Encryption and Advance Encryption Standards (AES)

Saumya Kanti Sarma
Pillai College of Arts, Commerce and Science, Panvel

ABSTRACT:
Encryption is the process of converting readable data (plain text) into unreadable format (ciphertext) to protect it from unauthorised access. This process ensures the confidentiality of sensitive information. The process of encryption and decryption relies on a randomly generated string value which are knows as KEYS which serves as the foundations for transforming data. These keys can be of two types: a private key or a public key.
Encryption can be further classified into two types: SYMMETRIC Encryption: Where same keys are for both encryption and decryption. ASYMMETRIC Encryption: Where different keys are used for encryption and decryption. In this paper, we will focus primarily on symmetric encryption. To be more specific on Advance Encryption Standards (AES) also known as Rijndael algorithm and explore its principles and evolution.

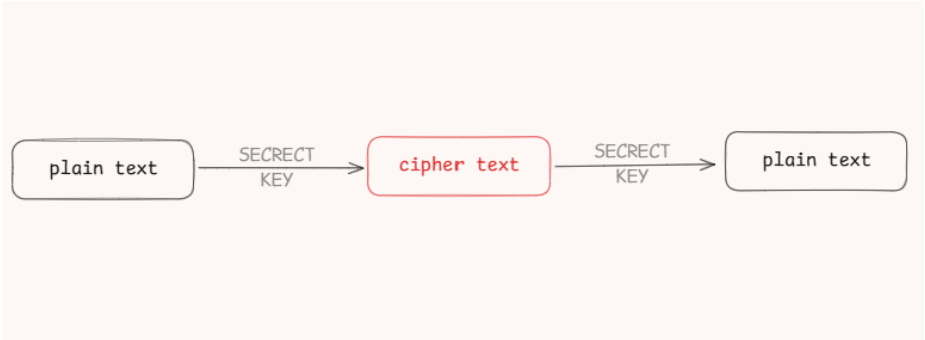

Figure: simple representation of symmetric encryption

KEYWORDS:
Encryption, cipher text, Advance Encryption Standards, AES, private key, public key,

INTRODUCTION:

A brief history of AES

Back in 1970s, the US government used an encryption system called Data Encryption Standard (DES). DES was very strong for it's time and was used to protect bank transactions, government data and many more. The main issue with DES was its key size, which was only 56-bit and by late 1990s, computer became a million time faster which made DES encryption weaker. Due to the small key size of DES algorithm, there were 2^{56} possible variations of keys (about 72 quadrillion that is $72x10^{18}$ possible pairs). This might sound a very large number but with modern computers of that time like Deep Crack (build by Electronic Frontier Foundation) and DESCHALL (distributed computer system specially build to crack DES algorithm) brute-forcing that many keys became practical. So, in 1997, NIST (National Institute of Status and Technology) launched an open worldwide competition to design a replacement for DES. 5 algorithms were shortlisted to become the new encryption standards and after 3 years of global testing. Finally in the year of 2001, Rijndael Algorithm; created by Joan Daemen and Vincent Rijmen was finalized to be called as the Advance Encryption Standard i.e. AES and till date is not any evidence to crake this algorithm.


Prof. J.J.C. Daemen


Vincent Rijmen

How AES Works?

Step 1: Text arrangements

AES has the ability to deal with three different key sizes such and that are 128, 192 and 256 bit and each of these ciphers has 128-bit block size. AES uses two common techniques to encrypt and decrypt data called as Substitution and Permutation Network (SPN). A SPN is number of mathematical operations that are carried out in a block cipher algorithm. AES algorithm generates a 128 bits (16 bytes) fixed plaintext block size. These 16 bytes are represented in 4x4 matrix. For texts longer than 16 bytes, AES algorithm breaks the text into chunks to fit into the size. For texts smaller then 16 Bytes, the algorithm adds some extra padding characters at the end of the texts and perform its operation.

