GU J Sci, Part A, 5(3): 89-100 (2018)

Gazi University

Journal of Science

PART A: ENGINEERING AND INNOVATION

http://dergipark.gov.tr/gujsa

Implementation of Message Encryption Algorithms in Real Time Closed Network Systems

Ataç SANCAR[1,*], Bünyamin CİYLAN[1]

[1]*Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi, Ankara, Türkiye*

Article Info

Received: 28/05/2018
Accepted: 27/09/2018

Keywords

Encryption,
Decryption,
Security,
Embedded system

Abstract

In the case of messaging systems used in closed network systems in military and other systems, encryption processes are generally not needed.Since these systems are usually real-time systems, interpretation of messages (encryption of the message and decriyption of the message) will adversely affect time synchronization and traceability. However, this situation also causes significant security vulnerabilities in such critical systems.

In this study, different encryption methods were applied to the messaging structures used in military real - time closed network systems.The effects of these applied cipher methods on performance were made by creating three different test environments and the results obtained are presented in detail.

1. INTRODUCTION

In today's technology; the delivery times of the projects have been shortened due to the tough competition conditions that have been increasing rapidly in the projects, the high quality expectations of the customers, the reduction of the cost items and quick / efficient results.For this reason, the system / software developed has begun to come into question with certain error conditions and security vulnerabilities, with the source and the cause changing [1,2]. Nowadays, the widespread use of computer technology in every area and especially the development of computer networks facilitates information access. In addition to being easy to access information, there is also a need to ensure information security. Therefore, protecting and safely protecting information from threats or attacks has become a major problem.With the ever-widespread use of information systems, security weaknesses or exploits in information technology have also begun to increase.

Many products and projects related to security issues are being developed in order to ensure confidentiality, integrity and continuity in information technologies. This clearly demonstrates the importance of information security. Information security is the securing of confidentiality, integrity, availability and availability of information by protecting information from unauthorized access. Information security; technology (software and hardware), human, process, methodology and methodology, and it seems to be very important for the world of information [3].

In addition, information security is defined as "to protect information from damage as an asset, to prevent the right technology from being used by the unwanted person in any environment, using the right purpose and in the correct way". At this point, attention should be paid to the issue of cryptography. Cryptography is a general name given to the subject of encryption, which is used to convert a message or information temporarily to an unreadable form and to convert the information back to readable on the other side. Another definition of cryptography is the development of mathematical methods for communicating information in an unsecured environment without infiltration [4].

*Corresponding author, e-mail: sancaratac@gmail.com

In this paper, we present the results of applying different encryption methods to the military real-time closed network system, how the applied encrption methods have an effect on the interpretation (encryption and decryption) of the message and how the encryption of the messages in the systems does not affect the operation of the system. In the second part of the study, cryptology algorithms and their uses; the details of the working environment in the third part, the comparison process in the measurement results in fourth part and finally the results and recommendations of the study in fifth part.

2. GENERAL CRYPTOLOGY APPROACHES

Cryptography is known aas of encyription science. With the rapid development of technology, military, electronic, banking systems and many other places have become the fields of use of cryptography. One of the most important requirements in today's systems is the seamless transfer of information and confidentiality. Various encryption, keying and decryption algorithms are developed using cryptography, so that data can be transmitted securely and received from the other side. The most common cryptography algorithms are encryption algorithms [5].

Cryptography has introduced two different algorithms depending on key usage characteristics.

- Symmetric encryption algorithms
- Asymmetric encryption algorithms

In this study, symmetric and asymmetric cryptographic approaches will be utilized with an additional cryptographic message which is named as of authentication code function. These results will yield comparative performance results for selected algorithms.

2.1. Symetric Encryption Algorithms

In symmetric encryption, the message to be transmitted by encryption is subjected to a series of processes by the encryption algorithm. During this process, the message is encrypted with the same encryption key also found on the receiver side. When the recipient returns the encrypted message to the original, it decrypts the message with the encryption key that it has. That is, the same keys are used in encryption-decryption processes in symmetric key-based encryption algorithms [6,7].

