JOURNAL OF NEW RESULTS IN SCIENCE (JNRS)
ISSN: 1304-7981
http://dergipark.gov.tr/jnrs
Research Article

Volume : 6
Issue: 1
Year: 2017
Pages: 1-10

Received: 02.11.2016
Accepted: 05.01.2017

Editors-in-Chief: ***Ebubekir ALTUNTAS***
Area Editor: ***Ahmet FENERCIOGLU***

An Encrypted Messaging Application with Multi Fragmented Caesar Encryption Method between Mobile Devices

Levent GOKREM[a,*] , **Omer Faruk NASIP**[b] ,

[a] *Gaziosmanpaşa University, Faculty of Engineering, Engineering and Natural Sciences, Mechatronics Engineering, 60100 Tokat-Türkiye, email:levent.gokrem@gop.edu.tr*
[b] *Gaziosmanpaşa University, Rectorate, 60100 Tokat- Türkiye, email:omerfaruk.nasip@gop.edu.tr*
**Corresponding author*

ABSTRACT: Mobile devices, especially smart phones are widely used today. Users may benefit from the important services like banking, shopping and messaging, through these devices in mobile environments. This widespread use requires the adoption of various measures to ensure the security of personal information. In this study, a mobile application that allows mobile messaging environment to the people communicating via encrypted messaging was developed. In the application, Multi Fragmented Caesar Encryption algorithm was used. The application was developed for Android devices. This application ensures the information security while two users can message each other securely through a shared encryption key.

Keywords – *Mobile devices, multi fragmented caesar encryption algorithm, android, ınformation security*

1. Introduction

The concept of information security knowledge as an asset of protected from damage by correctly using it, in any environment, to be achieved by preventing unwanted persons can be defined as. In Information Technology security the objective of the threats they may face when using these technologies by analyzing the individuals and institutions taking the necessary measures, we can say that (Canbek and Sağıroğlu, 2006). But, even if all precautions are taken, for the continuous development of attack techniques, no one and no institution, the systems is safe completely we should not assume that (Canbek and Sağıroğlu, 2007). The basic method of cryptography that are used in ensuring information security. Cryptography is the process of making is closed from the open state of data. Cryptography ensures data confidentiality, integrity, safety and security (Coşkun and Ülker, 2013).

Altug M. has used symmetric encryption algorithms for encrypted messaging Polybius algorithm in her study (Altuğ, 2012). Güven B. has aimed his work in formal institutions, especially universities have their own internal correspondence of the application in a computing environment is intended to be done in a secure manner (Güven, 2013). S. M. Çınar and his colleagues in the work of the e-mail system security at the application level with respect to an original algorithm; the encryption process is performed (Çınar et al. 2013). Apart from these, Android, iOS and Windows operating systems that are used for

encrypted Messaging on smartphones with the "telegram" (Anonymous, 2014a) and "TextSecure Private Messenger" (Anonymous, 2014b) on your mobile applications are available.

In this study, mobile application that allows encrypted messaging between smartphones mobile devices widely used today are developed. Multi Fragmented Caesar Encryption Algorithm is used in developed encryption algorithm (Aydoğan, 2014). Application that you are using the SMS service for the transmission of messages a maximum of 160 characters for each message are used.

2. Cryptology

Information is value (Coşkun and Ülker, 2013). From the past up to the present day, has been a major force that must be protected to ensure the continuity of society (Jones, 2005). To achieve this, by being aware of a potential threat is possible (Coşkun and Ülker, 2013). Major information security threats; information losses in the information, make changes to elements such as being possessed by someone else. Cryptology, information security, integrity and privacy are concerned with (Sağıroğlu and Alkan, 2005; Anonymous, 2015e). If we make the definition of cryptography, we can say that hiding and revealing of information is a branch of mathematical science that deals with. The Science of cryptology is divided into two subsystems (Coşkun and Ülker, 2013; Soyalıç, 2005; Yılmaz, 2010; Anonymous, 2015b) (Figure 1):

