

SECURITY APPROACHES IN INTERNET COMMUNICATION

Utku KOSE

Afyon Kocatepe University, Turkey
utkukose@aku.edu.tr

ABSTRACT

In today's world, information security is an essential factor, which must be taken into consideration to ensure secure applications and services in information technology. Since the inception of the information technology concept, there has been a remarkable interest in security approaches that aim to protect information or digital data. Especially, rise of the Internet and internet technologies has caused searching for newer approaches, methods and techniques that try to provide secure internet communication sessions for computer users over the Internet. In this sense, this chapter aims to examine security approaches in internet communication. For this purpose, role of the coding science: "cryptology" in providing secure internet communication and related techniques in this scope are also explained within the chapter. Furthermore, in order to give an example for usage of cryptology techniques, an e-mail application, which was developed to send or receive encrypted e-mail messages, is also introduced in this chapter.

Keywords: information security, internet communication, encryption techniques.

1 INTRODUCTION

Nowadays, the security concept is an important factor, which is associated with almost all fields in peoples' modern life. It is too important that this concept has been a remarkable subject to the humankind for a long time period. Basically, the "security" term can be defined as "the protection of a person, property or organization from an attack" [1]. But it also has more specific meanings that are used to define similar situations, aspects and features of different fields in the life. Additionally, there are also different concepts, which are derived originally from the "security" term and used to define security approaches and techniques in different fields. The term: "information security" is one of these concepts and it is mostly associated with information technology.

Briefly, the information security term is described as protecting information or digital data against any attack that can be performed by using different attacking technologies, methods and techniques [2]. At this point, the popularity and extensiveness of information security is connected with advancements, developments and improvements in the field of information technology. Actually, the rise of the Internet and internet technologies has caused rapid developments and improvements in information security and formed its current situation in the modern life. Today, it is more important to ensure secure web services and web applications for

people who use these technologies to perform their works and communicate with other people from all over the world. Especially, providing secure internet communication between two people has become an important subject that must be taken into consideration for protecting send or received digital data. Because of this, there are many different approaches, methods and techniques that try to provide secure internet communication sessions for people over the Internet.

This chapter aims to examine the foremost information security approaches in especially internet communication. Additionally, role of the cryptology in providing secure communication sessions and related methods or techniques that can be evaluated in this sense are also examined and explained in the chapter. In this aim, principles of encryption techniques like private-key encryption and public-key encryption and their usage in the internet communication systems or applications are explained. As an example for usage of these cryptology techniques, an e-mail application, which was designed and developed to be used for sending or receiving encrypted e-mail messages, is also introduced in the chapter. This application employs a private-key encryption algorithm, which aims to provide an effective approach to encrypt the mail message and related attachments. By explaining structure of this algorithm and features of the related application, the chapter tries to give more concrete ideas about security approaches in internet communication.

The chapter is organized as follows: The second section explains the foremost approaches, methods and techniques that can be used to ensure a secure internet communication. This section also introduces some systems and programs that can be used to provide security in communication sessions. Immediately afterwards, the third section introduces the coding science: cryptology and explains using features of widely-used encryption techniques briefly. Next, the fourth section introduces the related e-mail application and finally, the chapter ends with a discussion–conclusions section.

2 ENSURING SECURITY IN INTERNET COMMUNICATION

In order to ensure security in internet communication, many different approaches, methods and techniques have been introduced in time. Additionally, different kinds of systems and programs have also been designed and developed to implement introduced approaches, methods or techniques in the internet environment. Definitely, all of these developments and improvements aim to ensure a secure communication over the Internet. At this point, the “secure communication” concept must be defined in order to understand the subject better. Secure communication can be defined as performing communication in different ways that make a third party unable to listen to the communication session [3, 4]. Nowadays, this concept is used as the “secure internet communication” to define security aspects of the internet communication.

2.1 Security Approaches in Internet Communication

Security approaches in internet communication can be examined under different categories and titles. In this section, the foremost approaches, methods and techniques are taken into consideration to explain the subject briefly. In internet communication, the security can be categorized under three main titles. These are [5, 6]:

- Hiding the content,
- Hiding individuals of the communication,
- Hiding the communication environment.

The first title: “Hiding the content” examines the approaches that enable users to hide contents of messages (information or digital data) that are received or send during the communication session. The related approaches include “encryption”, “steganography” and “identity based systems” [5, 6]. The encryption is the technique of making information or digital data unclear with special mathematical functions. The encryption is explained in more detail in Section 3. Steganography is an approach that is used to hide information or digital data in a digital media like

voice, video and pictures. This can be done by replacing the least significant bit of each pixel belonging to the chosen media [7]. Figure 1 shows a representative sample that explains steganography. The last approach: identity based systems try to provide secure communication by evaluating each user’s identity. In this way, the communication channel is open to only trusted users.