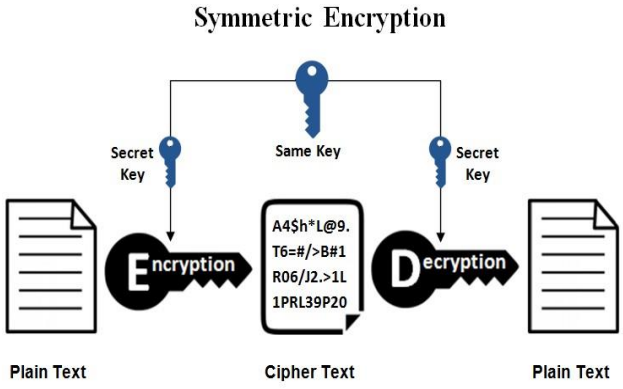

Figure 1. *Symetric encryption model (For more details, the reader is referred to [8, Fig. 1].)*

There are too many symmetric encryption algorithms. The main symmetric encryption algorithms are:

- AES (Advanced Encryption Standard)
- DES(Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- RC2 (Rivest Cipher)

2.2. Asymetric Encryption Algorithms

To solve the key distribution problem in the symmetric cryptography technique, a cryptosystem based on the principle of using the keys separately for each of the encryption and decryption processes has been developed. In this system, encryption is done by public key known by everyone. Since encryption and decryption are performed with algorithms that are not symmetrical to each other, they are also known as asymmetric encryption systems. AES is is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs and others involve shuffling bits around. AES processes have four operations which are SubBytes, ShiftRows, MixColumns, XorRoundKey [9-11].

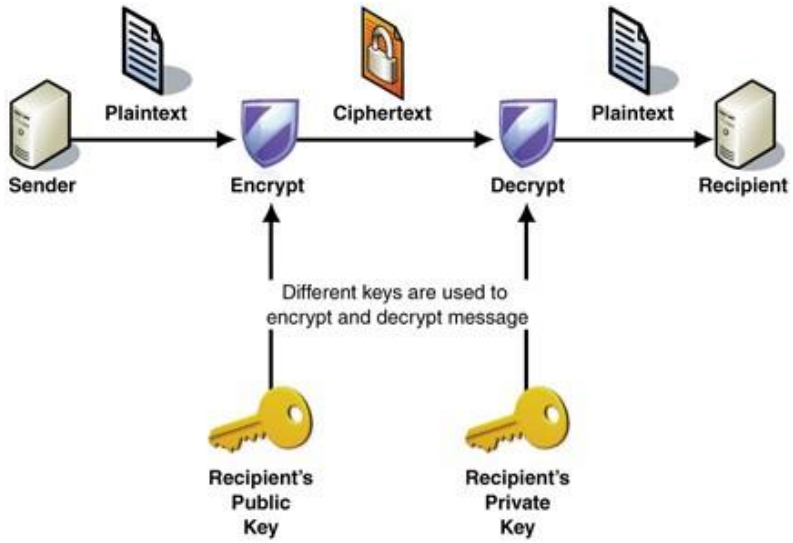

Figure 2. *Asymetric encryption model (For more details, the reader is referred to [12, Fig. 1].)*

There are too many asymmetric encryption algorithms. The main asymmetric encryption algorithms are:

- RSA (Rivest-Shamir-Adleman)
- El Gamal
- PGP (Pretty Good Privacy)
- Diffie-Hellman
- DSA (Digital Signature Algorithm)

2.3. Message Authention Code Algorithms

The cryptographic message authention code(MAC) function provides various security features. It converts the data into a bit sequence and a summary value in a specific length. The data to be summarized is called the summarized value, the summarized value is the message summarized or briefly summarized [13].