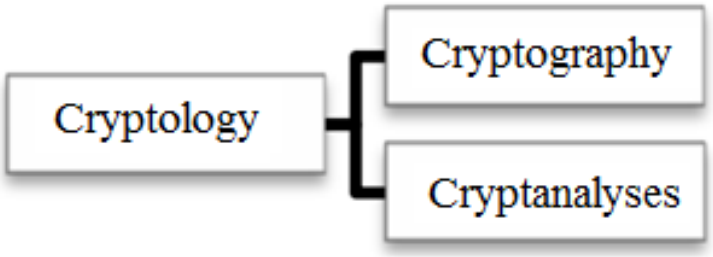

Figure 1. Cryptology the Science of sub-branches (Coşkun and Ülker, 2013)

2.1. Cryptography

Cryptography is the process of converting from open data to become hidden. It ensures data confidentiality, integrity and safety. People who this process is called cryptograph. The understandable text is called plain text or clear text. By being undergone different processes of plain text to be converted into a form that cannot be understood if it is obtained as a result of the new form of the encrypted text is called (Soyalıç, 2005; Yılmaz, 2010; Anonymous, 2015b; Akleylek et al. 2011). The main purpose of cryptography is to ensure the confidentiality of the information. Three basic methods are used for this purpose can be mentioned (Coşkun and Ülker, 2013; Nabiyev, 2010):

- Substitution methods
- Displacement methods
- Algebraic methods

2.2. Cryptanalyses

Analysis of the texts that have been encrypted and the code cryptology is the science which is interested in the solution of the bottom order, the process of obtaining the original text from the encrypted text. From the past until today, cryptograph between analysts as a result of the competition with better and more complex systems continues to be developed and improved (Coşkun and Ülker, 2013).

The encrypted data has always intrigued mankind. There are various techniques in order to obtain the encrypted information cryptanalyses. These techniques are used against offensive techniques is known as cryptography techniques. Some of these are described below (Coşkun and Ülker, 2013):

- Chiphertext-Only Attack
- Letter Frequency Analysis
- Known-plaintext Attack
- Chosen-plaintext Attack

3. Encryption Techniques

Information that is encrypted with a key, however, depending on the algorithm used, can be decrypted with the corresponding key. According to the value of the corresponding key in the message to be sent is encrypted, and is sent to the receiver a clear line. Analyzed according to the value of the received encrypted message key again and clear (understandable) obtains the text. An encrypted message is sent from the transmission line because it can do no harm to third parties to access this message. Here the value of the key that is used in decoding the encrypted message to ensure safety always be kept confidential and should be known by anyone except the recipient. These cryptographic techniques encryption and decryption symmetric and asymmetric key encryption the same key is used that is used that is divided into different techniques (Yılmaz, 2004).

3.1. Symmetric Encryption Techniques

The same key is used for both encryption and decryption. Because it is used in the encryption process one key, this key should be known by anyone except the sender and the recipient. Because of this property, this technique is called secret key encryption.

If we talk about an algorithm that uses a symmetric encryption technique, the first method of this algorithm we have to mention. For example, the letter displacement, placement or reversing of letters between the text, most of these methods are simple ones. Then it is necessary to determine the value of the key for the implementation of this method. This is the oldest known symmetric encryption algorithm in cryptography, a Caesar in the text there is the principle of the shift of a certain number of characters. This determines who can communicate with a key value encryption method. How shifting this value to the Open text, the encrypted text will be encrypted and specifies that shifting how to reverse will be resolved. So the key point here is the key that must remain a secret between the offset values of persons having a texting date (Yılmaz, 2010).

Seen in Figure 2, the general structure of symmetric encryption algorithms.

