Designing a New Data Encryption Algorithm Using a Genetic Code Method

Mustafa Zengin, Zafer Albayrak

Faculty of Engineering, Karabuk University, Computer Engineering Department,
Baliklar Kayasi Mevkii 78050 Karabuk, Turkey,
mustafazengin@ogrenci.karabuk.edu.tr; zalbayrak@karabuk.edu.tr

Abstract: Today, the widespread use of information and communication tools along with the developing technology has facilitated access to information. These developments have revealed the importance of data security. Many encryption algorithms have been developed to ensure secure data transfer. In this article, we have developed a new Genetic Encryption Algorithm (GEA) inspired by the DNA structure. The GEA is compared to a DES (Standard Encryption Algorithm), an AES (Advanced Encryption Algorithm) and a RSA encryption algorithm. A short evaluation is made, presenting the results, along with tables and graphs.

Keywords: Cryptology; Genetics; Encryption; Algorithm; Performance

1 Introduction

The widespread use of computer technology has increased the importance of data security. With the effect of the Covid-19 epidemic, the use of internet and mobile devices has increased dramatically, especially studies in areas including, e-commerce, banking, finance, security and education are being carried out using the internet. A survey conducted during the Covid-19 progress, exploring the time that people spend on the Internet found the world average is 6 hours and 45 minutes. In a world where access to information is so easy, it has become an essential need to ensure data security. The secure transfer of data against attacks or threats, has become an important topic. The thought that data, that is needed to be kept confidential and correct, in the communications between computers, can be intercepted by unauthorized persons, is a big problem. The encryption of data is one of the simplest methods to ensure secure data exchange between computers. There are many encryption methods developed to ensure data security and protection of data [1]. These methods are explained in the subject of Cryptography. Cryptography is the process of making a message or data temporarily unreadable by passing it through various mathematical operations and converting this message to a normal readable state, upon reaching the desired target.

The cryptographic algorithms used today, are examined in two parts, symmetrically or asymmetrically, depending on the key structure [2]. In symmetric encryption algorithms, a single secret key is used for encryption and resolution of data. Using a single key while encrypting and resolving data creates a security problem. Because the key used in encryption is transmitted securely to the recipient and is used to resolve the same message, reveals the importance of key security. Symmetric encryption algorithms are faster and more efficient than asymmetric encryption algorithms [3]. However, they create security weaknesses because a single common key is used. DES, 3DES, AES are shown as the most widely used symmetric encryption algorithms [4]. The basic feature of symmetric encryption algorithms performs encryption by dividing the desired message into blocks and converting them into bits. For example, when the working principle of the DES algorithm is examined, it first divides the message into 64-bit blocks and then a 64-bit block back into 32-bit right and left bits. A 32- bit encrypted result is obtained by passing the 32-bit right bit through the f function with a 48-bit key bit. Then, the 32-bit left bit is passed through the f function with the same 48-bit key bit, and a 32-bit encrypted result is obtained. This f function produces a 32-bit result, using 32-bit data and a 48-bit key. This is the process of performing the action. This operation allows multiple results to be produced for the same bit. By extending with a 32-bit key, 48-bit data is provided. It splits the 48-bit data into groups, dividing the data into 8 blocks. Each block consists of a 6-bit segment. Each 6-bit piece has been reduced to 4 bits militarily this time. It consists of 8 blocks of 4 bits, that is, a total of 32 bits of data. A 64-bit block is obtained from 32-bit right and left messages that are encrypted [5]. With this method, all blocks are encrypted and form the working principle of the DES algorithm. Two public keys are used in asymmetric encryption algorithms. Using two different keys for encryption and resolution of data provides high security. However, compared to symmetric encryption algorithms, it is very slow and processing speed takes longer. The most widely used asymmetric encryption algorithm is the RSA algorithm. The main feature of asymmetric encryption algorithms is that they are easy to do, difficult to undo and time consuming because they operate with large prime numbers. For example, multiplying two numbers is easy, but finding their factors is difficult or takes time. Squaring a number is easy, but finding its square root is difficult. For this reason, asymmetric encryption algorithms are the most reliable encryption algorithms. The performance and success of cryptographic algorithms are determined according to the key size used in encryption, processing speed and the amount of memory used [6]. The “brute force” breaking times of the algorithms vary according to the key size used. The sample DES algorithm has a key structure of 56 bits. The brute force password cracking time is 2^{56} seconds. [7].

The aim of this study is to develop algorithms that perform better than the encryption algorithms used today in order to provide secure data transfer between large computer networks. GEA (Genetic Encryption Algorithm), which was developed as a result of the studies, has a symmetric encryption algorithm feature, so its processing speed is faster than asymmetric encryption algorithms [8].

Since the key size used is 128 bits, it is harder to crack a brute force password, it is more secure 2^{128} seconds. Because the brute force break time is The GEA encryption algorithm is faster than the DES, 3DES and RSA encryption algorithms, and the breaking time is more difficult than the DES and 3DES algorithms [9].