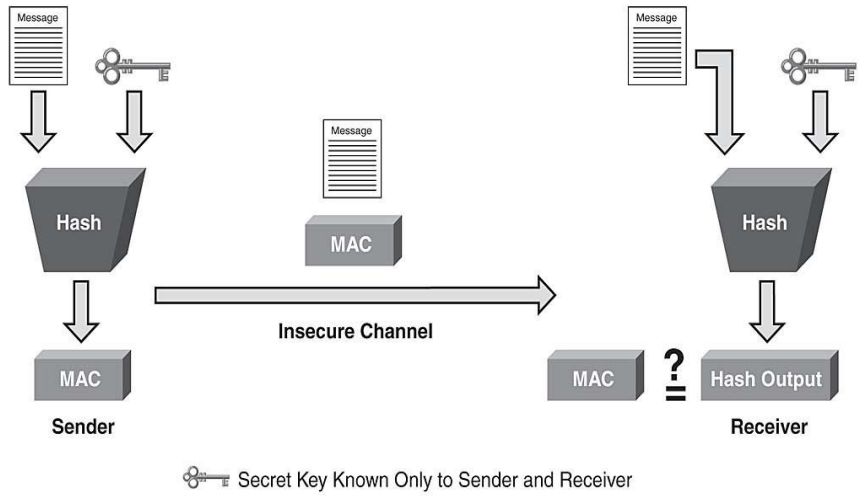

Figure 3*. Messsage Authentication Code Model (For more details, the reader is referred to [14, Fig.2.1].)*

Cryptographic MAC functions are widely used in digital signature with information security issues, message authentication code and other verification methods.[15,16] There are too many MAC functions algorithms. The main MAC functions algorithms are:

- MD5 (Message Digest 5)
- SHA-1 (Secure Hashing Algorithm)
- HAVAL

Different testing environments have been developed for the detailed examination of the performance of these algorithms. Test environments are treated in three different ways.

3. CREATION OF TEST ENVIROMENTS

In this article, various cryptographic operations (AES, RSA, MD5) on the messaging protocol including real time closed network system communication are applied on different test equipment. The results of the effects of different equipment and encryption methods on the tests are explained in detail in Chapter 4.

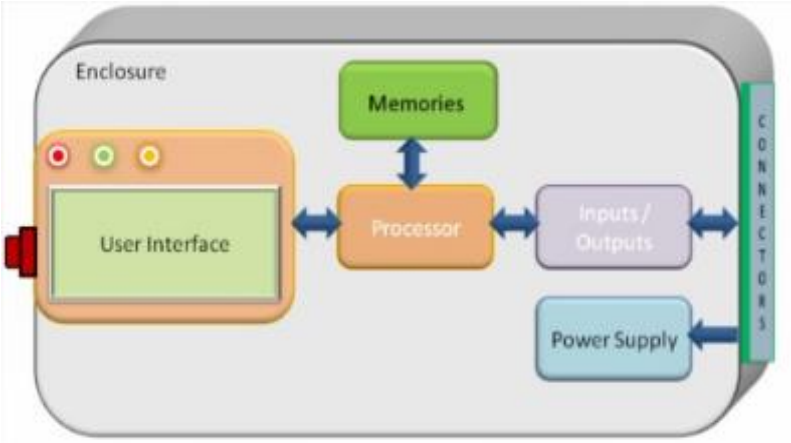

Figure 4. *Test Equipment Structure (For more details, the reader is referred to [17, Fig. 1].)*

The properties of the test equipment used are listed below:

Test Equipment 1:

Operating System : macs sierra
Ram: 8gb ddr3
Processor: core i5 2.3 ghz

Test Equipment 2:

Operating System: Windows 7
Ram: 8 gb
Processor: core i5 3.30 ghz

Test Equipment 3:

Operating System: vxWorks 6.9
Ram : 8GB DDR3 SDRAM with ECC per processor
Processor: VPX6-463(VPX QUAD-CORE) Intel-i7(Core™ i7-4700EQ fourth generation processors running at up to 2.4GHz)

Four different test types were defined according to the three different test environments created and the results of these test types are shown in detail.