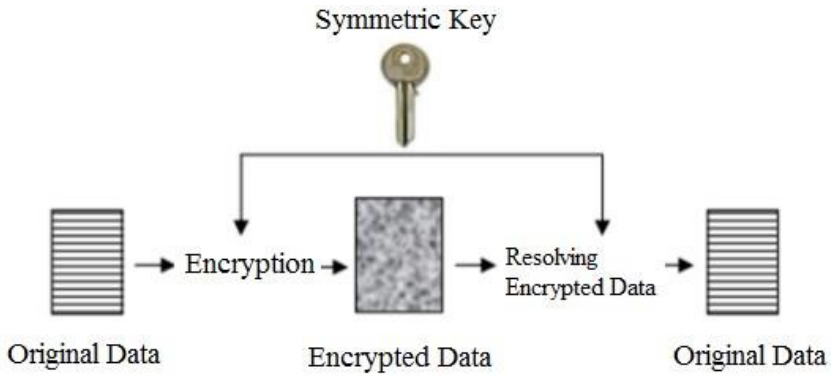

Figure 2. The general structure of the symmetric encryption algorithm (Yılmaz, 2010)

A technique that uses symmetric encryption algorithms, the XOR encryption, des, 3DES, idea, RC2, RC4, RC5 algorithms can be given an example.

3.2. Asymmetric Encryption Techniques

Asymmetric encryption techniques are based on the principle of using a separate key for each of the operations for encryption and decryption. The key used for encryption because it is available to everyone, encryption techniques public-key encryption techniques is called. There are pair of keys in each user open (general) and confidential (private) for encryption. The encryption process is done with the public key that is known by everyone. In the analysis of the encrypted text; only the text was sent, the user knows a secret key is used. In this technique, the sender and the receiver the same secret information (key) the necessity of holding has been eliminated. Any person can send encrypted messages using the public key but only the secret key that pair of it can resolve the encrypted message. There are two primary uses for Asymmetric encryption includes encryption and authentication (digital signature) (Yılmaz, 2010). The general structure of Asymmetric encryption algorithms has been shown in Figure 3.

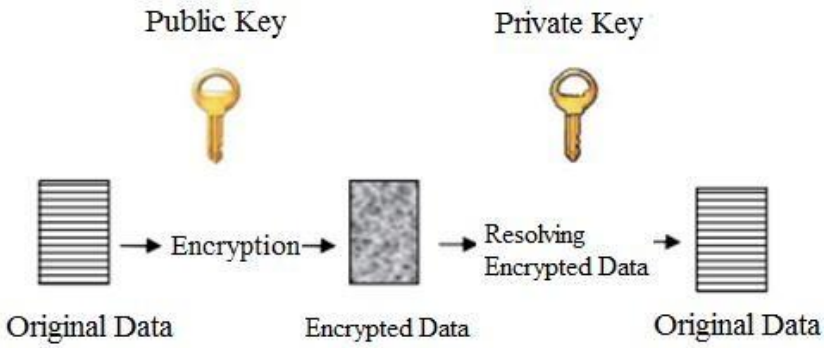

Figure 3. The general structure of an asymmetric encryption algorithm (Yılmaz, 2010)

Examples of asymmetric encryption algorithms RSA, DSA, Diffie-Helman, ElGamal can be given. The most widely used of these is RSA. RSA can be used for message encryption and electronic signature. The RSA algorithm is the first algorithm that is used for the digital signature (Anonymous, 2015a).

4. Encrypted Messaging Application

This In the performed application, "Multi Fragmented Caesar Encryption algorithm" that mentioned in Y. Aydoğan the thesis was used (Aydoğan, 2014). Thanks to this application, the person who is using the application can specify a different key for all the people in the book. The people who use the application, to be able to send encrypted messages to each other for each other for a time sufficient to determine the same key value. After determining the key, communication is done between these two people by this key value. In this way, a third party even gets the encrypted text; because it does not have a key value so will not have access to the clear text. In this application, the best widely used character set that includes 100 characters is used. This Set is used in the application of the sequential case is as follows:

"abcçdefgğhıijklmnoöpqrsştuüvwxyzABCÇDEFGĞHIİJKLMNOÖPQRSŞTUÜVWXYZ0 123456789<>[]_{}!#$%&’()*+-|.,:; @=".