In the continuation of the study, in Section 2, cryptology and encryption algorithms, in Section 3, the studies in the literature, in Section 4, the structure of the genetic encryption algorithm developed inspired by the structure of DNA is explained. In Section 5, performance analysis of encryption algorithms is made and explained. The results of the study were evaluated in the last section.

2 Cryptology and Encryption Algorithms

Cryptology is the process of encrypting data and analyzing encrypted data. Encryption is the method and methods for encrypting data by performing the mathematical operations required to encrypt the data. Cryptanalysis is the science that covers the analysis of encrypted data. The purpose of encryption science is to provide data security to prevent data from falling into the hands of unwanted people. The purpose of password analysis is to analyze the data and convert existing passwords to their original state. Encryption, one of the basic concepts of cryptology, is the process of making plain text content unreadable. The main thing in encryption is to prevent data from being read by unauthorized people. The process of deciphering the password is the reverse of encryption and makes encrypted data meaningful, readable and understandable [10] [11].

When encryption methods are examined, it is seen that various techniques based on mathematical operations are used. While simple encryption techniques were used to provide data security in line with the opportunities provided by technological developments in history, modern encryption methods are used today. According to the characteristics of the keys used in modern encryption methods, they are divided into two as symmetric encryption algorithms and asymmetric encryption algorithms [12] [3].

2.1 Symmetric Encryption Algorithms

When we look at the structure and principles of symmetric encryption algorithms, a single key is used to encrypt data and recycle encrypted data and make it meaningfully readable. This key used is private.

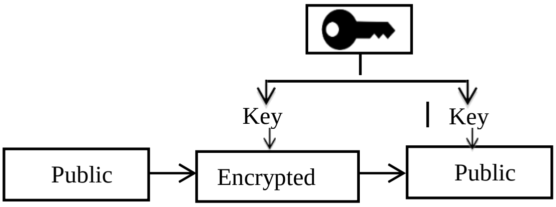

Figure 1
Symmetric Encryption Algorithms

A common key is used between people who provide encryption of data and analyze encrypted data. Therefore, in symmetric encryption algorithms, it is very important to securely transmit the key to the other party [8].

2.2 DES Encryption Algorithm

The standard data encryption algorithm uses the same key to encrypt data and recycle encrypted data. Therefore, the security of the key is very important. The working principle of the DES algorithm is shown in Figure 2.

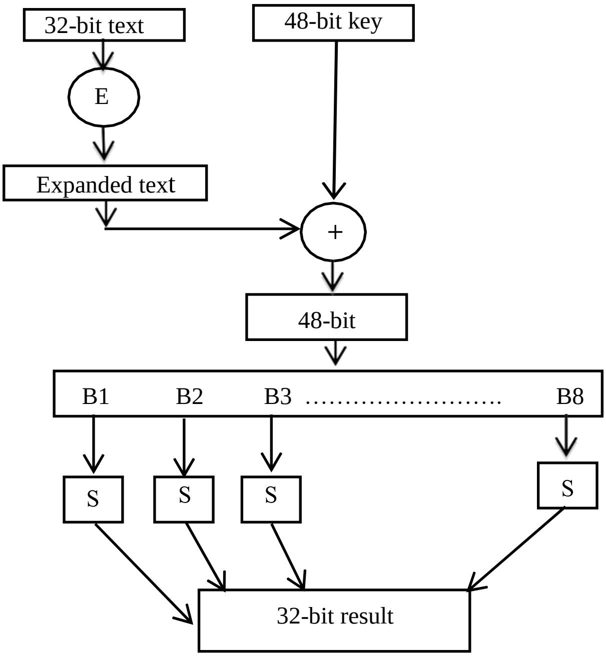

Figure 2
DES Encryption Algorithm

When the DES algorithm encrypts the data, it is processed in 64-bit blocks and the data is encrypted according to the symmetric encryption method with the help of a 56-bit key. Thus, 64-bit encrypted data is obtained [13]. The DES (Data Encryption Standard) algorithm is split into 64-bit data blocks encrypted with the same 56-bit key to restore data to 56-bit blocks. Thus, readable, meaningful data is obtained. As a result, data that seems meaningless by encrypting the data becomes meaningfully readable [4] [14].

2.3 AES Encryption Algorithm

The advanced data encryption algorithm uses the same key as the DES algorithm to encrypt and recycle encrypted data. For this reason, the security of the key to be used in encryption is very important. The working principle of the AES algorithm is shown in Figure 3.

