Encryption from Past to Future

KEREM SALTIK
Istanbul Beykent University
Department of Software Engineering
Ayazaga, Hadim Koruyolu Cd. No:19
34398 Sariyer/Istanbul, TURKEY

YUSUF TALHA YILMAZ
Istanbul Beykent University
Department of Software Engineering
Ayazaga, Hadim Koruyolu Cd. No:19
34398 Sariyer/Istanbul, TURKEY

KEMAL GOKHAN NALBANT
Istanbul Beykent University
Department of Software Engineering
Ayazaga, Hadim Koruyolu Cd. No:19
34398 Sariyer/Istanbul, TURKEY

Abstract: Encryption has been an important tool from past to present for protecting the confidentiality, integrity, and accessibility of information. Throughout history, there have always been pieces of information that people wanted to keep hidden. For this reason, encryption methods emerged as a necessity and have evolved over time. With the advancement of mathematics and physics, the issue of security and data storage—one of the most critical concerns for states and major corporations—still remains important today. Due to these problems and developments, cryptologists have existed throughout history and have created various algorithms to protect data. One of the earliest encryption methods, Caesar cipher, was based on shifting letters according to a specific pattern, whereas modern cryptography has reached a more advanced level through mathematical algorithms and technologies. In quantum cryptography, a new chapter has been opened, where this method, based on physics rather than mathematics, has become a promising approach for the future. With the threat of quantum computers to classical encryption methods, quantum cryptography has come to the forefront. This method, based on the laws of physics, encrypts information through photons and is capable of revealing external interference. As in all areas of technology, competition in this field continues, and while efforts are made to improve encryption, counter efforts to break these encryptions are also being developed. This competitive environment contributes to the advancement of both sides. In this study, encryption methods and their historical development have been taken into consideration. In addition, using a common decryption method, the working principles and reliability of these encryption techniques are evaluated and compared. Although the results in the brute-force test were as expected, in terms of encryption and decryption times, classical encryption methods performed faster than modern ones. Based on these results, the study aims to understand future technologies and developments.

Key–Words: Cryptology, Classical Encryption, Modern Encryption, Quantum Encryption, Symmetric and Asymmetric

Received: April 11, 2025. Revised: April 25, 2025. Accepted: May 19, 2025. Published: July 7, 2025.

1 Introduction

This article is a study that aims to inform about the development of encryption methods that have existed since the past and will be used today and even in the future. Information and the security of this information in every field from past to present are of great importance for every person and even every civilization. As people understand the security and importance of information, some steps are being taken on this issue and efforts are being made to find a solution to this problem. Although people are not aware of this at first, the basis of encryption algorithms used in the past or today is based on mathematics. For this reason, encryption methods, which have actually been developing as an extension of technology and science from the beginning, have emerged as a new field to meet research and people's efforts. To give a more specific example, in the Caesar cipher, one of the first encryption methods, the letter "D" is used instead of "A" and the letter "B" is used instead of "E". Although this method seemed different from mathematics at that time, when we look at it today, it is not a different method from the pattern subject of mathematics. Cryptography and cryptology, which people are familiar with by hearing these terms more and more today, are one of the fields that have been formed to meet these needs.

Cryptography can be seen as the field that encompasses technical methods used to protect the confidentiality, integrity and accuracy of information and data. Cryptology, on the other hand, is a broader discipline that deals with encryption and decryption as a whole and includes cryptography. The aims of these two areas are similar: to develop encryption systems and to analyze these systems, thus ensuring that the protected data cannot be accessed by unauthorized persons and is only reserved for those with this authority.

If we look at the security of information and encryption methods, the security of information is based on 3 basic principles. These can be called confidentiality, integrity and availability. When looked at in more detail, confidentiality can be said to be the secrecy of information, that is, restricting the use of only authorized persons in this area and the access of unauthorized persons. Integrity refers to the preservation of the accuracy and completeness of information. Encryption methods can corrupt the formats of data and damage the data that is intended to be protected, even if people do not make changes to the data. Therefore, the principle of integrity is very important in this regard. Finally, accessibility ensures that authorized users can access information when they need it. When these principles and mathematical algorithms come together, encryption methods that ensure the security of information emerge. Encrypted data can only be decrypted and read by those who have the correct key. These encryption methods not only belong to the past but also contributed to the rise of modern encryption; they have also contributed to the emergence of modern encryption methods used today. If we talk about modern encryption methods, these methods are divided into symmetric and asymmetric. Additionally, hash functions and hybrid cryptosystems are also important parts of modern cryptography. To be more detailed and explanatory:

1.1 Symmetric Encryption

It supports using the same key to encrypt data, making it faster and more effective in large data sets. Examples of this method are AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish and Twofish. DES has now been replaced by AES due to insufficient security and is widely used in online banking, wireless networks, and government applications. Although it has advantages such as being fast, requiring low processing power and being usable on small-sized devices, it also has disadvantages such as security breaches that may occur if this key is captured because the same key is used for encryption [1].