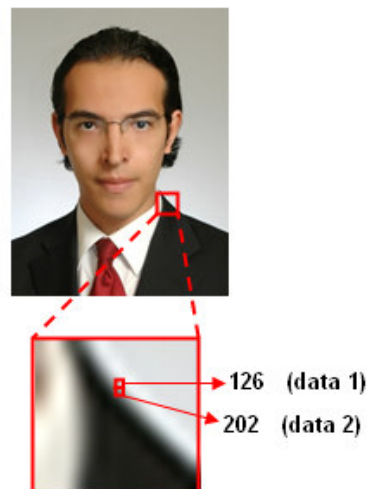


Figure 1: A representative sample that explains steganography

The second title: “Hiding individuals of the communication” examines the approaches that aim to hide individuals of the communication from third parties or malicious factors. The term: “anonymity” can also be used to define approaches under this title. The related approaches include “anonymous systems or applications” and “trace routing techniques” [5, 6]. Anonymous systems or applications are some kind of software or hardware solutions that enable users to hide themselves from factors that want to listen to the communication session. For instance, “anonymous proxies” allow computer users to access to the Internet via fake addresses of different countries and they become untraceable in this way. Figure 2 represents a diagram that shows the anonymous proxy approach simply. In addition to anonymous systems and applications, some special routing techniques also enable users to become untraceable.

The last title: “hiding the communication environment” refers to the approaches that allow users to make the communication environment “hidden”. The simplest way to achieve this work is to make communication environment less popular and notable on the Internet environment. Apart from this, a random data flow can also be created for the communication environment. By creating random data flow, the communication environment becomes harder to detect.



Figure 2: Anonymous proxy approach

2.2 Systems and Programs to Ensure Security in Internet Communication

On the market, there are many different types of systems and programs that are widely used to ensure security during internet communication. These systems and programs can be categorized under the titles below:

- Firewalls,
- Anti Virus-Spyware-Malware Programs,
- Monitoring Systems,
- Encryption-Decryption Systems,
- Secure Messaging (IM) Programs,
- Secure Conferencing Programs,
- Other Specific Systems or Programs

Firewalls are some kind of program or hardware systems that are specially designed and developed to block unauthorized access to a computer system [8]. Nowadays, there are many different firewall programs that can be installed and used over an operating system. Some software companies like “Agnitum” and “Check Point Software Technologies Ltd.” develop and provide today’s popular firewall programs like “Outpost” and “Zone Alarm”. On the other hand, there are also more advanced hardware systems that act as firewalls for more advanced computer systems like servers.

Anti Virus-Spyware-Malware programs provide security solutions against dangerous program and code types like viruses, trojans, spywares and malwares. Protecting computer systems against these types of dangerous factors is too important to ensure security for especially internet communication. Today, different software companies like “Kaspersky Lab.”, “Eset”, “Symantec”, “McAfee” and “Trend Micro” provide

special programs that combine functions of Anti Virus-Spyware-Malware protecting mechanisms. Furthermore, there are also more advanced and effective programs that combine both firewall and Anti Virus-Spyware-Malware protecting mechanisms. These programs are usually called as “Internet Security” programs. As a result of increasing number of dangerous program, code types and other malicious factors, computer users, who often work on the Internet, often prefer to use “internet security” programs.

Monitor systems are often used to watch active processes over a network system. By using this type of systems, unwanted activities over the network system can be detected easily and necessary precautions can be taken against possible attacks in the future. In this way, unwanted third parties and malicious factors on a special communication session can be detected and removed immediately. Nowadays, there are many kinds of monitoring systems that are developed by different software companies. For instance, “Microsoft” offers a free network monitoring program named “Microsoft Network Monitor”. Additionally, another company named “Paessler” works on only network programs and provides a free network monitoring tool. Finally, “Net Optics” provides many different advanced monitoring and filtering solutions for communication security.

In order to achieve a secure communication, another method is using encryption-decryption systems. On the market, there are hardware and software based encryption-decryption solutions that try to provide high-level security for valuable information and stored digital data. Today, encrypting information and digital data is the most effective and popular approach to provide security in almost all fields of the modern life.