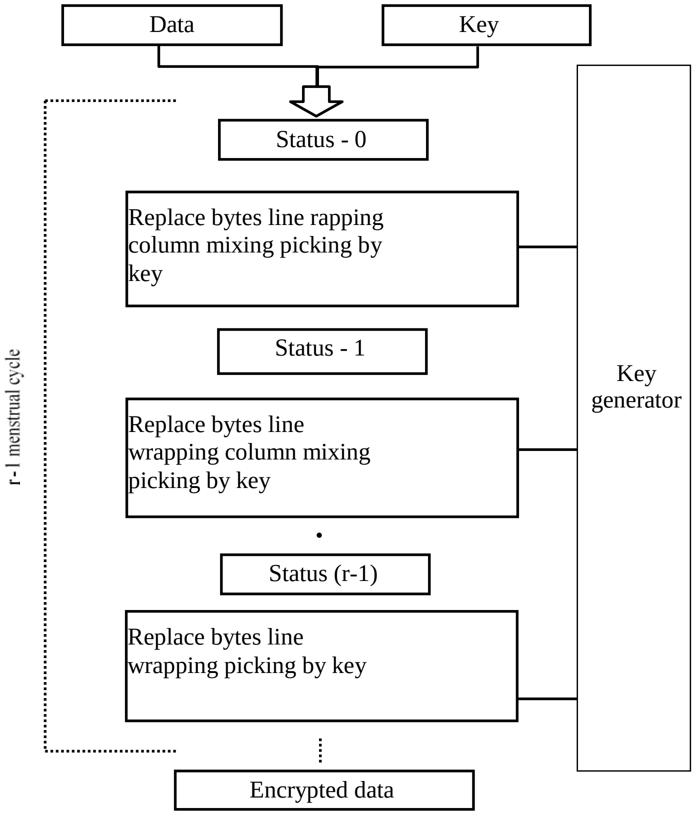
Data
Key
Status - 0
Replace bytes line rapping column mixing picking by key
Status - 1
Replace bytes line wrapping column mixing picking by key
Status (r-1)
Replace bytes line wrapping picking by key
Encrypted data
Key generator
r-1 menstrual cycle

Figure 3
AES Encryption Algorithm

The AES symmetric encryption algorithm consists of a return transformation block and a key generation block. Because the Advanced Encryption Standard is a repetitive algorithm, if 128-bit keys are used for encryption or decryption, it results in 10 repeats, 12 repeats in 192-bit keys, and 14 repeats in 256-bit keys [15]. The flexible nature of the AES encryption algorithm does not adversely affect processing speed and performance, even when using a different key [16].

2.4 Asymmetric Encryption Algorithms

Two different keys are used in these encryption algorithms. A different key is used when encrypting data and deciphering encrypted data. The working principle of asymmetric encryption algorithms is shown in Figure 4. Two different keys are used in asymmetric encryption algorithms. It is not hidden like the key in symmetric encryption algorithms. In addition, a single secret key is used in symmetric encryption algorithms, while two keys are used in asymmetric encryption algorithms. One of the keys is the public key. The other key is hidden. The public key is used to encrypt the data, while the secret key is used to analyze the encrypted data [17].

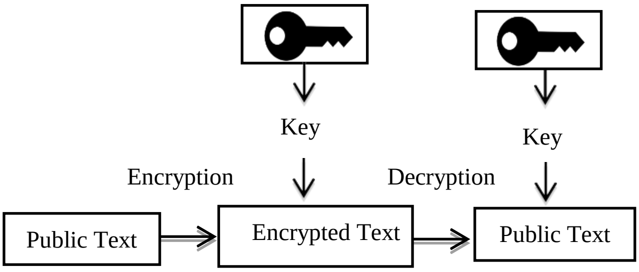

Figure 4
Asymmetric Encryption Algorithms

2.5 RSA Encryption Algorithms

The key used to encrypt data in the RSA encryption algorithm is public. The same key is not used to decrypt encrypted data. The working principle of the RSA encryption algorithm is shown in Figure 5. The security of the RSA algorithm is based on the algorithmic difficulties of factoring the numbers. This asymmetric encryption algorithm is used as a public key, along with another value selected by the product of two large prime numbers. Prime multipliers are stored. The data can be encrypted using the public key, but if the public key is large enough, the encrypted message can only be deciphered if the prime number multiplier is known [4].