4.1. Multi Fragmented Caesar Encryption Algorithm

At least 2 or more to be determined number of the character for Multi Fragmented Caesar Encryption which is a symmetric encryption algorithm. This number means that there are how many layers of the algorithm. If this number is 3 we can say that 3 Multi Caesar encryption algorithm. In this algorithm each set is determined by the value of the fragmentation key and offset key. When encrypting open text, the values of the indices of the characters of the text will be encrypted and will be processed according to the mode of the number factor. In this way, it's not always the same for each character. Therefore, the breakability of algorithm is quite difficult. Multi Fragmented Caesar Encryption algorithm comprises the following sequential steps:

Step 1: How many multi of the algorithm (K) will be to specify

Step 2: Set K keys K for shift and fragmentation

Step 3: With the function of each part according to the displacement of the shift key, rolling encryption to find

Step 4: Find the encryption function through each character which character would shifting. The number of multi k=3, The fragmentation keys P1= { 15 , 10 , 20 , 30 , 25 } , P2= { 10 , 25 , 15 , 30 , 5 , 15 } , P3 = { 20 , 15 , 25 , 40 } and shift keys R1= { 2 , 4 , 3 , 5, 6 } , R2= { 3 , 2 , 5 , 4 , 3 , 1 } , R3= { 5 , 1 , 4 , 6 } that we have identified as Caesar cipher encryption function, with the "Ankara" text "Çöödçşe" in the form of encrypted. As it is seen the word fourth character "a" for character "c" character, while sixth character "a" for the character "e" character has been. In this example, the encryption path Figure 4.'s is like. The algorithm is a symmetric encryption algorithm because it is also encrypted using the same key texts are resolved. Open the cipher text by applying the inverse of the displacement process (resolved) text is obtained.

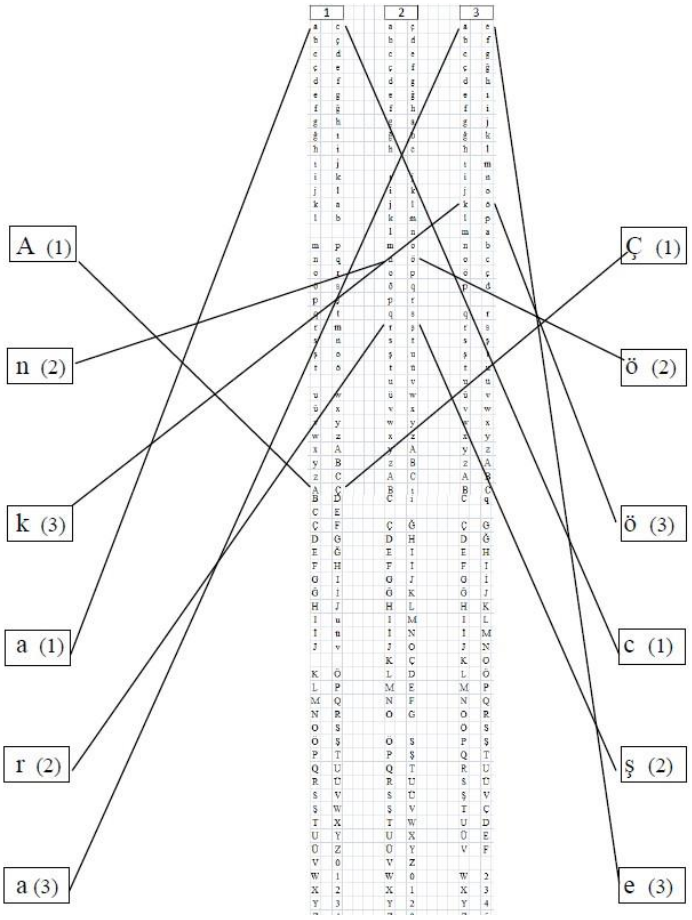

Figure 4. Multi Fragmented Caesar Encryption algorithm example path

4.2. Performed Encrypted Messaging Application

Performed application using by Multi Fragmented Caesar Encryption algorithm ensures clear text to encrypted text and encrypted text to clear text. The application was developed for devices with Android operating system. Transfer and storage of messages was performed by "SMS Manager" in application. This application was carried out using Android Studio software development environment (Okumuş, 2012) with Java programming language (Anonymous, 2015c). Android SQLite was used for database library and the key values for user input in the application (Anonymous, 2015d).

