Introduction to Cryptography and Advanced Encryption Standard

Md. Shapan Miah*

Department of Mathematics, University of Dhaka, Dhaka-1000, Bangladesh

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2024.1109065

Received: 23 September 2024; Accepted: 28 September 2024; Published: 11 October 2024

ABSTRACT

Cryptography, the art and science of securing information, is vital in securing sensitive data in today's digital age. This paper begins with an overview of cryptography's core principles and role in modern computing. It then delves into the core of our discussion, Advanced Encryption Standard (AES) [1,3].

AES, a widely used encryption standard, is a cornerstone of modern data encryption. In this paper, we explore its history, the complexities of its algorithm, key length considerations, and security in the face of evolving threats, including quantum computing. We also shed light on AES's practical applications showing its pervasive influence on data security. This paper provides a concise yet informative introduction to cryptography and a detailed examination of AES encryption, offering readers valuable insights into its significance in the digital realm.

Keywords: Cryptography; Encryption; Decryption; Group; Field; Rings; Round; Block Cipher.

AMS Subject Classifications 2020: 03G05, 03G27, 05C25.

INTRODUCTION

Digital communication is of utmost importance in transferring massive amounts of data worldwide every day. Throughout the decades, the concern about data security has increased because of spying and manipulation by malicious users. To prevent that, various security measures were invented and applied to ensure that the data reaches only to our intended users. The study of utilizing mathematical tools to protect data by encrypting and decrypting is known as cryptography. With the assistance of cryptography, we may store and send private data in a way that only the intended receiver can read it over a public networking system like the internet. The science of data security is known as cryptography, whereas the scientific method to analyse and dismantling secure exchange is known as cryptanalysis [3]. The process of performing traditional cryptanalysis requires an intriguing blend of analytical thinking, the use of mathematical tools, pattern recognition, patience, tenacity, and good fortune.

The core concern of cryptography is offering confidentiality, integrity, nonrepudiation, and authentication through encryption and decryption algorithms. Predominantly, there are three types of algorithms which are symmetric, asymmetric, and hashing.

Encryption has been used to obscure sensitive data since ancient eras, but it got its prime attention during the second World War in the Twentieth Century. Scientists and researchers spent several decades in search of a strong encryption algorithm because of the rising of threats to computer-based digital communication. We had several algorithms, those algorithms were considered to be unbreakable but today they are not unbreakable. For example, we can say the DES encryption algorithm developed by IBM.

The Advanced Encryption Standard (AES) algorithm is a type of encryption method that uses block cipher techniques. After three competitive rounds and rigorous cryptanalysis by top encryption experts, NIST choose the Rijndael algorithm (which is also known as the AES encryption algorithm) as the winner in October 2000, created by Belgian cryptographers Joan Daemen and Vincent Rijmen. Initially, AES was approved only for encrypting non-classified government data. By 2003, AES received approval for securing secret and top secret classified data for the U.S. government. The core purpose of this algorithm was to displace the DES algorithm because of its vulnerability. Advanced Encryption Standard (AES) is a symmetrical encryption algorithm. This means the similar key is applied here for encryption [4,7] and the reverse conversion decryption [4]. The only thing which must be kept is undercover the key. It may uses various key lengths. Nowadays safety anxiety grows with cloud adoption at institution level, information centre, recent users and cryptography algorithm has a extraordinary influence safety concern. In reality it is used for confirming coverty, data savings, communication, safety for hardware and software.

One of the key fields that draw researchers to conduct studies is the hardware and software establishment of the AES encryption algorithm. In recent years, numerous research papers have been published on the AES algorithm to provide greater detail and compare its performance with other well-known encryption algorithms. In [11] Lu, etal showed that the AES encryption algorithm outperforms three widely used algorithms: RC2, DES, and 3DES. The AES encryption algorithm was standardized in the Federal Information Processing Standard (FIPS) 192, released in November 2001 [12, 13].

In this paper we have discussed about AES encryption process [7] and decryption. AES is based on mathematics. So mathematical concepts [2,5] are discussed in Appendix A. Some basic terms which are necessary for encryption like round and block cipher [7] are explained in this manuscript. Then encryption and decryption are explained here elaborately. Finally we have shown an encryption & decryption example using python code [9,10] and drawn our conclusion.