By combining different kinds of security approaches, some secure instant messaging (IM) and conferencing programs have been designed and developed by software companies. Some of these programs are also “open source” and they offer “free” and “developing” security solutions for internet communication. For instance, “Skype” is one of the most popular internet communication programs and it provides secure voice and chat communication with 128 bit AES and 1024 bit asymmetrical protocols [6]. On the other hand, “Zfone” is an open source program that enables users to make secure voice communication. Some popular IM programs like “Yahoo Messenger” uses secure approaches to provide more security in their communication services. “WASTE” is also another IM program that uses high strength “end-to-end” encryption and an anonymous network. As different from other ones, the WASTE is an open source IM program [6].

In addition to the mentioned ones, there are also many more systems or programs that have

been developed to be used for more specific aims. Some of these systems or programs ensure the security indirectly. Because of this, they must be used with the support of other security systems or programs.

3 THE CODING SCIENCE: CRYPTOLOGY AND ENCRYPTION TECHNIQUES

Today, different types of mathematical methods and techniques are used to send information or digital data from one place to other places safely. The related methods and techniques also enable computer users to store their valuable information or digital data with more secure approaches. These methods and techniques are examined within “Cryptology”. Cryptology is the name of the science, which incorporates both “cryptography” and “cryptanalysis”. Cryptology can also be called as the “coding science”. At this point, cryptography and cryptanalysis refer to different aspects of the cryptology. Because of this, these terms must be defined in order to understand main scope of the cryptology.

Cryptography is the field of encrypting information or digital data by using mathematics, computer science and engineering approaches. On the other hand, cryptanalysis is associated with studies and practices of making encrypted information or data unencrypted. In this sense, cryptanalysis works on weak and strong features of an encryption algorithm designed and developed within cryptography approaches [9, 10]. In other words, cryptanalysis is the field, which is used to analyze and break safe communication sessions. In order to achieve this, cryptanalysis employs different types of methods and techniques like analytic judgment, applications of mathematic tools and combinations of figure definition. Figure 3 represents a diagram that shows fields of the cryptology.

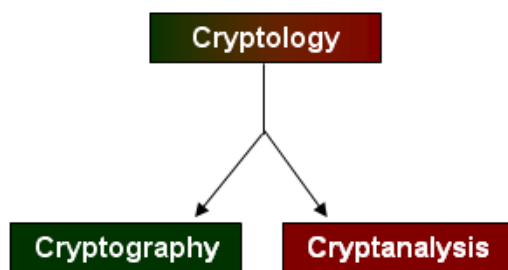


Figure 3: Fields of the cryptology

There are three more terms that must be examined within this subject. These are: cryptographer, cryptanalyst and cryptologist. Cryptographer is the term, which is used to define person whose work or research studies are based on

cryptography. On the other hand, the person who studies on cryptanalysis is called as the cryptanalysis. As it can be understood from previous explanations, both the cryptographer and the cryptanalysis are cryptologists.

Cryptology is too important for computer users because it provides security for computer-aided works such as transferring data between computer systems, designing and developing new computer-based technologies and also performing Internet communication. In today’s world, cryptology is also often used to provide security in computer-based systems or applications like e-business, e-marketing, e-science, e-government and e-signature [11]. At this point, two elements of the cryptology: encryption and decryption techniques have important roles on status of provided security levels. The encryption term can be defined as transforming information or digital data with a special function and the encryption key used by this function. On the other hand, decryption is defined as converting the encrypted information or digital data to its original, unencrypted form. In encryption works, two different encryption-key techniques are widely used. These are named as “public-key encryption” and “private-key encryption” respectively. Today, another approach, which is called as “Hybrid Cryptosystem”, is also used to combine advantages of both public-key and private-key encryption techniques. In order to have more idea about cryptology and its effects on Internet communication, it is better to explain features of public-key and private-key encryption techniques.

3.1 Public-Key Encryption

Public-key encryption technique can also be called as “asymmetric encryption”. In this encryption technique, the user, who wants to ensure a secure communication, needs two different keys. These keys are called as “private key” and “public key” respectively. Each key that the user can use has different roles during the communication. The public key is known by everybody. But the private key is known by only one user. The encryption process is performed by using the public key whereas the decryption process is performed with the private key [12, 13]. At this point, some mathematical equations are used to make the connection between public and private keys. In other words, encrypted information or digital data can be decrypted by using the private key, which is connected with the public key that was used for encrypting the mentioned information or digital data. Because of this, it is impossible to decrypt the encrypted information or digital data with the help of other private keys. In this technique, it is too important that the user must hide his / her private key from other users. But he / she can share the public key with other people [14]. Figure 4

represents a diagram that explains a typical communication session based on public-key encryption technique.