1.2 Asymmetric Encryption

It uses two keys, public key and private key, and avoids the disadvantages of the symmetric encryption method. However, it is slower than symmetric encryption and more difficult to use on large data sets. Examples of this method are RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) and Diffie-Hellman [2].

The areas of use of modern encryption are quite numerous and widespread, such as e-commerce, banking, email security, VPN (virtual private networks) and blockchain. As a result, this encryption method takes the help of advanced algorithms to ensure the security of data. While symmetric encryption is preferred for speed and performance, asymmetric encryption provides secure key exchange.

In this context, the main research question is to what extent encryption techniques, which have evolved from past to present, ensure information security, whether they meet today's requirements, and what innovations they may lead to in the future. Due to the ever-increasing need for information security, it has become essential to examine the advantages and disadvantages of both classical and modern encryption methods, and to determine which method is more suitable under specific circumstances.

The primary objective of this study is to investigate the historical evolution of encryption methods, uncover the fundamental mathematical principles behind them, and evaluate their impact on security. Additionally, the study aims to conduct a comparative analysis of symmetric and asymmetric encryption techniques and provide a comprehensive perspective on their areas of application in the modern world. The research questions have been formulated as follows:

- How have historical encryption techniques contributed to modern encryption systems?
- In which scenarios are symmetric and asymmetric encryption methods more advantageous?
- Which sectors in today's world have a greater need for encryption technologies?
- What are the strengths and weaknesses of encryption methods in terms of security, performance, and accessibility?

2 Literature Review

When we look at the historical development of encryption, the first examples date back to the Egyptian, Roman and Greek civilizations [2]. Encryption methods can be categorized as follows.

2.1 Old Encryption Methods

2.1.1 The Caesar Code (58 BC)

Historically, it is considered the most famous old encryption method. It is known as the Caesar shift method and was used by Roman Emperor Julius Caesar, and its logic is based on creating a password by shifting each letter of the alphabet a certain number of times. It was also used in the Middle Ages [3].

- Working Logic: A key is determined for encryption and the letters are shifted by the determined key value. For example, when the key value is selected as 2, the word ”EXAM” is encrypted as ”GZCP”.
- Features: Since the encryption method is simple and can be easily solved using frequency analysis, it is limited in terms of security.

2.1.2 Atbash Encryption (500 BC)

It performs encryption based on the reverse alphabet logic [4].

- Working Logic: Each letter is replaced with the letter opposite it. For example, instead of 'A', 'Z' is used. Since the letter 'A' is the first letter of the alphabet and the letter 'Z' is the last letter of the alphabet, they correspond to each other. The same situation can be exemplified by using the letter 'Y' instead of the letter 'B'. The word 'EXAM' is encrypted as 'VCZN'.
- Features: Since it is an old method, it provides weak security. The reason it was used in the past was that it provided an easy solution.

2.1.3 Scytale Encryption (500 BC)

The method used by the ancient Greeks and Spartans is using a cylindrical encryption device (scytale), where the text on the tape is rolled up to a specified thickness and the decryption is done once the cylinder of the correct diameter is obtained [5].

- Working Logic: The message to be hidden is wrapped in a cylinder of a certain diameter and after it is encrypted, it can be read in a certain order.
- Features: Although it is a simple method, it is an effective method because the encrypted message can only be decrypted by people who have a certain cylinder.

2.1.4 Cubed Encryption (Polybius Square)

This method, which comes from the ancient Greek period, enables encryption by placing alphabet letters in a 5x5 shape. Each letter is converted to a number pair. There is no clear information about how it is converted.

- Working Logic: A 5x5 square is created and letters are placed in it. However, if we talk about the English alphabet, there will be two letters in a square since there are 26 letters. When the word ”EXAM” is given, each letter is represented by the number in which it is in the order.
- Features: It is based on simple number and letter matching, but this method can only be used on handwriting and is weak in terms of reliability.

2.1.5 Sword Cipher (Transposition Cipher)

It is a method in which the order of the letters is changed. It includes types such as block transposition and column transposition.

- Working Principle: The letters in the message content are replaced according to the specified rule.
- Features: It performs the letter change process without changing the content of the message. It is usually solved by using a key.