During installation, the application asks for permission to access SMS and phone book from the user. After the installation is done, the users on the first login to the application have been asked to determine a personal password. For open the application, the user has to enter the password correctly every time. This password depending on the user's request can be changed within the application. In this way, people outside of the user are denied access in application. In application, only encrypted messages to enable the display of a special character is added to the beginning of the encrypted message that is sent, and thus a clear message by the application are prevented from being displayed.

That allows determining the value of a different key for every record in the book thanks to the application, contacted by a different channel for each record. If a foreign person has not

public encryption key, encrypted texts analysis is impossible. This is very important for the security of personal information.

4.3. The Application's Interface and Steps to Use

The application is installed to devices with Android operating system .apk extension by using the setup file. User successfully login to the application and the application is determined the input password is entered correctly redirected to the main page. There are too display of incoming and outgoing encrypted message, encrypted message and a key to the numbers in the book to write new to be able to assign buttons to switch to pages on the homepage (Figure 5).

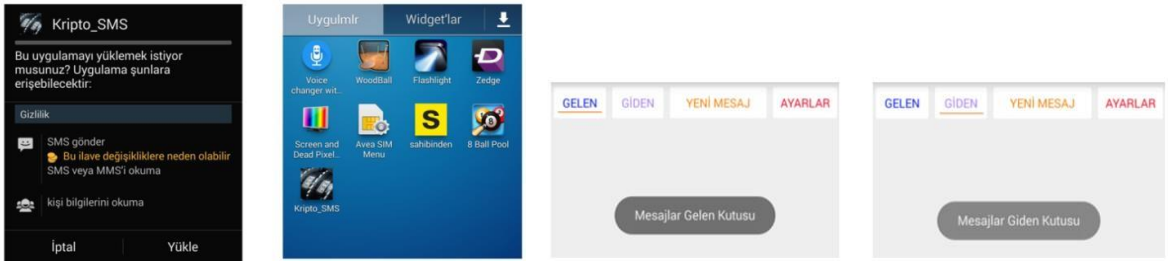

Figure 5. In the installation menu of the application view, the listed pages of incoming and outgoing messages

On the settings page, in the phone book for contacts that are assigned an encryption key. The key assignment is selected and the person from the contacts list will be made the number appear in the text. The desired key value is entered in the key part and save button is pressed. Thus, the person with this key, the key value will be saved and sent to him encrypted messages to be sent Figure (6, 7, 8, and 9).