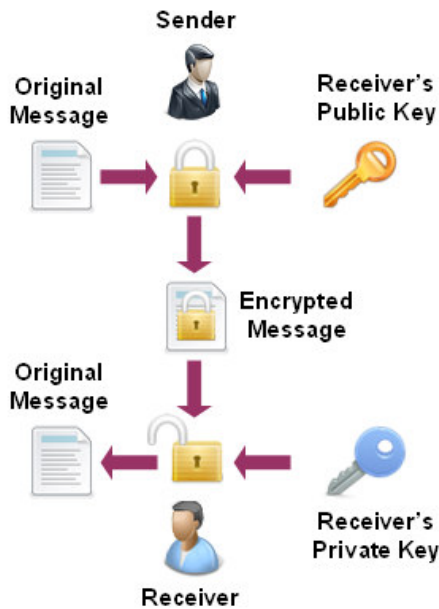


Figure 4: A typical communication session based on public-key encryption technique

Today, RSA (Rivest-Shamir-Adleman) algorithm is the most popular approach that uses the public-key encryption technique. In addition to this algorithm, El Gamal, PGP (Pretty Good Privacy), Diffie-Hellman key definition and DSA (Digital Signature Algorithm) are also other widely used approaches that use the public-key encryption technique [14 – 16].

3.2 Private-Key Encryption

Private-key encryption technique can also be called as “symmetric encryption”. In this encryption technique, only one key is used for encrypting or decrypting the information or digital data [12, 17]. The private-key encryption technique comes with two different approaches: “block encryption” and “row encryption”. In block encryption systems, the original message is separated into fixed length blocks and each block is encrypted individually [9]. In this way, a block is matched with another fixed length block from the same alphabet. In designing of block codes, mixing and diffusion techniques are used and these techniques are applied by using “permutation” and “linear transformation” operations respectively [18]. At this point, strength of the related block encryption algorithm is set by S boxes, number of loops, using keys in XOR operations, block length and key length. Using random key is also another

important factor to improve strength of the applied algorithm [19]. The other approach: row encryption is a new form of permutation algorithms which were used in the past [9]. Row encryption technique needs a long key data. Because of this, transition files with feedback feature are used to produce a half-random key. The encrypted message content is created by performing XOR operations with the produced key on the original message. At this point, the receiver must produce the same key in order to decrypt the encrypted message [9]. Figure 5 represents a diagram that explains a typical communication session based on private-key encryption technique.

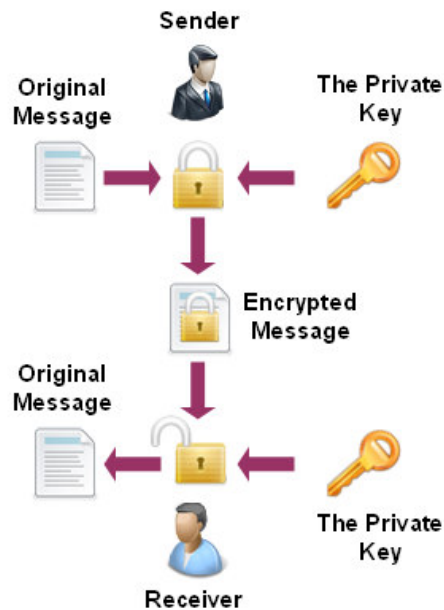


Figure 5: A typical communication session based on private-key encryption technique

Today, DES (Data Encryption Standart) algorithm is the most popular approach that uses the private-key encryption technique. Additionally, AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorirhm), Skipjack, RC5, RC2 and RC4 algorithms are also other popular approaches that use the private-key encryption technique [11, 14 – 16, 19].

The explained encryption techniques provide different types of security solutions and approaches for different systems. Because of this, their advantages and disadvantages must be known to choose suitable technique for any designed system. Private-key encryption ensures a fast encryption technique whereas public-key encryption provides a slow, but a trusted one. Additionally, private-key encryption technique is useful on digital data, which is stored in a media [12]. But it may be expensive to ensure security in sharing the private

key with other users. Although public-key and private-key encryption techniques employ some different features, they are widely used in different types of applications or systems, which aim to ensure security in especially Internet communication.