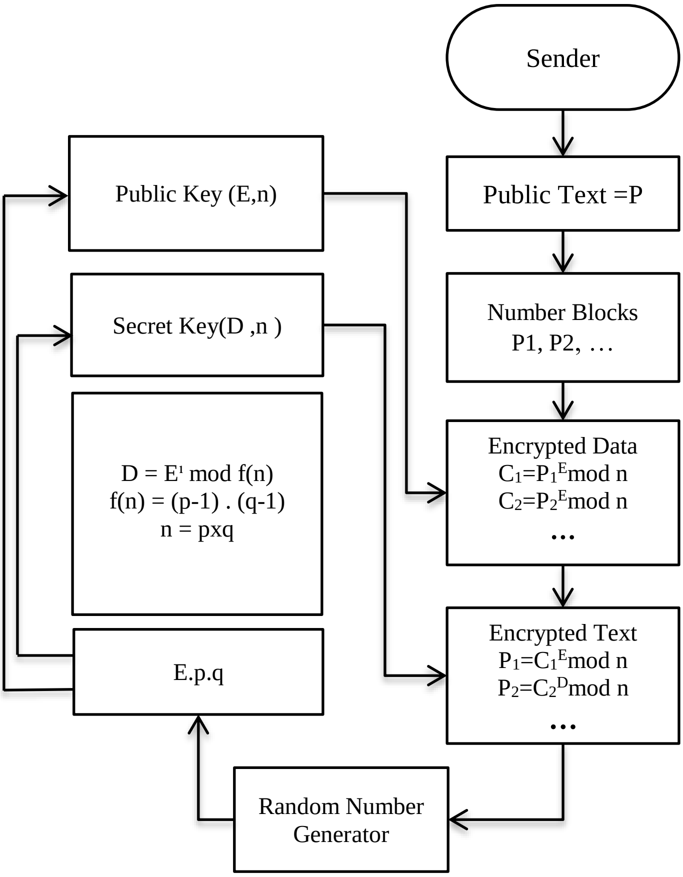

Figure 5
RSA Encryption Algorithm

3 Related Literature Studies

As a literature research for performance analysis of encryption algorithms many articles have reviewed and detailed. In [18], a study was conducted on cryptography algorithms to perform performance and security analysis of simple encryption algorithms. While encrypting on different image files, data distribution, pixel count comparison, encryption time and encryption quality analyzes were performed. They concluded that S-AES and LBlock algorithms provide fast and sufficient security using less resource. In [19], information was given about the methods used in classical encryption methods and methods used in modern encryption. In the encryptions made with the help of the key used in modern encryption methods, the working time of the algorithms, the processor and memory usage features of the algorithms were examined. This work was done only on pixels and images.

In [20], parameters such as the accuracy, efficiency and key exchange of a preferred algorithm for BLOWFISH, IDEA, CAST-128, RC6, DES, 3DES, AES and RSA encryption were analyzed. It is emphasized that it can be provided by applying to multiple algorithms to create efficient encryption systems.

Thakur et al, Among the symmetric encryption algorithms, the most commonly used DES, AES and Blowfish symmetric encryption algorithms were examined and performance analyzes were compared in terms of speed, block size and key size. As a result of the java simulation program used, Blowfish showed that the encryption algorithm has better performance. [21]

In [22], DES, AES, 3DES, RC2, Blowfish, IDEA, Twofish, TEA, symmetric encryption algorithms and RSA asymmetric encryption algorithm were used to ensure data security. While these encryption algorithms encrypt the data, time, memory and processor usage performance criteria are compared. As a result of the studies, the DES algorithm performed better than the AES algorithm in small data sizes. The DES algorithm did not perform well on large data sizes compared to the AES algorithm.

In [23] symmetric and asymmetric encryption algorithms are examined. Key sizes were analyzed during encryption or decryption. They examined the factors that affect the performance of data encryption algorithms.

Matching of organic bases in Deoxyribbo Nucleic Acid (DNA) structure was investigated. As a result of this research, the matching of the bases inspired us to develop a symmetric encryption algorithm with 128-bit random key structure [24].

4 Designing a New Data Encryption Algorithm Using Genetic Code Method (GEA)

The DNA structure, in which the biological properties of living things are carried, forms the basis of our algorithm. Structure of DNA (Deoxyribbo Nucleic Acid) There are organic bases such as Adenine "A", Guanine "G", Cytosine "C" and Thymine "T". A different encryption algorithm has been developed based on the relationships of these organic bases with each other [25].

In this study, While ASCII coding of Adenine, Thymine, Guanine and Cytosine bases in the structure of DNA was done, the "Watson Crick's" model was used. This method is linked by hydrogen bonds between Adenine and Thymine, Guanine and Cytosine base in DNA. The reciprocal substitution of these bases introduces complexity in terms of encryption. This complexity constitutes the security of the encryption process. The data to be encrypted and the ASCII values of the keyword to be used were calculated. These ASCII values, which are calculated as a decimal number system, are converted into genetic code. The ASCII value of each character is converted into a quad number system. Numerical values are created. (When we convert the data in the decimal number system to the system of four numbers, the remaining values are 0, 1, 2, and 3.)

The main reason for converting our ASCII values to four number systems is to match four organic bases. This match is shown in Figure 6. The mapping of DNA bases on the left. By assigning a number value to each of the middle DNA bases, which base matches which number matches. The figure on the right shows how DNA bases match the number values we assign.

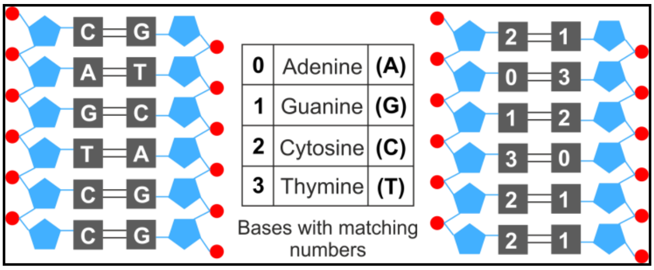

Figure 6
Coding of DNA Organic Bases

In this way, our numbers turn into organic bases that match the corresponding organic bases, as in DNA matching. (There is a match between Adenine and Thymine, Guanine and Cytosine, and vice versa.) This 3 - 0, 2 - 1. Thus, the quad number system creates a new DNA chain. The keyword match used in encryption with this DNA match is aggregated in a quadruple system. A single DNA chain is created. In the quad number system, these newly created numbers are converted to their equivalents in the decimal system. Finally, character values in the ASCII number table in the decimal system are obtained. Although these values seem meaningless and complex, they show encrypted data. By recycling these encrypted ASCII values, the encrypted data is converted to the original state, that is, by reversing these processes to decode the encrypted data [26] [27]. Among the biggest disadvantages of symmetric encryption algorithms is the use of a single key when encrypting and decrypting data, and the small key size. In this study, greater usability of the key size is provided.