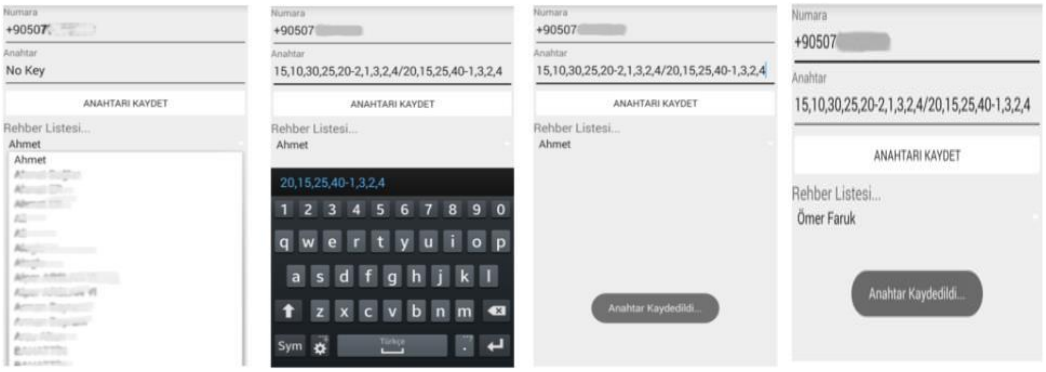

Figure 6. Key assignment

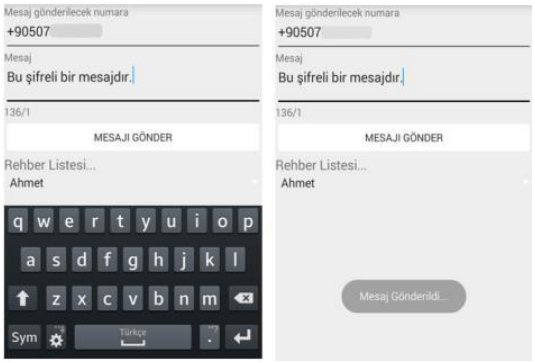

Figure 7. Creating and sending new messages

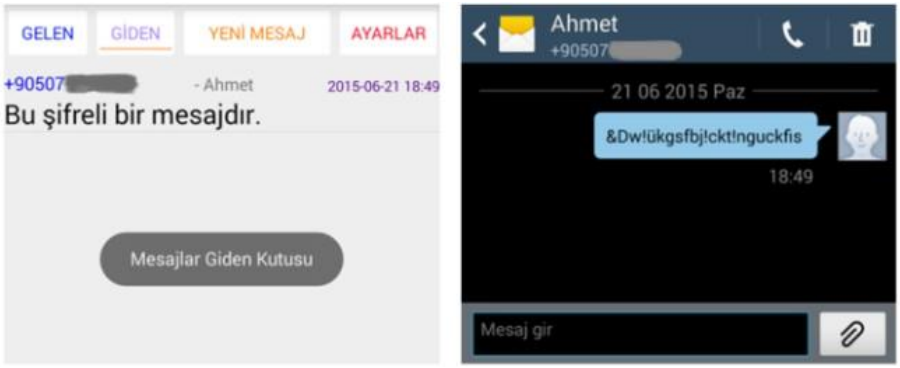

Figure 8. The appearance of the encrypted message that is sent outside of the application view in the application and resolved

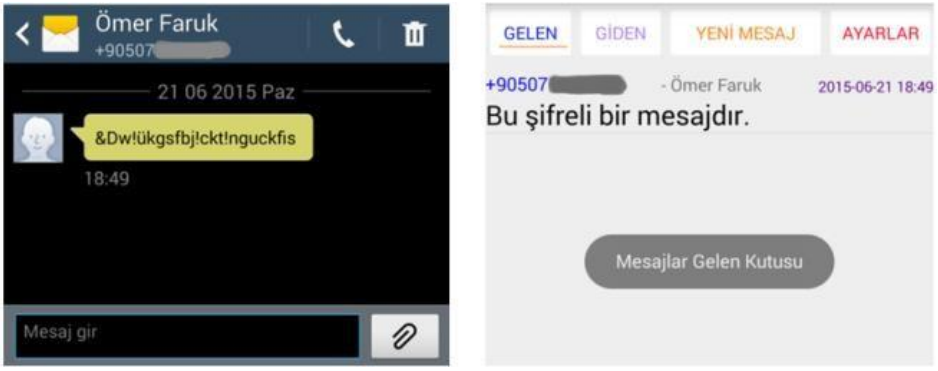

Figure 9. Received and resolved outside of the encrypted message within the application view the application view

5. Result and Discussion

The application that developed for devices with Android operating system which is quite common, for message communication using SMS technology between the devices. In application, the use of SMS technology, it should not need an Internet connection and uses of the width of the area in terms of accessibility are advantageous condition.

Thanks to Multi Fragmented Caesar Encryption algorithm, which is the encryption algorithm that is used in the application-encrypted messages to be resolved by a frequency analysis of the letters in the alphabet the letters are prevented. Because this is symmetric encryption method the encrypted text in the Open text did not correspond to the same character and the same character always. Password for logging in to the application the level of security that is much greater. However, the encrypted text can be analyzed with Kasiski analysis method.