4 A SECURE APPLICATION FOR E-MAIL COMMUNICATION

In order to give more concrete ideas about security approaches in internet communication, a sample e-mail application can be examined in detail. The developed application enables computer users to encrypt their message text and attachments and send the encrypted content to the receiver(s) via easy-to-use interface. At this point, decryption of the message is done by the receiver(s) with the same application. The application comes with a simple but strong enough private-key encryption algorithm to ensure security for send or received e-mail messages. Before explaining the encryption algorithm of the application, it is better to explain using features and interface of the developed application.

4.1 Using Features of the Application

The e-mail application was designed and developed by using the C# programming language. At this point, object oriented programming methods and techniques allowed developers to create a fast, stable and simple application structure. Interfaces of the application have been formed with simple but effective controls. Coding and designing processes of the application were performed on the Microsoft Visual Studio 2005 platform. Figure 6 represents a screenshot from the application.

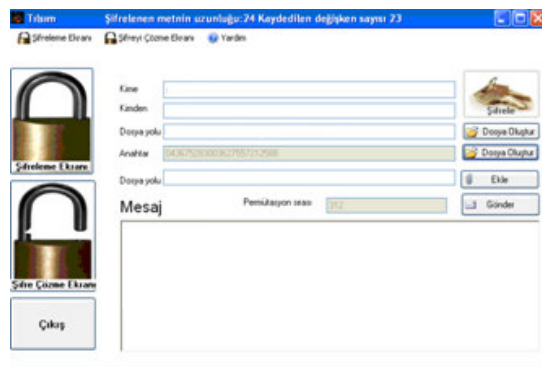


Figure 6: A screenshot from the application

The e-mail application has a user friendly design and simple controls that enable computer users to perform the related operations in a short time. The application comes with three different interfaces, which can be used to perform different

operations related to e-mail communication. The user can view these interfaces by using the provided controls on the application. With the first interface, folders of the adjusted mail address (inbox, sent box...etc.) can be viewed. On the other hand, other two interfaces are used for encrypting plain mail messages or decrypting the received encrypted ones. In this way, the same application can be used by both sender and receiver users to ensure a secure communication. Working structure of the developed communication system is shown in Figure 7 briefly.

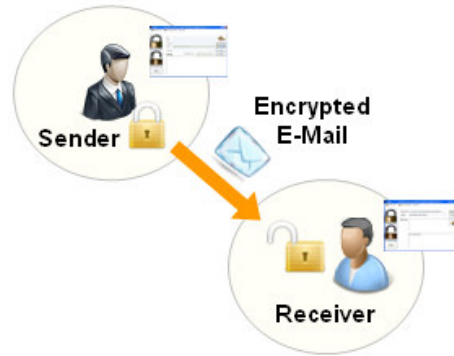


Figure 7: Working structure of the developed communication system

This simple but strong enough application employs an effective private-key encryption algorithm, which enables user to encrypt their original mail message text and related attachments with some basic mathematical functions. In this way, a secure e-mail communication channel between two users can be realized easily. In order to have more idea about security aspects of the e-mail application, features of this algorithm must be explained in detail.

4.2 The Encryption Algorithm

The encryption algorithm, which is provided in the developed application, ensures strong approaches to change original form of the message text to more complex and different forms of data. For instance, the whole message text is divided into some blocks to improve effectiveness of the encryption approach. At this point, variable blocks are used instead of constant blocks. Additionally, the security level of the algorithm is increased by producing random numbers for each encryption process. Moreover, this algorithm also requires longer encryption keys for longer message texts. Thus, longer message texts are encrypted with more complex keys. On the other hand, the most important feature of the algorithm is that it is based on the private-key encryption technique. With the support of the private-key encryption, the

developed algorithm offers an effective and fast encryption process. Furthermore, it also supports encrypting big size data.

With the developed algorithm, the encryption process is performed and completed in four steps. These are:

- Separation of the original text,
- Random permutation production method,
- Key production and bit-level encryption (XOR method),
- Production of the key and the encrypted data.

Under the next subtitle, these steps are explained in more detail.

4.2.1 Encryption steps

The first step of the encryption process is based on separation of the original message text into different numbers of text blocks. The related number is automatically defined according to the character count of the text. Separation of the text is also performed according two rules: If the character count of the original text can be divided into three and a half or seven, the original text is separated into the character count. Otherwise, the character count is set to a definite number, which can be divided into five. In order to achieve this, some space characters are added to the original message text.

In the next step, random permutation production method is used to change original content of the message text. For this purpose, random numbers are produced for each block, which was obtained in the first step. Positions of each character in the blocks are changed according to produced random numbers. As a result of changing character positions, a simply encrypted text, which was created with the permutation method, is obtained. With the permutation method, properties of the related text characters are protected. But their positions are automatically changed [17].