SOME BASIC TERMS FOR AES

In this section we'll discuss about some main words which help us to realising the AES works better.

Round

A round is a conversion procedure applied during encryption which involved some function substitution, transposition and blending with the acquirement to have a maximum output cipher text. In table 2.1 we see each key shape, number of round which provide a high secured system.

Table 2.1 Structure of AES

AES Types and Key Shape	Data Block Size	Matrix Block	Rounds
128	128	4 × 4	10
192	128	4 × 6	12
256	128	4 × 8	14

Block Cipher

A block cipher is a process to encrypt information by class at time and uses the similar key in decryption and encryption. Actually the objective of block cipher method is to eliminate resemblance of cipher text when encrypting even if the similar message is being encrypted again. The below matrix gives the representation of 128 in block matrix 4×4 column major.

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

AES runs on rows, columns and entity of the existing matrix. Likewise, for other two types might have four (192-bit) rows and six (256-bit) or eight columns. Note that the key size must be the same as the primary block matrix.

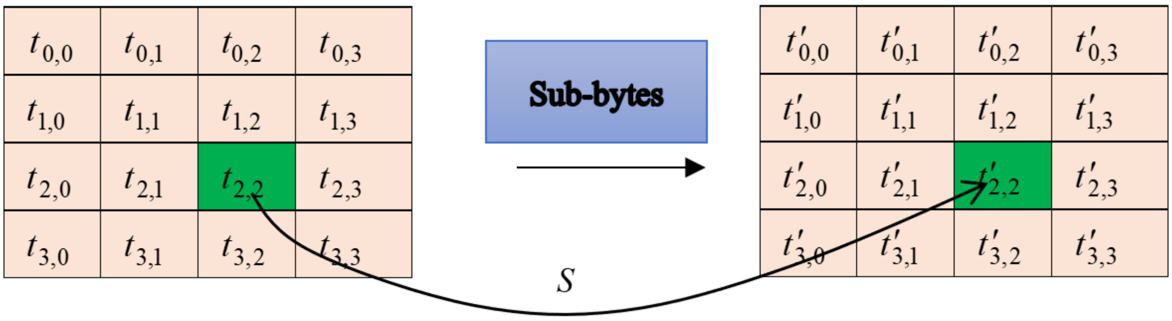
Before starting encryption, the plaintext data needs to be padded to ensure the consistency of data length with block sizes. Common padding schemes include PKCS#7 and ISO/IEC7817-4 padding.

ENCRYPTION PROCESS

The AES encryption process consists of multiple rounds, depending on the key length. Now we'll discuss about various steps which are used in encryption algorithm.

Substitution of Bytes

This step involves a non-linear substitution, where each byte is replaced with corresponding value from the substitution box (S-box). In figure 3.1 we see that every byte $t_{i,j}$ is replaced with sub-byte $t'_{i,j}$ using substitution box. To eliminate destroys founded on facile algebraic features, the S-box is formed by combining the inverse function with an invertible affine transformation.



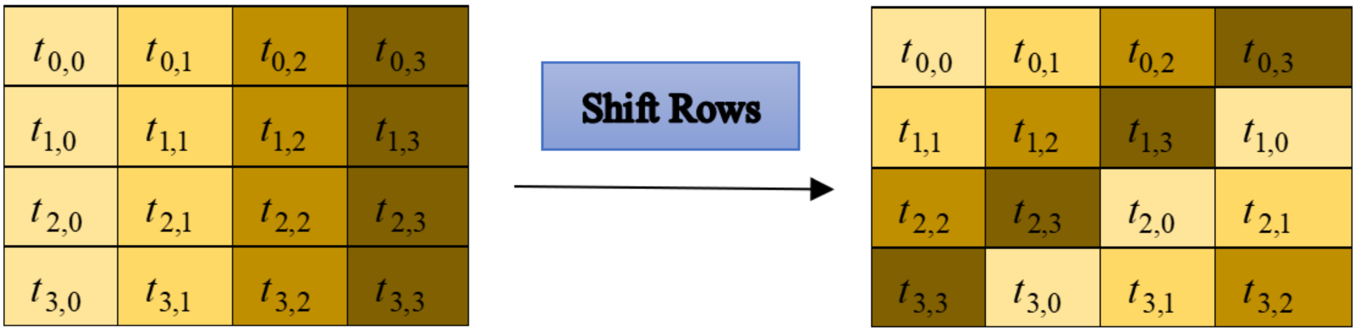
$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$
$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$
$t_{2,0}$	$t_{2,1}$	$t_{2,2}$	$t_{2,3}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$