Personal and corporate information securities are very important nowadays. Thanks to this application, to persons or organizations between each other, they can communicate securely with the help of a common encryption key is determined. This study developed in the future, the implementation of applications that provide encrypted voice and video communication services is targeted.

References

Akleylek, S., Yıldırım, H. M., Tok, Z. Y., 2011. Cryptology and Its Applications: Public Key Infrastructure and Certified Electronic Mail. Akademik Bilişim, İnönü University, Malatya, 713-718.

Altuğ, M., 2012. An Encrypted Messaging Application for Mobile Phones with Polybius Algorithm. (Master Thesis), Gazi University, Bilişim Enstitüsü, Department of Electronic and Computer Systems Education, Ankara.

Anonymous, 2014a. Telegram. https://telegram.org Access Date: 23.06.2015

Anonymous, 2014b. TextSecure Private Messenger. https://play.google.com/store/apps/details?id=org.thoughtcrime. securesms&hl=tr Access Date: 02.06.2015

Anonymous, 2015a. Android Studio IDE. https://developer.android.com/sdk/index.html Access Date: 21.05.2015

Anonymous, 2015b. Kriptoloji, http://tr.wikipedia.org/wiki/Kriptoloji Access Date: 10.06.2015

Anonymous, 2015c. Java Official Web Site. https://www.java.com/tr/ Access Date: 21.05.2015

Anonymous, 2015d. SQLite Android Bindings Documentation. https://www.sqlite.org/android/doc/trunk/www/index.wiki Access Date: 21.05.2015

Anonymous, 2015e. Tübitak Bilgem Ulusal Bilgi Güvenliği Kapısı. "BGYS- 0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu". http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html Access Date: 12.06.2015

Aydoğan Y., 2014. Multi Fragmented Caesar Cipher Method and Its Applications. (Master Thesis), Gaziosmanpaşa Üniversity, Institute of Sciences, Department of Mathematics, Tokat.

Canbek, G., Sağıroğlu, Ş., 2006. A Review on Information, Information Security and Security Processes. Journal of Polytechnic, 9(3), 165-174.

Canbek, G., Sağıroğlu, Ş., 2007. Attacks Against Computer Systems and Their Types: A Review Study. Erciyes University Journal Of Institue of Science, 23(1-2), 1-12.

Coşkun, A., Ülker, Ü., 2013. Development of A Cryptographic Algorithm for National Information Security and Determination of Confidence Against Letter Frequency Analysis. International Journal of Informatics Technologies, 6(2), 31-39.

Çinar, M.S., Çinar, I., Bilge, H.Ş., 2013. Secure Email Application Using an Original Encryption Algorithm. 6th International Information Security & Cryptology Conference, pp. 332-337, 2013.

Güven, B., 2013. Development of Cryptographic Document Management Systems Devoted to Non-Documentation of Work Procedures for Universities. (Master Thesis), Karabük Üniversity, Institute of Sciences, Department of Computer Engineering, Karabük.

Nabiyev, V., 2010. Yapay Zekâ. 3. baskı, Ankara.

Jones, A., 2005. Information Warfare-what has been happening? Computer Fraud&Security.

Okumuş, İ., 2012. The Factors Affecting Speed of the RSA Cryptosystem. (PhD Thesis), Atatürk Üniversity, Institute of Sciences, Department of Mathematics, Erzurum.

Sağıroğlu, Ş., Alkan, M., 2005. Bilgi Güvenliği Bilimi (Kriptoloji), Her Yönüyle Elektronik İmza. Grafiker Yayınları, Ankara, 21-50.

Soyalıç, S., 2005. Cryptographic Hash Functions and Its Applications. (Master Thesis), Erciyes Üniversity, Institute of Sciences, Department of Mathematics, Kayseri.

Yılmaz, R., 2010. Some Statistical Tests for Cryptographic Applications. (Master Thesis), Selçuk University, Institute of Sciences, Department of Statistics, Konya.

Yılmaz, T., 2004. The Solutions of Security Problems for Smart Cards. (Master Thesis), Selçuk University, Institute of Sciences, Department of Computer Systems Education, Konya.