In the third step, the final form of the encrypted message text is obtained. In this sense, random numbers between 0 and 9 are produced according to character count of the encrypted text and each character of this text is encrypted at bit-level with randomly produced key numbers. During the encryption process, the XOR (eXclusive OR) method is used [According to the XOR method, the result (output) is “1”, if two inputs are “different”. Otherwise, the result (output) is “0”]. As a result, a set of new characters are obtained for the last form of the message text. Table 1 shows some examples for the XOR encryption process of different characters.

Table 1: Some examples for the XOR encryption process of different characters.

| Character (in binary) | Key (in binary) | Encrypted Character (in binary) |
|--------------------------|--------------------|------------------------------------|
| Z (01011010) | 3 (00000011) | Y (01011001) |
| A (01000001) | 7 (00000111) | F (01000110) |
| J (01001010) | 9 (00001001) | C (01000011) |
| U (01010101) | 1 (00000001) | T (01010100) |
| M (01001101) | 5 (00000101) | H (01001000) |

In the last step, created encryption – decryption key and the encrypted data are organized in two separate temporary files and contents of these files are transferred to the application interface to be saved by the user in .txt file formats. Figure 8 represents a flowchart, which briefly explains and shows each step of the developed encryption algorithm.

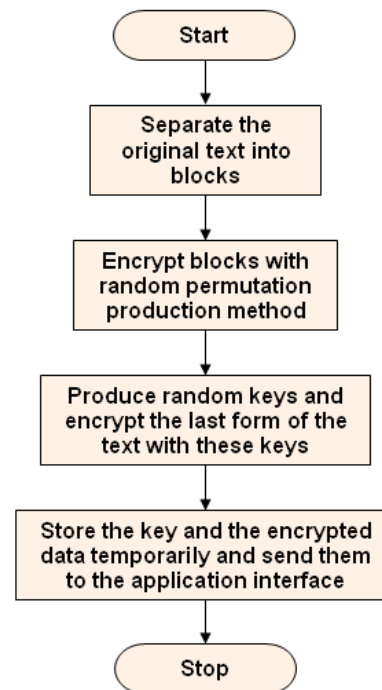


Figure 8: Flowchart of the developed encryption algorithm

By using the explained algorithm steps, the developed application allows users to encrypt both their mail messages and attachments easily. At this point, it is also important to explain decryption process of the application.

In the decryption process, the obtained key file is used by the application for the encrypted mail message text. In order to understand decryption steps better, main parts of the key file must be examined first. Figure 9 shows a brief schema that shows the related key file parts.

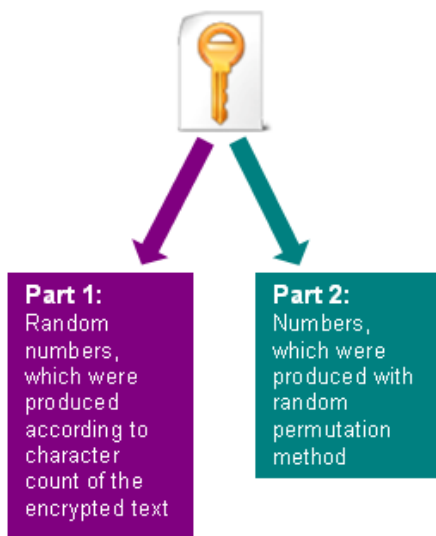


Figure 9: Parts of the key file

As it can be seen from the Figure 9, the key file consists of two different parts, which can be called as “Part 1” and “Part 2” respectively. During the decryption process, the application gets the encrypted form of the text [before the bit-level encryption (XOR)] by using the “Part 1”. Afterwards, the original message text is created by using the “Part 2”. At this point, the original message text is the decrypted text for the receiver. As a result, the receiver has a chance to get the original message in a more secure way with the help of mentioned method.

All of the explained processes are performed by the e-mail application via two different interfaces. In the application, these interfaces are named as “Encryption Screen” and “Decryption Screen” respectively. In order to have more idea about usage of the e-mail application, these interfaces must be explained briefly.

4.3 Encryption and Decryption Interfaces of the Application

As mentioned before, the developed e-mail application includes simple and user friendly interfaces to provide fast and easy using experience for computer users. As different from e-mail folder interface, “Encryption Screen” and “Decryption Screen” have similar interfaces and controls. For encrypting any mail message text, the user can open the Encryption Screen. Figure 10 shows a

screenshot from the Encryption Screen of the e-mail application.