2.2 The Middle Ages and the Renaissance

When we look at this period, encryption methods were mostly used for military and diplomatic purposes. The most important methods that stand out here are the Vigenère cipher (16th century) and Frequency analysis.

2.2.1 The Vigenère Cipher

It performs letter shifting similar to the Caesar cipher method, but the difference is that it performs the encryption process by using a different shift for each letter in the alphabet. However, this method was introduced to the modern encryption world in the 19th century. It was developed based on polyalphabetic encryption [6].

- Working Logic: A keyword is used and the letters of the word or text to be encrypted are replaced with the letters of the keyword and a new keyword emerges. If the number of letters of the object to be encrypted is greater than the keyword, the keyword is cycled through from the beginning. Then, the indexes (indexes) of the letters of the text or word to be encrypted and the newly formed keyword are found in the dictionary. These numbers are added to the sequence number of the first letter of the word to be encrypted and the sequence number of the first letter of the new keyword and the resulting number corresponds to the first character of the password in the alphabet. In this way, it goes to the last character and when the process is finished,

the encryption is completed. If the text to be encrypted is "EXAM" and the keyword is "KEY", the password of the input will emerge as a result of the following steps.

- Message: EXAM
- Keyword: KEY
- New Keyword: KEYK
- The numerical equivalents of the letters in the new keyword in the alphabet will be K = 10, E = 4, Y = 24, respectively. The places of the message letters in the dictionary will be E = 4, X = 23, A = 0, M = 12, respectively.
- When the encryption process is started, first the index number (24) of the first letter (E) of the message and the index number (10) of the first letter (K) of the new keyword are added. The result will be 14 and the letter in the 14th index in the alphabet is the letter 'O'. This will continue until the last letter and the password will be "OBUW". In addition, if the total is more than the number of letters in the alphabet, it is divided by the number of letters in the alphabet and its mode is taken and according to the result, the letter corresponding to the letter in the alphabet is taken.

2.2.2 Pigpen Cipher

In this encryption method, a special shape or symbol is used for each letter in the alphabet. It is also known as the Masonic Cipher or Freemason Cipher, from which it can be concluded that it was used especially by Masons [7].

- Working Logic: To decipher the password, find the letter that the symbol represents. It basically consists of two main parts, linear symbols that replace the letters and circular symbols that contain the letters.
- Features: Unless the symbols are known, it is difficult to decipher the code.

2.3 Present and Future

2.3.1 Advanced Encryption Standard (AES)

It is used in many areas, especially data security, internet communication and database encryption. It was accepted as an encryption standard by the United States National Institute of Standards and Technology (NIST) in 2001. Data is encrypted in blocks and encryption is performed by performing operations on the blocks. Security depends on the complexity of the algorithm and the key length [8].

- Working Logic: In the initialization step, the key is added to the 128, 192 or 256 bit data block [9]. This step is also called AddRoundKey. The second step is the main rounds step. In this step, the round process is applied according to the number of bits. There are 10 rounds for a 128 bit key, 12 for a 192 bit key and finally 14 rounds for a 256 bit key. Basically, four operations are applied in each round.
  - SubBytes: A table called S-box (Substitution box) is used to encrypt each byte, and the value from the table is used in place of each byte.
  - ShiftRows: There is no shifting in the first row of the data block. Every nth row except the first row is shifted by n-1 positions.
  - Mix Columns: Each column is mixed linearly to distribute the data. It increases the security of the password.
  - AddRoundKey: At the end of each round, a specific key is added to each block and the keys used in the previous round are changed in each round.
  - Final Round: All operations except the MixColumns operation are performed again.
- Features: Since symmetric encryption is used, the same key is used for encryption and decryption. Encryption is performed in block size. It supports three different (128 - 192 - 256) ahtar lengths. It is suitable for real-time data encryption.

2.3.2 Asymmetric Encryption

This method, which deals with mathematics as encryption and decryption methods, uses a pair of keys. The first of these is the public key. This key is used for encryption and is called the public key because it allows everyone to share it. The second key is called the private key. This key, unlike the other, is stored privately and is used to decrypt the encrypted message. Thanks to these two keys, a more secure system is formed due to the lack of key transfer between the sender and the receiver. However, there are some disadvantages since the private key must be stored carefully [10]. Example asymmetric algorithms are as follows:

- RSA (Rivest–Shamir–Adleman): It is one of the most widely used asymmetric encryption algorithms. It works with large prime numbers and is used for encryption, decryption and digital signature verification [9]. Its security comes from the basis of factoring the product of two large prime numbers, and this difficulty makes it difficult to break mathematically. However, it also has disadvantages such as being slower than other algorithms and requiring more processing power for large keys.
- ECC (Elliptic Curve Cryptography): It is an algorithm built on mathematical structures called elliptic curves. This algorithm, which provides security with a small key size, is used for both encryption and digital signatures. It proves to have disadvantages as it is mathematically more complex and is not supported in some older systems because it is a new technology [10].
- DSA (Digital Signature Algorithm): It is an algorithm specifically designed to create and verify digital signatures. Its security increases because it is based on the difficulty of solving the discrete logarithm problem. However, it is less flexible than other algorithms and is not as common as ECC and RSA, which are the precursors to some problems.