$t'_{0,0}$	$t'_{0,1}$	$t'_{0,2}$	$t'_{0,3}$
$t'_{1,0}$	$t'_{1,1}$	$t'_{1,2}$	$t'_{1,3}$
$t'_{2,0}$	$t'_{2,1}$	$t'_{2,2}$	$t'_{2,3}$
$t'_{3,0}$	$t'_{3,1}$	$t'_{3,2}$	$t'_{3,3}$

Fig. 3.1. Sub-bytes process.

Shift Rows

It is a row-wise movement by completing a rounded switch on the last three rows of state. In figure 3.2 we have tried to show that it shifts the second row of the following matrix three bytes to the right, the third row by two bytes to the right and the fourth row by one byte to the right which are shown by different colours.



$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$
$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$
$t_{2,0}$	$t_{2,1}$	$t_{2,2}$	$t_{2,3}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$

$t_{0,0}$	$t_{0,1}$	$t_{0,2}$	$t_{0,3}$
$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,0}$
$t_{2,2}$	$t_{2,3}$	$t_{2,0}$	$t_{2,1}$
$t_{3,3}$	$t_{3,0}$	$t_{3,1}$	$t_{3,2}$

Fig. 3.2. Shift Rows process.

Mix Column

Mix column is a linear conversion. It is a matrix multiplication treating the four bytes of a column. Columns are considered as polynomials. In figure 3.3 we see have shown that in the Mix Columns step, each column is treated as a polynomial and transformed through matrix multiplication with a fixed polynomial$c(x)$.