4. PERFORMANCE CRITERIA AND TEST RESULTS

In the study, AES, RSA and MD5 encryption methods were applied on three different test hardware for the communication protocol used in military real-time closed network systems and the "time spent on the encryption and decryption of the message" was taken as the primary performance criterion. Also, the tests were repeated for different sizes of messages, and the results were presented comparatively.

In addition, comparisons have been made with respect to power consumption via BSP (Board Support Package), but it has been observed that the results obtained here do not produce a consistent result. As a result of the necessary examinations, the test results were found to be optimal in 30 and 100 byte tests. Therefore, these two sets are exemplified in our article. When the data range is increased, it is observed that the changes can be ignored and also the results can be very different when the data range is reduced.

4.1. Results for Test Equipment 1

The details of the encryption-decryption times that Test Equipment 1 performs for 30 bytes of data are specified in Table 1.

Table 1. *Test equipment 1 performance results for 30 bytes data*

Encryption Method	Data Size	Encryption-Decryption Time (s)		
		Min Time	Max Time	Avarage Time
RSA	30byte	0,0063577	0,56408543	0,01050528
AES	30byte	0,0003261	0,27294197	0,00310216
MD5	30byte	0,0000937	0,03290743	0,000569543

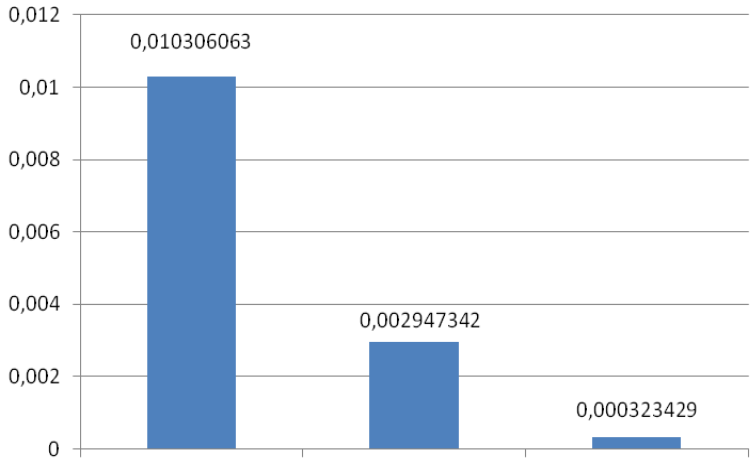

Figure 5. *Results for Test Equipment 1 (30byte)*

When the results are analyzed for 30 bytes of data, it is seen that the encryption and decryption processes have increased for MD5, AES and RSA algorithms. MD5 avarage time 0.1sn, AES avarage time 0.003 and MD5 avarage time 0.0003. all the following figures will be listed in this way.

The details of the encryption-decryption times that Test Equipment 1 performs for 100 bytes of data are specified in Table 2.

Table 2. *Test equipment 1 performance results for 100 bytes data*

Encryption Method	Data Size	Encryption-Decryption Time (s)		
		Min Time	Max Time	Avarage Time
RSA	100byte	0,004695	0,561231	0,010306
AES	100byte	0,004695	0,275243	0,002947
MD5	100byte	0,000088	0,015481	0,0003234