Feature	RSA	ECC	DSA
Key Size	Big	Small	Middle
Speed	Slow	Fast	Fast (For Signature)
Security F.	Factoring	Elliptic Curves	Discrete Logarithm
Area of Use	General Encryption	Mobile and IoT	Digital Signatures

Table 1: Summary Comparison of RSA, ECC and DSA

2.3.3 Quantum Cryptography

The reason why data is safe at the moment is that it is very difficult for computers working with classical logic to break passwords based on multi-factor equations. However, this is not a result that supports that information will remain safe in the future. In the changing and rapidly developing world, with the idea and invention of quantum computers, although large companies and states have made it easier, another question that came with this idea has caused contradictions in minds. People who have these computers can, if they wish, break the encryption methods used, without the need for millions of years, thanks to quantum computers. Quantum cryptography, as a solution to this problem, provides the reliability we need both today and in the future. If we go into it a little more and look at the differences with other methods, the encryption methods currently used consist of 0s and 1s in classical computers and can be read by decrypting with symmetric or asymmetric keys. Because in classical encryption, the basis of computers is based on mathematics. Quantum cryptography, on the other hand, changes this basis and uses the laws of physics instead of mathematics [11]. The cornerstone of this encryption method is the principle that we cannot know everything about a quantum particle with complete accuracy in this area of the laws of physics [11]. The key to the encrypted messages sent based on the laws of physics is sent to the other party with the help of photons, unlike classical encryption. These sent photons follow a path known only to the sender and receiver thanks to the filters they pass through. Because it is not clear which ones are 1 and which ones are 0 in the filters they pass through. If an outside eye wants to intervene in these photons, they will not be able to guess the correct order because they use their own filter and both parties will notice that there is an external intervention [12]. Because this basis, which is based on physics, affects the observer particles. Although it seems flawless and unbreakable, this method will be doomed to develop over time with the development of quantum computers and their becoming problem-free.

3 Method

The study, which examined encryption methods from the past to the future, was conducted with a model based on literature review. In order to understand the historical process and follow the development, past sources were analyzed and the foundations of current methods were explained and future potential developments were shed light. In this context, in addition to the articles reviewed and researched, each encryption method used and transferred from the past to the present was organized and tested, and the data was noted and used for comparisons. By putting these data into the same tests, success criteria and their comparisons with each other were examined. In addition, an explanatory and analytical approach was adopted in the research process. In the experimental results stage, information will be given about the encrypted version of the text after the encryption process of most encryption methods discussed in the literature review, then the encryption time and decryption speed of these methods, and finally, whether the attack was successful or not with a simple brute force test, the attack time and the number of attempts. Within the scope of the study, encryption methods currently used and to

be used in the future were discussed and studies were carried out in a limited area. As a result of the research conducted in this area, resource insufficiency was noted and it was aimed to eliminate this problem.

4 Experimental Results

To show the performance of the methods among themselves, "Special Topics in Software Engineering" was selected as a sample text and encrypted with each encryption method. The passwords generated by the methods are as follows (fig. 1).

Figure 1: Sample Text Encryption

In Table II, an encryption was used for each method and then these encryptions were decrypted and their times were measured. In Table III, a table is given for attacks performed using brute force. A brute force attack is a type of attack that occurs when all possibilities are systematically tried to decrypt encrypted data. In order to break the passwords, it tries all the combinations required to find the key. The basic logic of this attack is as follows:

- Key Length and Character Set: If the length of the key of the encrypted message and the character set used are known, the attack can try every possible combination by working on this character set.
- Trial and Error: The aim is to try all the possibilities one by one and find the correct key.
- Time Consumption: As the length of the key and the character set vary and expand, the time it takes for the attack to be successful increases.