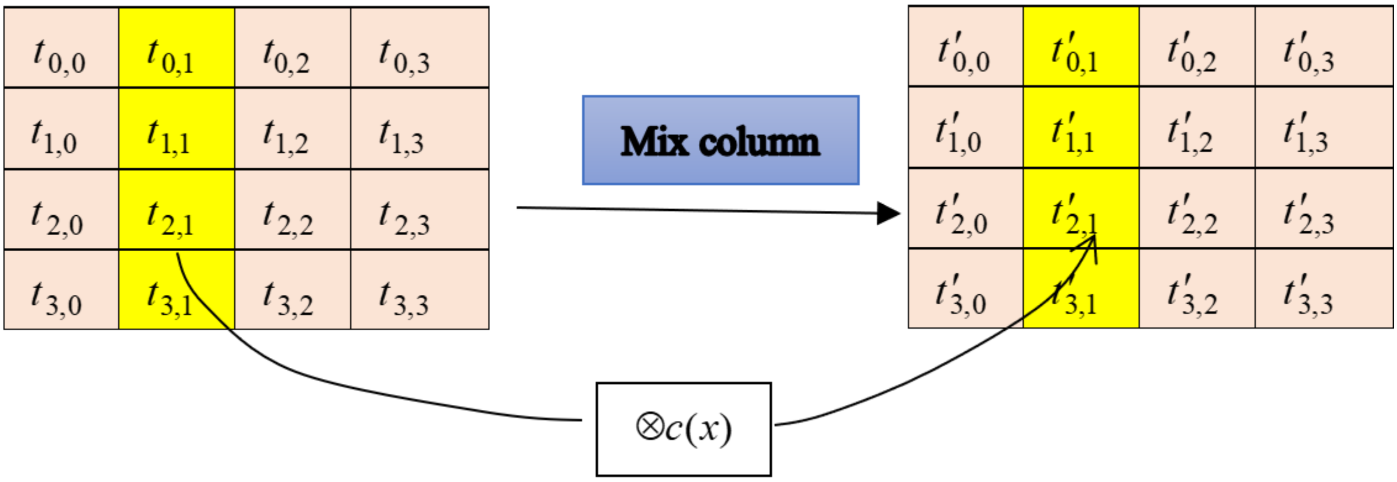

$t_{0,0}$ $t_{0,1}$ $t_{0,2}$ $t_{0,3}$
$t_{1,0}$ $t_{1,1}$ $t_{1,2}$ $t_{1,3}$
$t_{2,0}$ $t_{2,1}$ $t_{2,2}$ $t_{2,3}$
$t_{3,0}$ $t_{3,1}$ $t_{3,2}$ $t_{3,3}$
Mix column
$t'_{0,0}$ $t'_{0,1}$ $t'_{0,2}$ $t'_{0,3}$
$t'_{1,0}$ $t'_{1,1}$ $t'_{1,2}$ $t'_{1,3}$
$t'_{2,0}$ $t'_{2,1}$ $t'_{2,2}$ $t'_{2,3}$
$t'_{3,0}$ $t'_{3,1}$ $t'_{3,2}$ $t'_{3,3}$
$\otimes c(x)$

Fig. 3.3. Mix Column Process.

Add Round Key

The fourth transformation function of AES is called as Add Round Key. It is also known as forward add round key conversion. In this step, the existing 16-byte matrix and a 16-byte sub key are served as inputs. The existing matrix is bitwise XOR-ed with the 16-byte sub key. Add Round Key proceeds one column at a time. The sub keys attained in the schedule are portrayed in the next section. In figure 3.4 for every round a sub-key is formed from the main key with the help of Rijndael's key scheme.