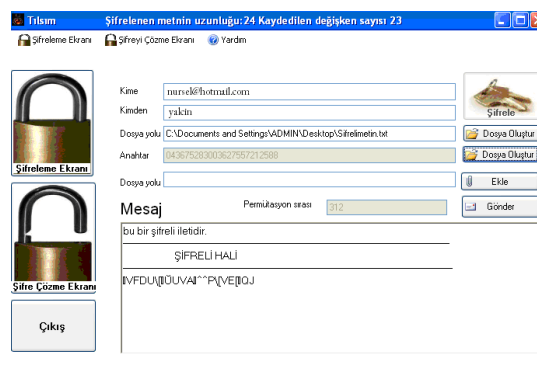


Figure 10: A screenshot from the Encryption Screen of the e-mail application

In order to provide a fluent using experience, users are enabled to change the view to encryption or decryption interfaces (screens) by using two buttons located on left and top side of each “screen”. Additionally, the users are enabled to learn more about the usage of the related “screen” by using the “Help” button. On the Encryption Screen, the user can type the original message text under the “Message” field. On the other hand, there are some more fields that are associated with typical e-mail message fields like “To” and “From”. Additionally, the user can also add one or more attachments to the message by using related controls on this screen. In order to start the encryption process for the mail message and related attachments, the “Encrypt” button can be used. During the encryption process, some statistical information can also be viewed on the title bar of this screen. At the end of the process, two .txt files are created for the produced key and the encrypted data. These files can be saved by the user to any directory. At this point, it is important to use .txt file type for the encrypted data to protect its content from foreign characters, which can be produced by other word processor programs. Moreover, process time is also lowered by using the .txt file type for the encrypted data.

After getting the key and the encrypted data, the user can send the message to the receiver(s) by using the “Send” button located on the Encryption Screen. While sending the encrypted mail message to the receiver, restrictions, which are applied by ports or firewalls, may affect the e-mail application. In order to solve this problem, a remoting application, which is held in a trusted authority, was developed. With this application, communication with the authority is performed over the port: 80, by using shaped XML structure, which is suitable for the semantic data model.

After receiving the encrypted e-mail, the Decryption Screen of the application can be used to

get the original mail message and its attachments. The Decryption Screen was designed as similar to the Encryption Screen. Figure 11 shows a screenshot from the Decryption Screen of the e-mail application.

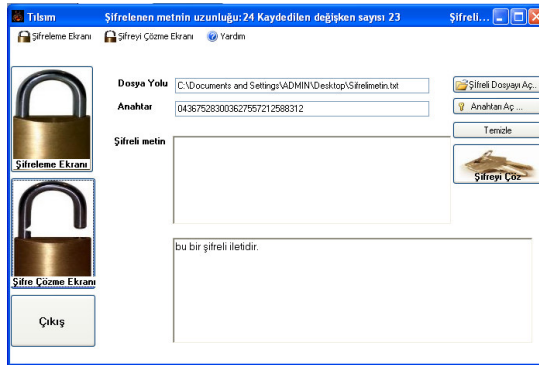


Figure 11: A screenshot from the Decryption Screen of the e-mail application

On the Decryption Screen, the receiver can view the encrypted message text under the “Encrypted Text” title. After choosing the key file, the text can be decrypted by using the “Decrypt” button. As soon as the decryption process is finished, the original text is shown in the text field located on bottom side of the Decryption Screen.

The introduced e-mail application provides an effective and strong security solution for e-mail communication over the Internet. It is too important that examining using features and functions of this application enables readers to have more concrete ideas about security approaches in today’s internet communication. Definitely, there are also many different kinds of applications or systems that try to ensure security for different fields of internet communication.

5 DISCUSSION–CONCLUSIONS

This chapter explained the foremost information security approaches in especially internet communication. In this sense, role of the cryptology in ensuring security for communication sessions and its fields that can be examined in this scope were explained in the related sections. In order to explain more about usage of cryptology in communication security works, principles and functions of encryption techniques like private-key encryption and public-key encryption were also examined. At this point, an e-mail application, which can be used for sending or receiving encrypted e-mail messages, was also introduced to enable readers to have more idea about the usage of cryptology and encryption techniques in providing security for internet communication. Features and functions of this application provide a simple but

strong enough approach to support explained subjects about the security factor in internet communication.