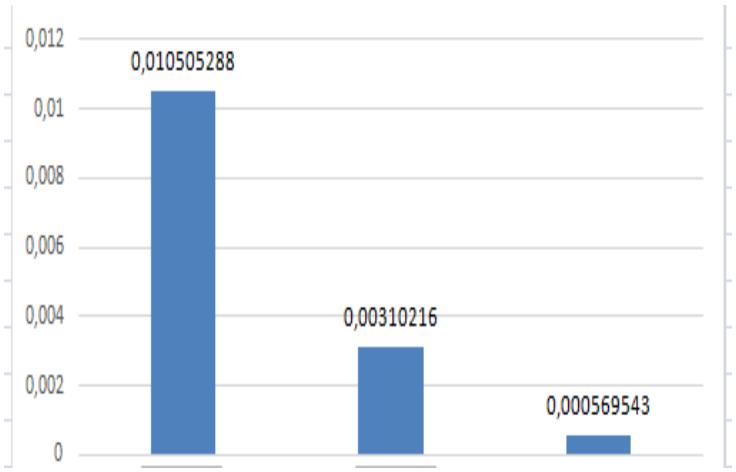

Figure 6. *Results for Test Equipment 1 (100byte)*

When the results are analyzed for 100 bytes of data, it is seen that the encryption and decryption processes have increased for MD5, AES and RSA algorithms.

4.2. Results for Test Equipment 2

The details of the encryption-decryption times that Test Equipment 2 performs for 30 bytes of data are specified in Table 3.

Table 3. *Test equipment 2 performance results for 30 bytes data*

Encryption Method	Data Size	Encryption-Decryption Time (s)		
		Min Time	Max Time	Avarage Time
RSA	30byte	0,0017552	0,41244197	0,006289181
AES	30byte	0,0001343	0,19002568	0,002132414
MD5	30byte	0,0000590	0,01719578	0,000275551

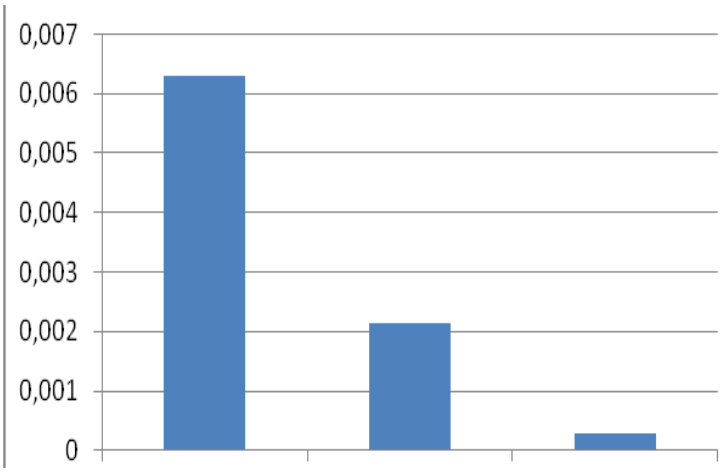

Figure 7. *Results for Test Equipment 2 (30byte)*

When the results are analyzed for 30 bytes of data, it is seen that the encryption and decryption processes have increased for MD5, AES and RSA algorithms.

The details of the encryption-decryption times that TestEquipment 2 performs for 100 bytes of data arespecified in Table 4.

Table 4. *Test equipment 2 performance results for 100 bytes data*

Encryption Method	Data Size	Encryption-Decryption Time (s)		
		Min Time	Max Time	Avarage Time
RSA	100byte	0,001928	0,40925951	0,006301198
AES	100byte	0,000064	0,18842932	0,001978986
MD5	100byte	0,000066	0,01585848	0,000272939

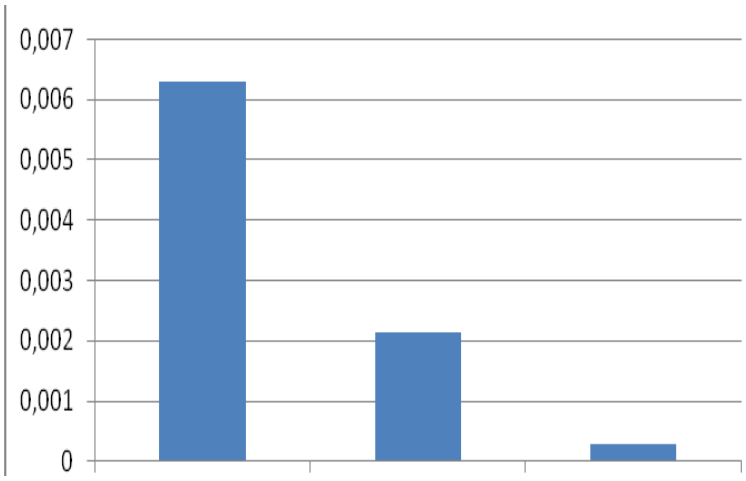

Figure 8. *Results for Test Equipment 3 (100byte)*

When the results are analyzed for 100 bytes of data, it is seen that the encryption and decryption processes haveincreased for MD5, AES and RSA algorithms.