5 Performance Analysis of Symmetric and Asymmetric Encryption Algorithms

One of the reliable methods used in performance evaluation of complex encryption algorithms is experimental analysis method [26] [27]. For this reason, performance analyses of symmetric and asymmetric encryption algorithms were done using experimental analysis method. DES, AES and RSA encryption algorithms were compared to see the performance values of the encryption algorithm (GEA) application with the developed genetic code method. The performance of GEA, DES, AES and RSA algorithms of the data to be encrypted was calculated by using experimental measurements in accordance with the processor (CPU) and memory (RAM) usage values during this process (encryption and decryption). In this analysis method, the processing time was evaluated in minutes, the memory megabyte used and the processor % used. This experiment was calculated according to the encryption and decryption of data packets of 58 Bytes, 102 Kilobytes, 1 Megabyte and 5 Megabytes.

5.1 Encryption and Decryption Analysis of 58 Bytes of Data

The process time, processor usage, and memory usage values obtained during the encryption and decryption of data with 58 bytes of character length were examined. Table 1 shows the performance values of DES, AES, GEA and RSA encryption algorithms when 58 bytes of data are encrypted.

Table 1
58 Byte Data Encryption

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	2	30	8
	AES	3	32	8
	RSA	8	29	8
	GEA	2	18	8

When the graphic in Figure 7 is examined, it is seen that the processor values used when encrypting 58 bytes of data are the same.

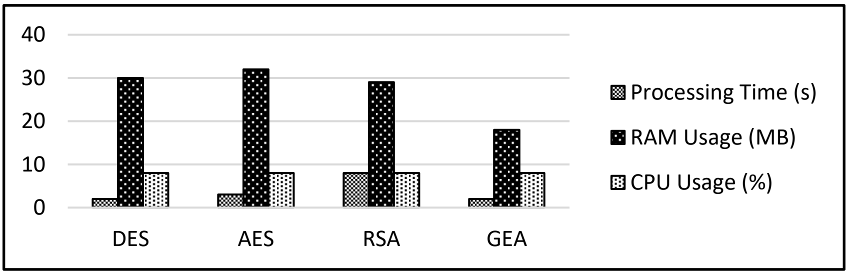

Figure 7
Byte Data Encryption

Although the processing time value of the GEA algorithm is the same as the DES algorithm, memory usage values perform better than other DES, AES and RSA algorithms. The reason for this is the switch structure used and the working principle used. While the GEA uses a 128-bit key structure, the DES algorithm uses a 56-bit key structure. Although this affects the processing speed, it increases the memory usage of the DES algorithm.

Table 2
Decryption of 58 Bytes of Data

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	1	26	8
	AES	1	28	8
	RSA	6	24	8
	GEA	1	14	8

Table 2 shows the performance values of DES, AES, GEA and RSA encryption algorithms for deciphering data of 58 bytes. While analyzing the 58 byte encrypted data in the analysis of the graph in Figure 8, the processing time and processor usage performance of DES, AES and GEA symmetric encryption algorithms are better than RSA, which is the asymmetric encryption algorithm. Symmetric encryption algorithms have the same values.

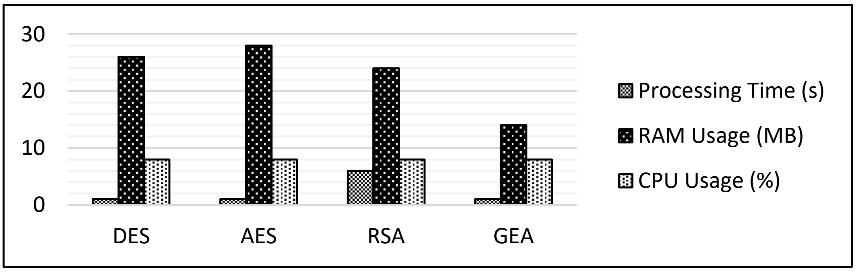

Figure 8
Decryption of 58 Byte Data

In general, the memory usage performance of GEA algorithm is seen to be better than that of DES, AES and RSA algorithms. This is due to the use of 128-bit key and working principle.

5.2 102 Encryption and Decryption Analysis of Kilobyte Data

The values for the processing time, processor usage and memory usage obtained during the encryption and decryption of data with 102 kilobyte character length were examined.