Today, the security concept is an extremely important subject because the information is currently more valuable for the humankind and there is a supremely effort to protect “valuable information” from environmental factors. As a result of rapid developments in the technology, more advanced systems, which provide better security solutions for valuable information or digital data, are designed and developed expeditiously. With the related developments in the technology, it is expected that the number of different attacking and “security breaking” methods and techniques will be reduced in time. But conversely, more attacking and “security breaking” methods or techniques are designed and developed by malicious people from day to day. Because of this, more research studies and works should be performed to take security precautions one step ahead from malicious methods and techniques against the security.

Although there are many different, advanced security applications and systems, the “human factor” is still a critical and important factor in providing a complete security for almost all fields in the modern life. It is important that the human factor is the weakest part of even more advanced security systems and it seems that this situation will not be changed in the near future. Because of this, people must be trained about current security approaches, methods and techniques that can be used to ensure information security. Moreover they also must be warned against potential “social engineering” methods and techniques that can be implemented to benefit from disadvantages of the human factor. This can be done by doing the following tasks:

- Arranging educational seminars or meetings about information security,
- Attending comprehensive conferences and symposiums about information security,
- Following the latest developments and improvements about security approaches, methods and techniques,
- Following the latest developments and improvements about attacking and “security breaking” methods and techniques.
- Being aware of social engineering methods.

“Getting access to source code...was kind of like the secret ingredient. I wanted to know what the secret was...”

Kevin David MITNICK

6 REFERENCES

- [1] R. Kurtus: What is Security?, Ron Kurtus' School for Champions, (2002). [Online] Retrieved April 10, 2010 from: <http://www.school-for-champions.com/security/whatis.htm>
- [2] N. Yalcin, and U. Kose: Sending E-Mail with an Encrypting Algorithm Based on Private-Key Encryption, In Proceedings of the International Conference on Information and Communication Systems 2009, pp. 33-37 (2009).
- [3] D. P. Agrawal, and Q.-A. Zeng: Introduction to Wireless and Mobile Systems, Thomson, (2005).
- [4] J. Kurose, and K. Ross: Computer Networking, Addison Wesley, (2003).
- [5] L. M. Surhone, M. T. Timpledon, and S. F. Marquesen: Secure Communication, Betascript Publishing, (2010).
- [6] Wikipedia – The Free Encyclopedia: Secure Communication, (2010). [Online] Retrieved April 13, 2010 from: http://en.wikipedia.org/wiki/Secure_communication
- [7] S. Sagiroglu, and M. Tunckanat: A Secure Internet Communication Tool, Turkish Journal of Telecommunications, Vol. 1, No. 1, pp. 1-10 (2002).
- [8] Wikipedia – The Free Encyclopedia: Firewall (computing), (2010). [Online] Retrieved April 14, 2010 from: [http://en.wikipedia.org/wiki/Firewall_\(computing\)](http://en.wikipedia.org/wiki/Firewall_(computing))
- [9] R. J. Spillman: Classical and Contemporary Cryptology, Prentice Hall, pp. 1-6, 132, 137 (2005).
- [10] R. A. Mollin: RSA and Public Key Cryptography, Chapman and Hall/CRC, pp. 1-25, 53 (2003).
- [11] S. Sagiroglu, and M. Alkan: Electronic Signature in All Respects: E-Signature, Grafiker Publishing, pp. 2, 8-9, 24, 31 (2005).
- [12] W. Trappe, and L. C. Washington: Introduction to Cryptography with Coding Theory, Prentice Hall, pp. 4-6 (2002).
- [13] M. D. Abrahams, S. Jajoida, and H. J. Podell: Information Security: An Integrated Collection of Essays, Institute of Electrical and Electronics Engineering, pp. 15, 350-384 (1995).
- [14] D. R. Stinson: Cryptography Theory and Practice, Chapman and Hall/CRC, pp. 114, 162 (1995).
- [15] C. Cimen, S. Akleylek, and E. Akyildiz: Mathematics of the Codes: Cryptography, Middle East Technical University – Center of Society and Science, (2007).
- [16] S. Singh: The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor, (2000).
- [17] K. Schmeih: Cryptography and Public Key Infrastructure on the Internet, Heidelberg, pp. 42 (2003).
- [18] M. T. Sakalli, E. Bulus, A. Sahin, and F. Buyuksaracoglu: Design Techniques and Power Analysis in Flow Codes, In Proceedings of 9th Annual Academic Informatics Conference, (2007).
- [19] S. Andac, E. Bulus, and M. T. Sakalli: Analyzing Strength of Modern Block Encryption Algorithms, In Proceedings of 2nd Young Researchers Congress of Engineering Sciences, pp. 87 (2005).