Encryption and Advance Encryption Standards

A deep understanding of AES algorithm and it’s encryption process

By: Saumya Kanti Sarma
FY-BCA-B
Roll: 2570

What is Encryption?

Encryption is the process of converting **readable data (plain text)** into an **unreadable form (cipher text)** to protect it from unauthorized access.

Example:

Types of encryption

1. **Symmetric Encryption:** The same key is used for both encryption and decryption.
2. **Asymmetric Encryption:** Uses two different keys: a public key for encryption and a private key for decryption.
3. **Hybrid Encryption:** Modern systems use both symmetric and asymmetric encryption.

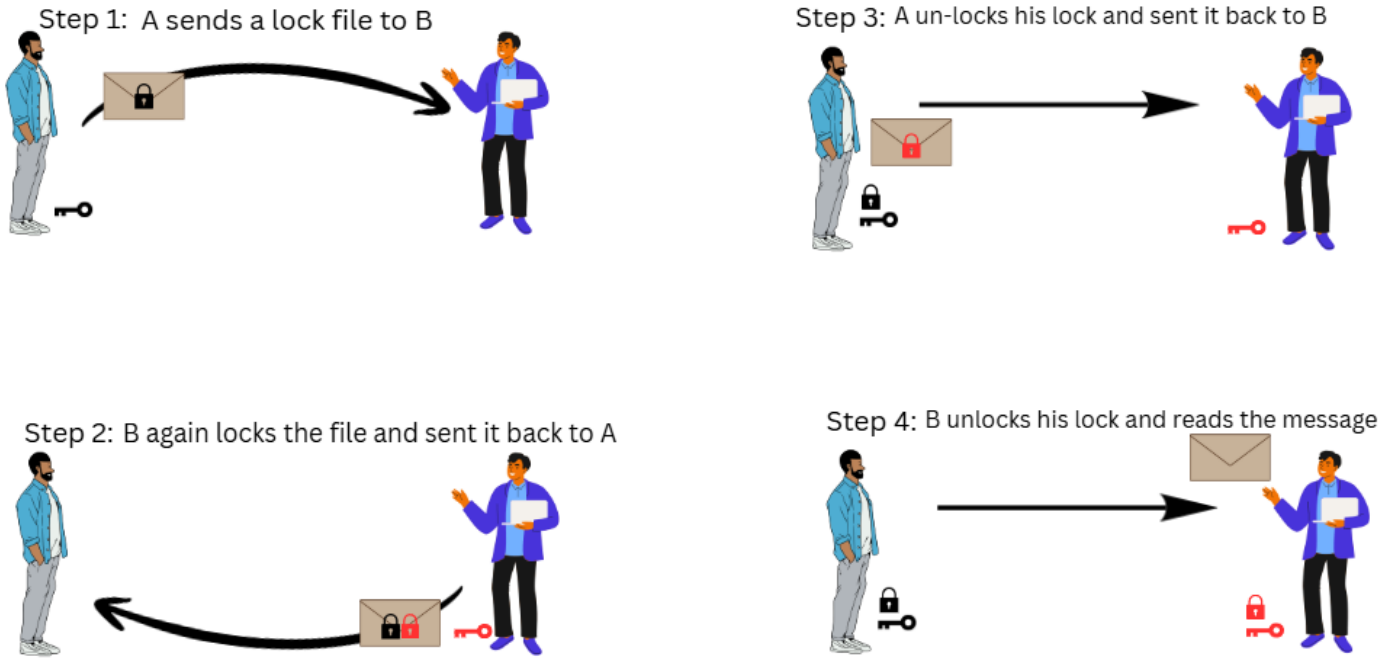
Example: Symmetric Encryption

- A simple traditional lock and key can be the best example of symmetric encryption.
- Here both locking (encrypting) and unlocking (decrypting) is done by the use of same key.

Types of encryption

1. **Symmetric Encryption:** The same key is used for both encryption and decryption.
2. **Asymmetric Encryption:** Uses two different keys: a public key for encryption and a private key for decryption.
3. **Hybrid Encryption:** Modern systems use both symmetric and asymmetric encryption.

Example: Asymmetric Encryption



What is Advance Encryption Standard?