Table 3 shows the performance values of DES, AES and GEA symmetric encryption algorithms while encrypting 102 kilobytes of data. RSA asymmetric encryption algorithm cannot make big data encryptions. Its algorithm is not suitable for this. It usually works on large prime numbers. Therefore, it will not be included in the above and subsequent data analysis.

Table 3
102 Kilobyte Data Encryption

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	171	35	24
	AES	173	42	26
	GEA	169	32	22

When the graphic in Figure 9 is analyzed, it is seen that GEA algorithm processing time, memory and CPU usage performance are better than other DES and AES algorithms. The reason for the good performance of the GEA symmetric encryption algorithm is due to the key size used and the working principle of the algorithm.

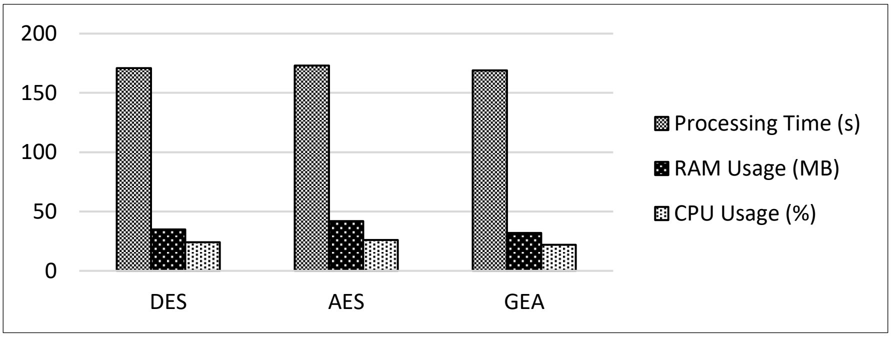

Figure 9
102 Kilobyte Data Encryptions

Table 4 shows the performance values of DES, AES and GEA symmetric encryption algorithms in the process of deciphering 102 Kilobyte data.

Table 4
Decryption Table of 102 Kilobyte Data

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	154	28	24
	AES	168	36	26
	GEA	148	26	22

When the graphic in Figure 10 is examined, it is seen that the processing time, memory and processor usage values of the GEA algorithm perform better than the DES and AES algorithms. This is just because of the key size and working principle used when encrypting data.

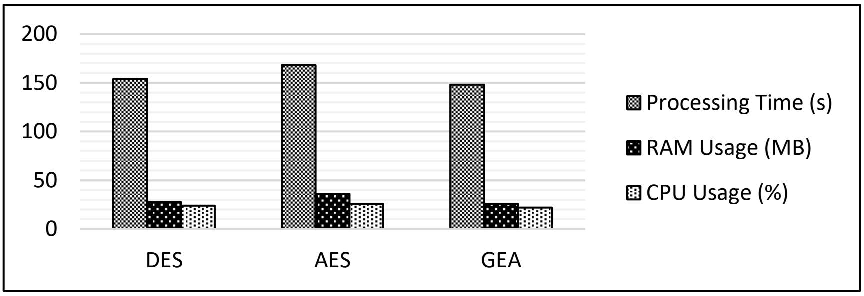

Figure 10
Decryption of 102 Kilobytes Data

5.3 Encryption and Decryption Analysis of 1 Megabyte Data

The processing time, processor usage and memory usage values obtained during the encryption and decryption of data with a character length of 1 Megabyte were examined.

Table 5
1 Megabyte Data Encryption Table

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	854	168	36
	AES	751	164	34
	GEA	853	166	35

Table 5 shows the performance values of DES, AES and GEA symmetric encryption algorithms for encrypting 1 Megabyte data.

When the graphic in Figure 11 is examined, it is seen that the AES encryption algorithm, memory and processor usage performance is better than DES and GEA algorithms. The reason that the AES algorithm performs better is due to the structure and working principle of the AES algorithm. The AES algorithm is that it has a flexible structure. Processing speed and performance do not change even if 128-bit, 192-bit or 256-bit keys of different sizes are used.

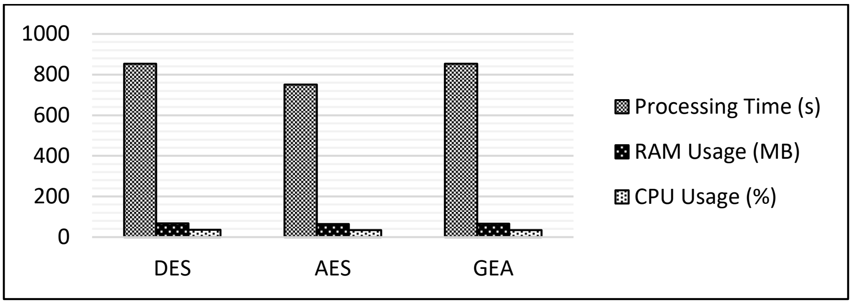

Figure 11

1 Megabyte Data Encryption

Table 6 shows the performance values of DES, AES and GEA symmetric encryption algorithms for password decoding of 1 Megabyte data.

