedia wireless applications. Since, our method is based on RSA, the security of our system is based on the idea that the modulus is so large that it is infeasible to factor it in a reasonable time. So, the ease of implementation using recent techniques indicates that this represents a suitable model for next-generation (4G and beyond) wireless communications, in particular for Orthogonal Frequency Division Multiplexing (OFDM) related communications [9],[10].

Issues in videos: video data is not directly encrypted or decrypted. First, video data is converted into a number of image frames and then cryptography algorithm is applied on individual image frames.

References

[1] Behrouz A. Forouzan, “Cryptography and Network Security”, ISBN: 987-007-126361-0, Edition 2008.
[2] Stallings W, "Network Security Essentials", ISBN: 0-13-120271-5, Edition 2003.
[3] Douglas R. Stinson, “Cryptography Theory and Practice”; Chapman & Hall/CRC Press, 3rd Edition, pp. 211-214, 2006.
[4] M. Grangetto, E. Magli, and G. Olmo, “Multimedia selective encryption by means of randomized arithmetic coding,” IEEE Trans. Multimedia, vol. 8, no. 5, pp. 905–917, Oct. 2006.
[5] Hamdan.O.Alanazi et al., B.B.Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, ISSN 2151-617, pp. 152-157, Mar 2010.
[6] Vishwa Gupta et al, Advance cryptography algorithm for improving data security, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, Jan 2012.
[7] M. Ito, N. Ohnishi, A. Alfaolou and A. Mansour, “New image encryption and compression method based on independent component analysis”, IEEE information and communication technologies from theory to application, pp. 1-6, April 2008.
[8] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
[9] Donald L. Schifung, Laurence B. Milstein, Raymond L. Pickholtz, Marvin Kullback, and Frank Miller, “Spread Spectrum for Commercial Communications”, IEEE Comm. Mag., April 1991.
[10] Jianming Wu, et al, A Wireless Multimedia CDMA System Based on Transmission Power Control. In IEEE Journal on selected areas of Comm., Vol. 14, No. 4, pp. 638-644, 1996.