4.3. Resutlts for Test Equipment 3

The details of the encryption-decryption times that Test Equipment 3 performs for 30 bytes of data are specified in Table 5.

Table 5. *Test equipment 3 performance results for 30 bytes data*

Encryption Method	Data Size	Encryption-Decryption Time (s)		
		Min Time	Max Time	Avarage Time
RSA	30byte	0,0003645	0,0004648	0,0003865
AES	30byte	0,0000264	0,0000285	0,0000273
MD5	30byte	0,0000189	0,0000211	0,0000198

When the results are analyzed for 30 bytes of data, it is seen that the encryption and decryption processes have increased for MD5, AES and RSA algorithms.

The details of the encryption-decryption times that Test Equipment 3 performs for 100 bytes of data are specified in Table 6.

Table 6. *Test equipment 3 performance results for 100 bytes data*

Encryption Method	Data Size	Şifreleme+Deşifreleme Süresi (s)		
		Min Time	Max Time	Avarage Time
RSA	100byte	0,0003945	0,0004743	0,0004154
AES	100byte	0,0000284	0,0000357	0,0000295
MD5	100byte	0,0000186	0,0000217	0,0000204

When the results are analyzed for 100 bytes of data, it is seen that the encryption and decryption processes have increased for MD5, AES and RSA algorithms.

4.4. Resutlts for Test Equipment 3

The details of the encryption-decryption times that Test Equipment 3 performs for 30 bytes of data are specified in Table 7 and Table 8.

Table 7. *Test equipment 3 performance results for 30 bytes data*

30byte	Avg Time	Max Time	Min Time
CBC	0,00010736	0,000110407	0,000107695
CTR	2,9951E-05	3,01783E-05	0,00003016
ECB	2,7811E-05	0,00002808	2,77317E-05

Table 8. *Test equipment 1 performance results for 100 bytes*

100byte	Avg Time	Max Time	Min Time
CBC	0,000108	0,0001109333	0,0001071383
CTR	0,0000299	0,000030375	0,0000296666
ECB	0,0000279	0,0000280466	0,000027888

4.5. General Performace Results

The results for different encryption algorithms for data of different sizes on the test equipment are as follows.

Table 9. *RSA algorithm times for with a length of 30 bytes messages*

RSA 30 byte (s)		
Test Equipment 1	avg time	0,139663
Test Equipment 2	avg time	0,006289

Table 10. *RSA algorithm times for with a length of 100 bytes messages*

RSA 100 byte (s)		
Test Equipment 1	avg time	0,010306
Test Equipment 2	avg time	0,006301

Table 11. *AES algorithm times for with a length of 30 bytes messages*

AES (ECB) 30 byte (s)		
Test Equipment 1	avg time	0,139663
Test Equipment 2	avg time	0,006289
Test Equipment 3	avg time	0,000107

Table 12. *AES algorithm times for with a length of 100 bytes messages*

AES (ECB) 100 byte (s)		
Test Equipment 1	avg time	0,010306
Test Equipment 2	avg time	0,006301
Test Equipment 3	avg time	0,000108

Table 13. *MD5 algorithm times for with a length of 30 bytes messages*

MD5 30 byte (s)		
Test Equipment 1	avg time	0,00057
Test Equipment 2	avg time	0,000276

Table 14*. MD5 algorithm times for with a length of 100 bytes messages*

MD5 100 byte (s)		
Test Equipment 1	avg time	0,000323
Test Equipment 2	avg time	0,000273

We compare the durations of the 3 different encryption algorithms for 3 different test environments to examine the results, while the durations according to the test environment and the selected algorithms are highly variable, it is also seen that these durations are not affected much by the message length.