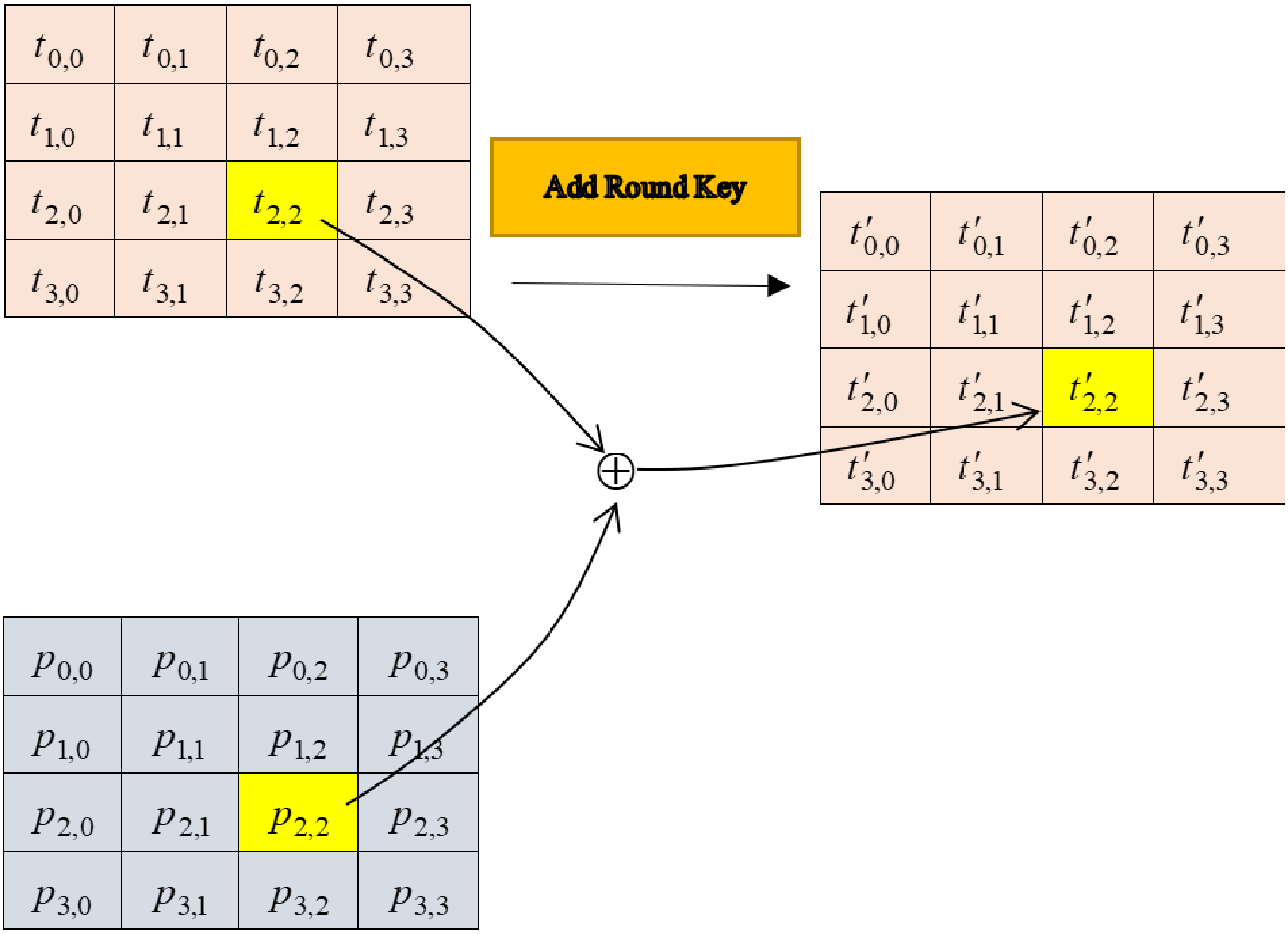

$t_{0,0}$ $t_{0,1}$ $t_{0,2}$ $t_{0,3}$
$t_{1,0}$ $t_{1,1}$ $t_{1,2}$ $t_{1,3}$
$t_{2,0}$ $t_{2,1}$ $t_{2,2}$ $t_{2,3}$
$t_{3,0}$ $t_{3,1}$ $t_{3,2}$ $t_{3,3}$
Add Round Key
$t'_{0,0}$ $t'_{0,1}$ $t'_{0,2}$ $t'_{0,3}$
$t'_{1,0}$ $t'_{1,1}$ $t'_{1,2}$ $t'_{1,3}$
$t'_{2,0}$ $t'_{2,1}$ $t'_{2,2}$ $t'_{2,3}$
$t'_{3,0}$ $t'_{3,1}$ $t'_{3,2}$ $t'_{3,3}$
$\oplus$
$p_{0,0}$ $p_{0,1}$ $p_{0,2}$ $p_{0,3}$
$p_{1,0}$ $p_{1,1}$ $p_{1,2}$ $p_{1,3}$
$p_{2,0}$ $p_{2,1}$ $p_{2,2}$ $p_{2,3}$
$p_{3,0}$ $p_{3,1}$ $p_{3,2}$ $p_{3,3}$

Fig. 3.4: Add Round Key process.