Table 6

Decryption Table of 1 Megabyte Data

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	648	142	34
	AES	587	158	32
	GEA	643	160	33

When the graphic in Figure 12 is analyzed, it is seen that the performance of AES encryption algorithm, memory and processor usage is better than DES and GEA algorithms. The reason for the good performance of the AES symmetric encryption algorithm is the structure and working principle of the AES encryption algorithm.

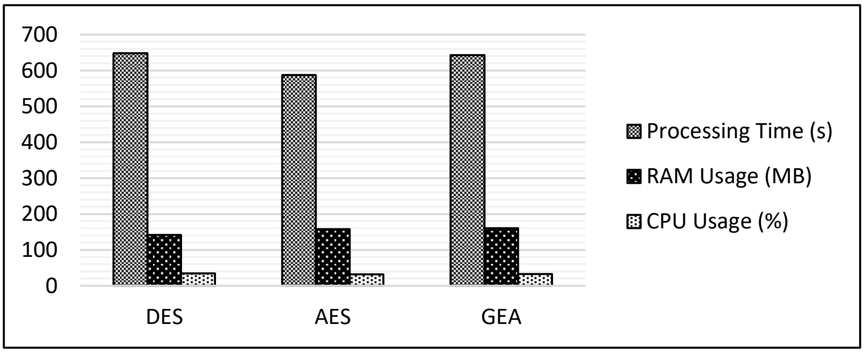

Figure 12

Decryption of 1 Megabyte Data

5.4 Encryption and Decryption Analysis of 5 Megabyte Data

The processing time, processor usage and memory usage values obtained during encryption and decryption of 5 Megabyte character length data were examined. Table 7 shows the performance values of DES, AES and GEA symmetric encryption algorithms for encryption of 5 Megabyte data.

Table 7
5 Megabyte Data Encryption

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	868	168	44
	AES	856	162	40
	GEA	886	174	54

When the graphic in Figure 13 is examined, it is seen that the performance values of the AES encryption algorithm are better, while the DES and GEA algorithm processing time, memory and processor usage performance values are very close to each other.

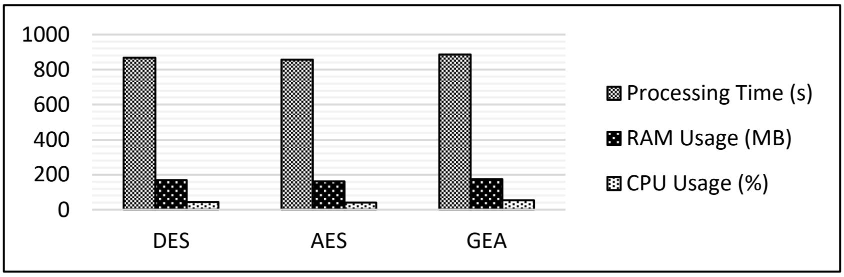

Figure 13
5 Megabyte Data Encryption

The reason for the good performance of the AES encryption algorithm is that it is more successful in terms of working principle in encrypting big data. Table 8 shows the performance values of DES, AES and GEA symmetric encryption algorithms for deciphering 5 Megabyte encrypted data.

Table 8
Decryption Table of 5 Megabyte Data

	Encryption Algorithms	Processing Time (s)	RAM Usage (MB)	CPU Usage (%)
Tested Computer	DES	648	142	34
	AES	587	138	32
	GEA	643	140	33

When the graphic in Figure 14 is examined, it is seen that the performance values of the AES encryption algorithm are better than the performance values of the DES and GEA encryption algorithms in the analysis of 5 Megabyte encrypted data. The reason for the better performance of the AES encryption algorithm is that the algorithm has its own unique working principle.

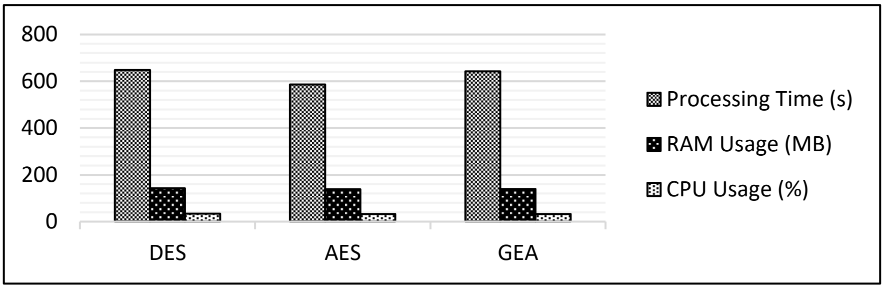

Figure 14
Decryption Graph of 5 Megabyte Data

Conclusions

Symmetric encryption algorithms performed better than asymmetric encryption algorithms, in encrypting data and analyzing encrypted data. Depending on the size of the key used for encryption and decryption, brute force breakage times vary. Since the DES algorithm uses a 56-bit key, the brute force break time is 2^{56} seconds. AES and GEA algorithms use 128-bit keys; the brute force break time is 2^{128} seconds. Genetic encryption algorithm developed to encrypt and decrypt small size data. DES performed better than AES and RSA encryption algorithms. The performance of the GEA algorithm is due to the amount of memory used for data encryption and recycling of encrypted data, processing speed, key size used and working principle. The AES encryption algorithm has been shown to be more successful in encrypting and decrypting large data. Since the RSA encryption algorithm does not tend to encrypt big data, it performs encryption based on the multiplication of large prime numbers, based on mathematical operations.