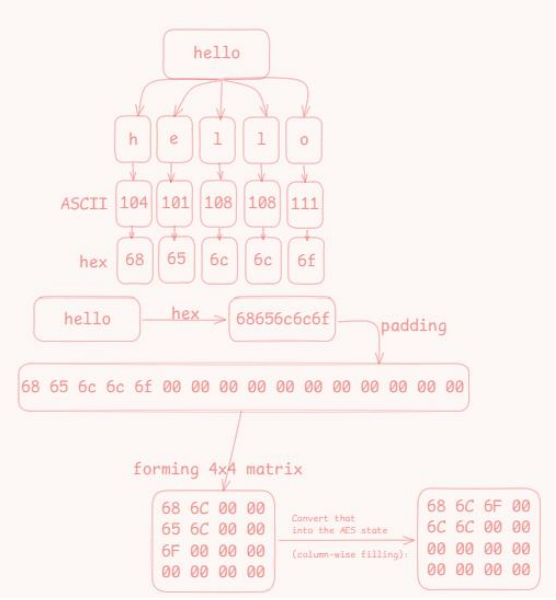

Fig: Diagram of text encoding process of the word Hello

Step 2: Key Expansion and encoding:

Another crucial feature in AES is the number of rounds. The number of rounds is one complete cycle of encryption operation applied to the data. For 128 bits long key AES has 10 rounds of operations, 12 rounds for 192 bits and 14 rounds for 256 bits long key. Each round takes the data and scrambles it more using 4 different techniques: SubBytes, ShiftRow, MixedColumn and AddRound Key.

Before the encryption rounds begin, AES performs a process known as Key Expansion or Key Scheduling. In this step, the original encryption key is expanded into a set of new keys called round keys, one for each round of the algorithm. This is done using a combination of substitution, rotation, and XOR operations. The first-round key is directly derived from the original key, while the remaining keys are generated from the previous ones. The process involves rotating the last column of the key, passing the bytes through the same S-box used in the SubBytes step, and then adding a special round constant (Rcon) to make each round unique. This ensures that even a small change in the original key results in completely different round keys, enhancing the overall security of the encryption.

Let's see a step-by-step example of AES Key Expansion using a 128-bit key, since that's the most common AES variant. Let's take an example key written in hexadecimal (each hex pair = 1 byte):

$Key = 2b7e151628aed2a6abf7158809cf4f3c$

We can divide this into 4 "words" (each word = 4 bytes):

$w0 = 2b7e1516$

$w1 = 28aed2a6$

$w2 = abf71588$

$w3 = 09cf4f3c$

AES-128 needs 11 round keys (w0–w43) in total (4 words per round × 11 rounds = 44 words).

So, from these 4 initial words, we'll generate 40 more. The keys are generated using the key expansion formula which is applied in each 4^{th} round. Each key generation process goes through rotation of bits, substitution of digits and other complex process. Luckly, the complex math behind generating complex keys

is not the main goal of this research paper. But, for better visual representation of the entire process follow this diagram.