The whole AES encryption process is shown in figure 3.5

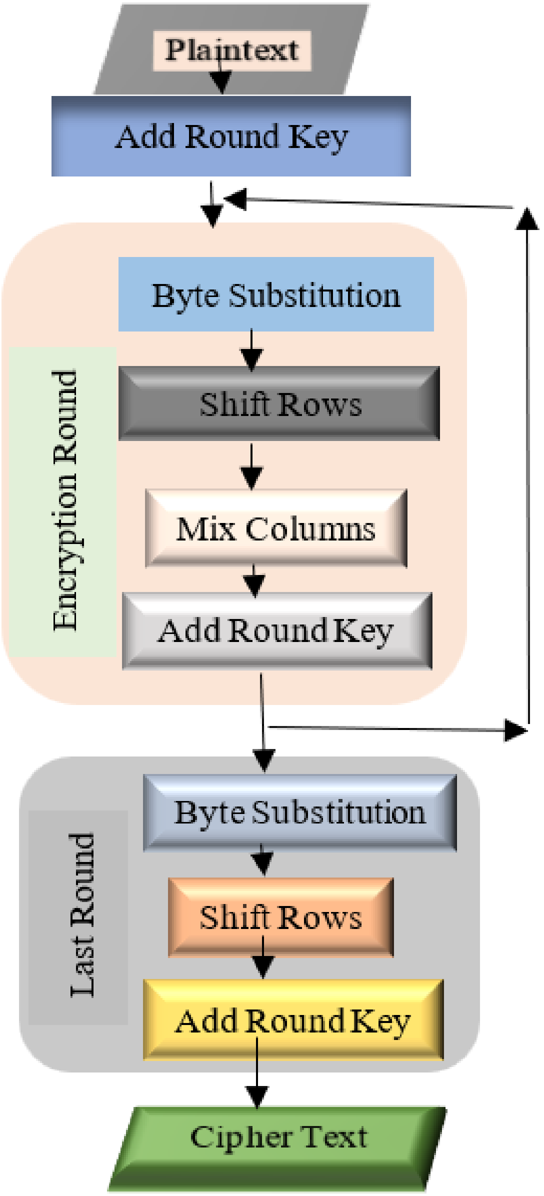


Fig. 3.5. AES Encryption block Diagram.

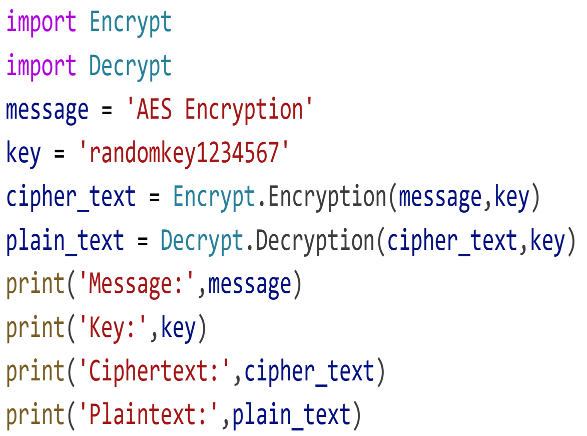
DECRYPTION PROCESS

So far we have seen that every mathematical action is performed in AES encryption is invertible i.e., Substitution of Bytes becomes Inverse Substitution of Bytes, Mix Column becomes Inverse Mix Column and Shift Rows becomes Inverse Shift Rows. Further observation is that we have to use the sub keys in reverse order. The decryption process of AES is similar to encryption process which are performed in reverse order as

- Add Round Key
- Mix columns
- Shift Rows
- Byte substitution

Since sub processes in each round are in reverse order, the encryption and decryption algorithms need to be implement separately, even though they are closely related.

We can see an example of AES Cryptography using python code as



```
import Encrypt
import Decrypt
message = 'AES Encryption'
key = 'randomkey1234567'
cipher_text = Encrypt.Encryption(message,key)
plain_text = Decrypt.Decryption(cipher_text,key)
print('Message:',message)
print('Key:',key)
print('Ciphertext:',cipher_text)
print('Plaintext:',plain_text)
```

The output of the above code will be found as follows

Message: AES Encryption

Key: randomkey1234567

Ciphertext: 2E865FC450E6ABB53AEEBD65C9AE68D1

Plaintext: AES Encryption

CONCLUSION

The evolution of AES, from its initial development to its status as a globally recognized encryption standard, describes the collaborative efforts of the cryptographic community and the commitment to staying ahead of emerging threats. Its adaptability to different key lengths which provides organizations with the flexibility to choose the level of security that suits their needs, balancing computational superior and resistance to brute force attacks. Furthermore, AES's efficiency in terms of both speed and memory usage makes it an ideal choice for every sector of security. Its compatibility with hardware acceleration and software implementations ensures that it can be seamlessly integrated into a wide range of systems and applications. While AES cryptography has demonstrated its resilience against a variety of attacks over the years, it's crucial to acknowledge that the cryptographic landscape is continually evolving. As computational power increases and new attack vectors emerge, encryption techniques must adapt to maintain their effectiveness. Researchers and developers must remain careful, continually seeking improvements in AES and exploring new cryptographic methods to stay ahead of potential threats.