Method	Encryption Time (s)	Decryption Time (s)
Caesar Cipher	0.001	0.001
Vigenère	0.002	0.002
AES	0.005	0.006
RSA	0.150	0.020

Table 2: Encryption and Decryption Speeds

Method	Attack Status	Time
Caesar Cipher	Successful	$<$1s
Vigenère	Successful	$<$5s
AES	Failed	N/A
RSA	Failed	N/A

Table 3: Brute Force Attack Results

5 Findings

According to the results of the brute force attack test, when Table III is taken as the most secure encryption methods, today's and medieval encryption methods are at the forefront, while when Table II is taken as the reference in terms of encryption and decryption speed, old and medieval encryption methods are at the forefront. When all methods are compared in general, the Vigenera encryption method stands out more than the other methods on average. A suitable ground has been prepared for future studies to add more encryption methods and to be able to do more tests on these methods.

6 Discussion

This study shows how encryption methods currently perform on a basic brute force, in addition to their performance in encrypting and decrypting the available data. The shortcoming of the current study is that not all encryption models were considered, and a study was conducted on the most commonly used methods at the time. In addition, only one brute force test was applied. Encryption and password performance measurements were made on only one word group.

7 Conclusion

This study, which examines and analyzes the historical process of encryption methods, focuses on their development in the process and their potential for the future. In line with this result, it is shown that encryption techniques have continuously evolved from the past to the present. Encryption methods, which have

become more complex and powerful in line with increasing data security requirements, range from classical encryption methods such as Caesar and Atbash to modern techniques such as AES and RSA, which are widely used today. The results obtained reveal that although classical encryption methods are simple and quickly applicable, they are insufficient against modern attack techniques. In contrast, modern methods provide strong protection with their more secure key structures and mathematical bases. However, it is likely that this area will be abandoned in the near future and that it will now be more complex and that it will switch to the laws of physics. A situation that will put the security of existing encryption algorithms at risk, especially with the development of quantum computers in this area, has emerged. As a result, it is clear that encryption algorithms are in a constantly evolving state and that more reliable, faster and more efficient solutions will be needed in the future. In the future, new generation technologies such as quantum cryptography will play an important role in creating stronger and more unbreakable systems compared to classical methods. This article, which emerged as a result of the inadequacies and lack of work in this field, was presented as a reference for future studies.

The rapid developments in quantum computing pose serious risks to existing encryption methods, making traditional techniques less reliable in the near future. According to Bernstein and Lange [13], it's crucial that we start looking into new types of encryption that can withstand quantum attacks. Mosca [14] emphasizes that we should already be preparing for security issues that quantum computing could soon cause, instead of waiting until problems arise. Similarly, Pirandola et al. [12] introduce quantum cryptography as a promising alternative—one that applies principles from quantum physics to strengthen communication security.

References:

[1] Mohammed N Alenezi, Haneen Alabdulrazzaq, and Nada Q Mohammad. Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2):256–272, 2020.

[2] Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, Tanvi Madhekar, and BS Thakare. Brief history of encryption. International Journal of Computer Applications, 131(9):28– 31, 2015.

[3] TÜBİTAK. Hafta4: Kriptografi. TÜBİTAK, Ankara, 2022.

[4] A Hassan, NJ Mallam, A Umar, AU Dakingari, and ZZ Illo. A modified atbash cipher with special characters and stack implementation.

[5] Martine Loekie Mariska Diepenbroek. Myths and histories of the spartan scytale. University of Bristol, 2020.

[6] Saputra Dwi Nurcahya, Dian Nazelliana, et al. Message security in classical cryptography using the vigenere cipher method. International Journal Software Engineering and Computer Science (IJSECS), 4(1):350–357, 2024.

[7] D Parrangan and Theofilus Parrangan. New simple algo- rithm for detecting the meaning of pigpen chiper boy scout ('pramuka'). Int. J. Signal Process. Image Process. Pattern Recognit., 6(5):305–314, 2013.

[8] Muhammad Rameel and Zain Asif. Fortifying information security: a comparative analysis of aes, des, 3des, rsa, and blowfish algorithm. EasyChair Preprint 13536, EasyChair, 2024.

[9] Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud. Studying the effects of most common encryption algorithms. International Arab Journal of e-technology, 2(1):1–10, 2011.

[10] Musa Ugbedeojo, Marion O. Adebiyi, Oluwasegun Julius Aroba, and Ayodele Ariyo Adebiyi. Rsa and elliptic curve encryption system: A systematic literature review. Int. J. Inf. Sec. Priv., 18(1):1–27, March 2024.

[11] Sadullah Çelik. Kuantum kriptolojisi ve siber güvenlik. Bilişim Teknolojileri Dergisi, 14(1):53–64, 2021.

[12] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. Advances in optics and photonics, 12(4):1012–1236, 2020.

[13] Daniel J Bernstein and Tanja Lange. Post-quantum cryptog- raphy. Nature, 549(7671):188–194, 2017.

[14] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5):38–41, 2018.