References

[1] C. C. Chang, M. S. Hwang, and T. S. Chen, “A new encryption algorithm for image cryptosystems,” *J. Syst. Softw.*, 2001, doi: 10.1016/S0164-1212(01)00029-2

[2] K. Raeburn and MIT, “RFC 3962 - Advanced Encryption Standard (AES) Encryption for Kerberos 5,” 2005

[3] W. M. H. Company, “Modern Cryptography: Theory and Practice,” *Theory Pract.* 2003

[4] R. Bhanot and R. Hans, “A review and comparative analysis of various encryption algorithms,” *Int. J. Secur. its Appl.*, 2015, doi: 10.14257/ijsia.2015.9.4.27

[5] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," *Int. J. Adv. Found. Res. Comput.*, 2014

[6] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.081141

[7] T. Nie and T. Zhang, "A study of DES and blowfish encryption algorithm," 2009, doi: 10.1109/TENCON.2009.5396115

[8] E. Islam and S. Azad, "Data encryption standard," in *Practical Cryptography: Algorithms and Implementations Using C++*, 2014

[9] P. P. Churi, "Performance analysis of data encryption algorithm," *Int. J. Recent Technol. Eng.*, 2019, doi: 10.35940/ijrte.C5775.098319

[10] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, 2016, doi: 10.1016/j.ijleo.2015.11.188

[11] A. Mousa, "Data encryption performance based on Blowfish," 2005, doi: 10.1109/elmar.2005.193660

[12] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *Journal of Advanced Research*. 2016, doi: 10.1016/j.jare.2015.07.002

[13] J. Grabbe, "The DES algorithm illustrated," *Laissez Faire City Times*, 1992

[14] M. Prerna and S. Abhishek, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Glob. J. Comput. Sci. Technol. Network, Web Secur.*, 2013

[15] M. J. Dworkin, "FIPS 197, Advanced Encryption Standard (AES)," *Netw. Secur. Natl. Inst. Stand. Technol.*, 2001

[16] S. D. Rihan, A. Khalid, and S. Eldin F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES," *Intetnational J. Eng. Res. Technol.*, 2015

[17] S. Ahmad, K. M. R. Alam, H. Rahman, and S. Tamura, "A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets," 2015, doi: 10.1109/NSysS.2015.7043532

[18] Ü. Çavuşoğlu and H. Al-Sanabani, "The Performance Comparison of Lightweight Encryption Algorithms," *Sak. Univ. J. Comput. Inf. Sci.*, 2019, doi: 10.35377/saucis.02.03.648493

[19] G. F. S. M. Asfiya Shireen Shaikh Mukhtar, "An Introduction of Advanced Encryption Algorithm: A Preview," *Int. J. Sci. Res.*, 2014

[20] K. Aggarwal, J. Kaur Saini, and H. K. Verma, "Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers," *Int. J. Comput.*

Appl., 2013, doi: 10.5120/11749-7244

[21] J. Raigoza and K. Jituri, “Evaluating Performance of Symmetric Encryption Algorithms,” 2017, doi: 10.1109/CSCI.2016.0258

[22] M. Mathur, “Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES,” *Proc. Natl. Conf. New Horizons IT*, 2013

[23] A. L. Jeeva, D. V Palanisamy, and K. Kanagaram, “Comparative analysis of performance efficiency and security measures of some encryption algorithms,” *Int. J. Eng. Res. Appl. ISSN*, 2012

[24] A. Majumder, A. Majumdar, T. Podder, N. Kar, and M. Sharma, “Secure data communication and cryptography based on DNA based message encoding,” 2015, doi: 10.1109/ICACCCT.2014.7019464

[25] B. Guttman, “DNA Structure,” in *Brenner’s Encyclopedia of Genetics: Second Edition*, 2013

[26] Şatır Esra Talu Furkan, "DES Algoritmasının DNA Modellenmesi ile Performans Analizi," International Marmara Sciences Congress, 2020

[27] Kovalchuk, A., Izonin, I., Strauss, C., Podavalkina, M., Lotoshynska, N., & Kustra, N. (2019) Image Encryption and Decryption Schemes Using Linear and Quadratic Fractal Algorithms and Their Systems. In *DCSMart* (pp. 139-150)

[28] D. S. Abd Elminaam, H. M. A. Kader, and M. M. Hadhoud, “Evaluating the performance of symmetric encryption algorithms,” *Int. J. Netw. Secur.*, 2010

[29] D. S. Abdul, H. M. Abdul Kader, and M. M. Hadhoud, “Performance evaluation of symmetric encryption algorithms,” 2009