In summary, AES cryptography plays a pivotal role in safeguarding our digital world, enabling secure communication, data protection, and privacy. Its robustness, efficiency, and adaptability make it a cornerstone of information security, but it is essential to keep abreast of developments in cryptography to ensure its continued effectiveness in an ever-changing landscape of threats and technology.

REFERENCES

1. Paar, C. & Pelzl, J., Understanding Cryptography, Springer-Verlag Berlin Heidelberg, 2010
2. Rosen, K. H., Elementary Number Theory and Its Applications, Addison-Wesley Publishing Company, Amsterdam London Sydney, 1986
3. Trappe, W. & Washington, W. C., Introduction to Cryptography with Coding Theory, 2nd edn., Pearson, 2011
4. Toa Bi Irie Guy-Cedric, A Comparative Study on AES 128 Bit and AES 256 Bit, International

Journal of Scientific Research in Computer Science and Engineering, Vol: 6, pp 30-33, August (2018).

5. Clark, W. E., Elementary Number Theory, University of South Florida, 2002
6. Daemen, J. & Rijmen, V., The Design of Rijndael: The Advanced Encryption Standard (AES), 2nd edn., Springer-Verlag GmbH Germany, 2020
7. Shripal Rawal, Advanced Encryption Standard (AES) and It's Working, International Research Journal of Engineering and Technology (IRJET), Vo.: 3, p-ISSN: 2395-0072, August (2016).
8. Katz, J. & Lindell, Y., Introduction to Modern Cryptography, 3rd edn., CRC Press, 2021
9. https://www.tutorialspoint.com/cryptography/origin_of_ cryptography.htm
10. https://www.sutori.com/en/story/the-evolution-of-cryptography--dcUs
11. Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285)
12. V. R. Joan Daemen. AES Proposal: Rijndael, version 2, AES submission. 1999.
13. Joan Daemen, Steve Borg and Vincent Rijmen."The Design of Rijndael: AES The Advanced Encryption Standard", Springer, 2002.

APPENDIX

Mathematical Preliminaries

A1. Congruences

If $a$and $b$are two integers, then $a$is said to be congruent to $b$modulo $m$if and only if $a-b$is divisible by $m$and can be expressed as $a \equiv b \pmod{m}$. If $a \equiv b \pmod{m}$, then $a-b=kn$for some $k \in \mathbb{Z}$.

A2. Rings of Integers

The set of integer which form a ring is called the ring of integers. The integer ring $\mathbb{Z}_n$ modulo n perform two operations addition and multiplication for all x and y in $\mathbb{Z}_n$ as

$$x+y \equiv c \pmod{n}, c \in \mathbb{Z}_n$$
$$x \times y \equiv d \pmod{n}, d \in \mathbb{Z}_n$$

A3. Galois Field

A field which has finite numbers of elements and in which addition and multiplication operations can be run. It can be represented as $\mathrm{GF}(2^{\mathrm{n}})$ where n is a positive integer.

A4. Group

A nonempty set G with a binary operation ° on G is called a group if the following axioms are hold:

(i) $\mathrm{a(bc)=(ab)c}$ for all $\mathrm{a,b,c} \in \mathrm{G}$

(ii) There exist e $\in$ Gsuch that ea=a for all a$\in$ G

(iii) For every $\mathrm{a} \in \mathrm{G}$ there exists $\mathrm{a'} \in \mathrm{G}$ such that $\mathrm{a'a=e}$.

A5. Field

A group S is called a field if every element of S has an inverse.

A6. Prime Fields

A field is called a prime field if it has no proper subfield.

A7. Extension Fields,$\boldsymbol{GF}(\mathbf{2}^{\boldsymbol{m}})$

If the order of a finite field is not prime, then the field is called an extension field. Elements are not treated as numbers but as polynomials in an extension field if $f(x), g(x) \in GF(2^m)$, then addition and multiplication are performed as

$f(x) + g(x) = \sum_{i=0}^{m-1} c_i x^i$, $c_i = a_i + b_i$ mod 2 and $f(x). g(x)\ mod\ P(x)$ respectively, where $P(x) = \sum_{i=0}^{m} p_i x^i$, $p_i \in GF(2)$ be an irreducible polynomial.