5. RESULTS AND DISCUSSIONS

We compare the durations of the 3 different encryption algorithms for 3 different test environments to examine the results, while the durations according to the test environment and the selected algorithms are highly variable, it is also seen that these durations are not affected much by the message length.

In this work, it is revealed how much delay is generated in the system by the used cryptography algorithms. Before the delays were compared, the test environments were considered as two different platforms. While the first and second tests are based on user interface platforms, the third and fourth tests are based on the real time application platforms which are running on the kernel module.

Both real-time and user interface platforms show performance differences for cryptography algorithms. For cryptographic algorithms Performance order is MD5, AES, RSA. For security purposes, MD5 is rated weaker than AES and RSA.

Both real-time and user interface platforms, increase of message size does not effect performance exactly. There is almost no differences between minumum and maximum performace time for reel-time systems. This situation is exactly the opposite for user interface platforms. cryptography algorithms performance for User interface platforms is at least 15 times higher than reel-time platforms.

As a result, we have examined which algorithm should be chosen for the domain and the usage requirement, and also the results are detailed.

CONFLICT OF INTEREST

No conflict of interest was declared by the authors

REFERENCES

[1] Blum, M., Goldwasser, S., "An efficient probabilistic public-key encryption scheme which hides all partial information*," Advances in Cryptology — Crypto 84 Proceedings*, *Lecture Notes in Computer Science*, 196, (1985).

[2] Avcioglu, A., Demirer, M., "Implementation of system testing automatization on computer aided systems for hardware and software", (2015).

[3] Baykara, M., Daş, R., ve Karadoğan, İ., "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", *In 1st International Symposium on Digital Forensics and Security*, 231-239, (2013).

[4] Topaloğlu, N., Calp, M. H., Turk, B., "Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi", *Bilişim Teknolojileri Dergisi*, 9(3), (2016).

[5] İnternet: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri, Ocak 2018.

[6] Yerlikaya T., Buluş E., Arda D., "Asimetrik Kripto Sistemler Ve Uygulamaları", *II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi MBGAK'2005*, İstanbul (2005).

[7] Adams, C., "Constructing symmetric ciphers using the CAST design procedure" *DDesigns Codes and Cryptography*, 12, 71-104, (1997).

[8] İnternet: https://www.ssl2buy.com/wiki/symmetric-vs- asymmetric-encryption-what-are-differences

[9] Yerlikaya, T., Buluş, E., Buluş, N., "Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri", http://ab.org.tr/ab06/bildiri/102.pdf, Ocak 2018.

[10] Yılmaz, M., Ballı, S., "Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(2), 18-28, (2016).

[11] Naor, M., Yung, M., "Public-key cryptosystems provably secure against chosen ciphertext attacks," *Proceedings of the Twenty Second Annual Symposium on the Theory of Computing*, ACM, (1990).

[12] İnternet: https://www.packtpub.com/mapt/book/virtualization_and_cloud/9781782170983/4/ch04lvl1sec33/asymmetric-encryption

[13] İnternet: http://anibal.gyte.edu.tr/hebe/AblDrive/59669005/w/Storage/104_2011_1_470_59669005/Downloads/bl470-b1-4.pdf, Ocak 2018, Online.
[14] İnternet: https://www.networkworld.com/article/2268575/lan-wan/chapter-2--ssl-vpn-technology.html
[15] Bellare, M., Kilian J., Rogaway, P., "The security of cipher block chaining." *Advances in Cryptology — Crypto 94 Proceedings, Lecture Notes in Computer Science*, 839, (1994).
[16] Rivest, R., "The MD5 message-digest algorithm," *IETF Network Working Group, RFC*, 1321, (1992).
[17] İnternet: http://embien.com/blog/embedded-system-design-architecture/