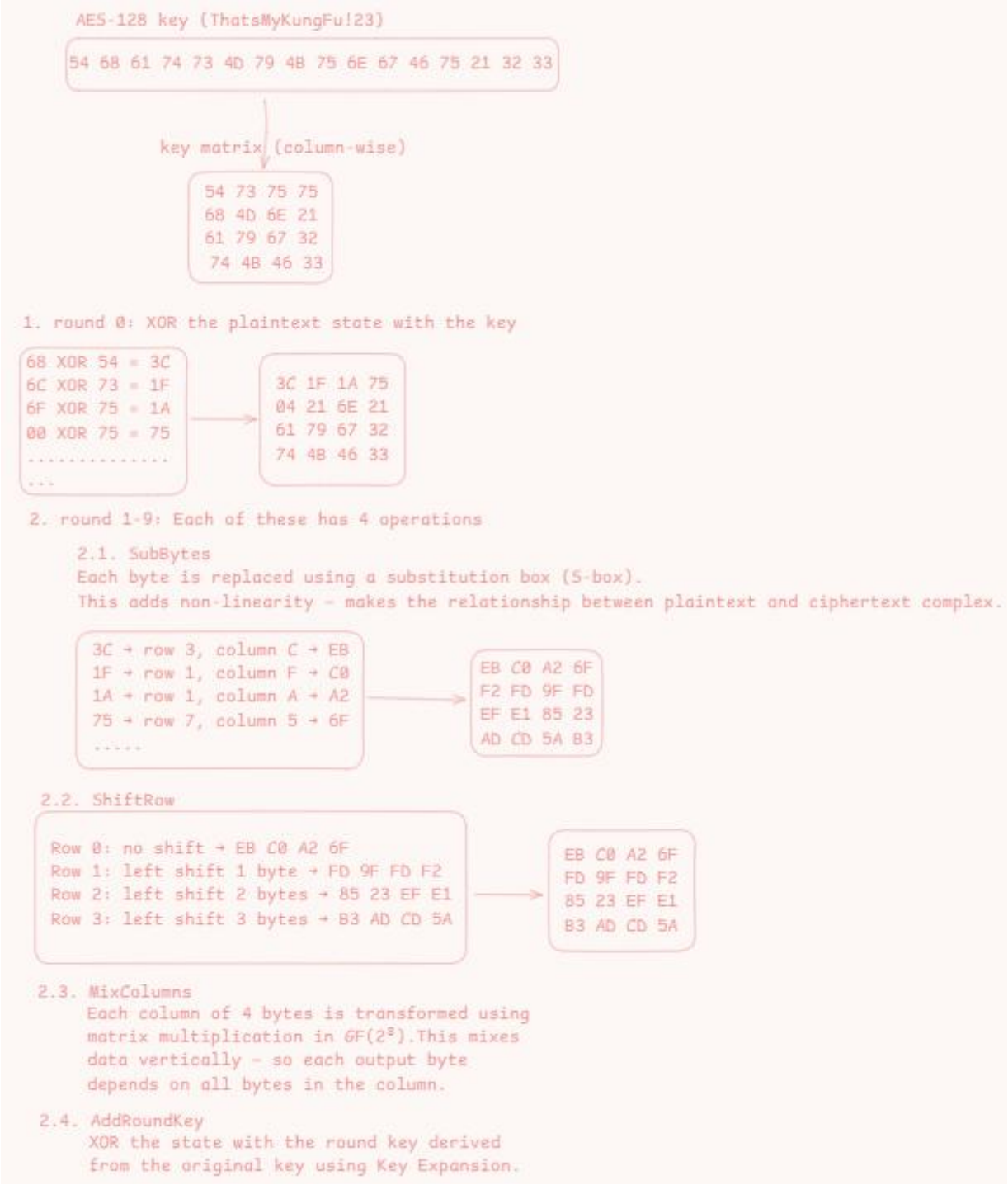

Fig: diagram of key expansion and encoding process

Step 3: Encryption

Once all the round keys are generated through key expansion, AES begins the actual encryption process. The plaintext is first divided into blocks of 128 bits (16 bytes) and arranged into a 4×4 state matrix. The first operation applied to this state is the AddRoundKey, where the plaintext block is combined with the initial round key using the XOR operation. After this, the data goes through several rounds of transformations each round consisting of SubBytes, ShiftRows, MixColumns, and AddRoundKey steps. The number of rounds depends on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. In the final round, the MixColumns step is omitted to simplify the process while still maintaining strong security. After all rounds are completed, the resulting 128-bit block becomes the ciphertext, which is the encrypted form of the original plaintext.

LITERATURE REVIEW:

Over the years, several studies and research papers have explored the development, implementation, and security features of the Advanced Encryption Standard (AES). Researchers have focused on its performance, efficiency, and resistance against various types of cryptographic attacks. According to Daemen and Rijmen, the algorithm was built to be simple in structure but strong in security, ensuring resistance to differential and linear cryptanalysis. Later studies demonstrated that AES performs efficiently on both hardware and software platforms, making it suitable for modern computing environments.

In a study by Stallings (2017), AES was compared with the earlier Data Encryption Standard (DES) and Triple DES (3DES), showing that AES offers stronger security with reduced computational cost. Similarly, P. Kumar et al. (2018) highlighted that AES provides faster encryption and decryption speeds with minimal resource usage, making it ideal for securing real-time communication and data transmission. Another research conducted by K. Singh et al. (2020) introduced hybrid models combining AES with other cryptographic techniques to enhance data confidentiality and integrity for cloud storage.

Recent developments also show that AES continues to evolve with optimization techniques for embedded systems and Internet of Things (IoT) devices. Studies in the field of parallel computing have shown how AES can be accelerated using GPU and FPGA architectures without compromising its security. From all these studies, it is evident that AES remains a robust, adaptable, and reliable encryption standard in both academic and industrial applications.

METHODOLOGY:

This research focuses on understanding the working principles and internal mechanisms of the Advanced Encryption Standard (AES) algorithm, particularly the AES-128 variant. The study uses a theoretical and experimental approach to analyse how plaintext is converted into ciphertext using symmetric key encryption.

1. Data Collection:
   Information was gathered from reliable online sources, including research articles, cryptography textbooks, and official AES documentation provided on research gate.
2. Algorithm Analysis:
   The AES encryption process was studied step-by-step, breaking it into core components such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. Each operation was analyzed to understand its contribution to data confusion and diffusion.
3. Key Expansion Study:
   The key scheduling algorithm was examined in detail to understand how round keys are derived from the original encryption key. A practical example using a 128-bit key was demonstrated to show the generation of round keys through substitution, rotation, and XOR operations.
4. Simulation and Visualization:
   Conceptual examples were illustrated to demonstrate how AES performs encryption on blocks of plaintext. Diagrams and tables were used to represent the 4×4 state matrix transformations during each round.
5. Evaluation:
   The study compares AES with its predecessor DES in terms of key size, performance, and resistance to brute-force attacks. This helps highlight the reasons AES became the global encryption standard.

The methodology ensures a clear understanding of both the theoretical foundation and practical implementation of AES encryption.

REFERANCE:

1. https://www.geeksforgeeks.org/ethical-hacking/what-is-a-symmetric-encryption/
2. https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data
3. https://www.researchgate.net/publication/327410017_A_Secure_and_High-Capacity_Data-Hiding_Method_Using_Compression_Encryption_and_Optimized_Pixel_Value_Differencing
4. https://www.researchgate.net/publication/379871849_A_Review_of_Encryption_and_Decryption_of_Text_Using_the_AES_Algorithm?_ftx_i=%7B%22rId%22%3A%22f6b9cc11-9446-4bda-b0d6-8ae7bd9e70ea%22%2C%22tId%22%3A%22PB%3A379871849%22%2C%22p%22%3A0%2C%22iT%22%3A%22click-publication-title%22%2C%22mV%22%3A%222.324.0%22%2C%22mN%22%3A%22FTXAckModel-rt%22%2C%22rSc%22%3A%22similar_user_publications_by_recent_publication_interactions%22%2C%22meta%22%3A%7B%22topMessageLinks%22%3A%22%22%7D%7D&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6ImhvbWUiLCJwYWdlIjoiaG9tZSIsInBvc2l0aW9uIjoicGFnZUNvbnRlbnQifX0
5. https://www.researchgate.net/publication/376254681_A_Lightweight_Image_Encryption_Scheme_Using_DNA_Coding_and_Chaos?_ftx_i=%7B%22rId%22%3A%220b37220c-6bbc-4640-940b-3c5420be65f7%22%2C%22tId%22%3A%22PB%3A376254681%22%2C%22p%22%3A1%2C%22iT%22%3A%22click-publication-title%22%2C%22mV%22%3A%222.324.0%22%2C%22mN%22%3A%22FTXAckModel-rt%22%2C%22rSc%22%3A%22TwoTowers%22%2C%22meta%22%3A%7B%22topMessageLinks%22%3A%22%22%7D%7D&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6ImhvbWUiLCJwYWdlIjoiaG9tZSIsInBvc2l0aW9uIjoicGFnZUNvbnRlbnQifX0

CONCLUTION:

The Advanced Encryption Standard (AES) has proven to be one of the most reliable and efficient encryption algorithms of the modern era. Its strong mathematical foundation, flexible key lengths, and resistance to known cryptographic attacks make it a global standard for securing sensitive data. Unlike its predecessor DES, which suffered from small key sizes and vulnerability to brute-force attacks, AES offers a much larger key space and a more complex structure, making it practically unbreakable with current computational power.

Through this paper, we have explored how AES functions internally from key expansion to the final round of encryption and how each step contributes to the overall security of the system. The study shows that AES's Substitution–Permutation Network (SPN) design provides both confusion and diffusion, two fundamental properties of strong cryptography. Furthermore, the continued trust and adoption of AES in applications such as secure communications, online banking, and data storage demonstrate its significance in information security.

In conclusion, AES not only replaced DES as a more secure standard but also set a new benchmark for encryption systems worldwide. As computing technologies evolve, AES remains the foundation for many modern encryption protocols, proving its long-term strength, adaptability, and importance in maintaining data confidentiality.