- The Advanced Encryption Standard (AES) is symmetric encryption algorithm used to protect data by converting readable information into an unreadable form. It uses the same key for both encryption and decryption.
- AES is also known as **Rijndael Algorithm,** which was the original name of the algorithm
- AES was developed by two Belgian cryptographers, **Joan Daemen** and **Vincent Rijmen**, and was adopted as a standard by the National Institute of Standards and Technology (NIST) in 2001.

Prof. Joan Daemen

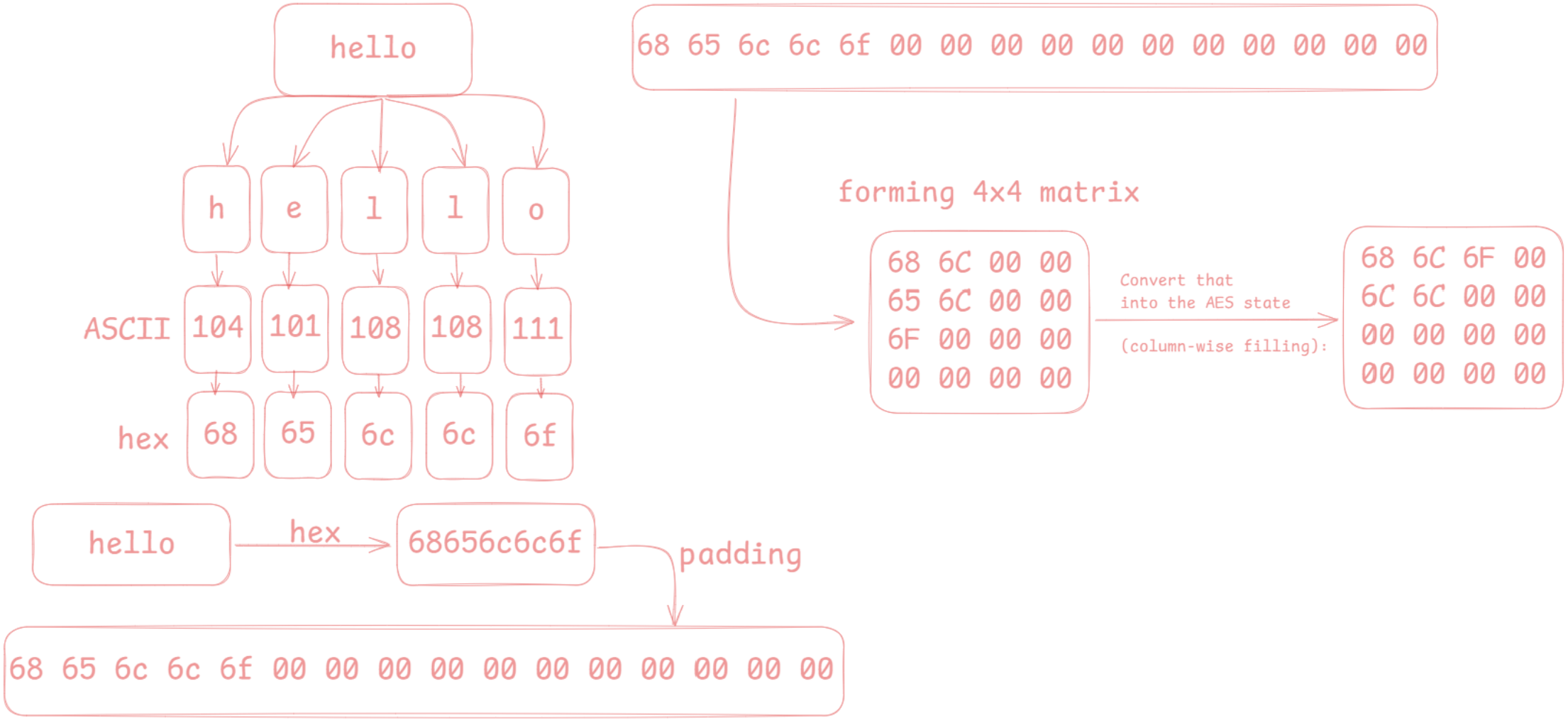
Prof. Vincent Rijmen

History of AES

- Back in 1970s, the US government used an encryption system called DES.
- The main issue with DES was using a 56-bit key and by late 1990s, computer became fast which made DES encryption weaker.
- So, in 1997, NIST launched an open worldwide competition to design a replacement for DES.
- 5 algorithms were shortlisted to become the new encryption standards.
- In 2001, Rijndael Algorithm was finalized to be called as the **Advance Encryption Standard.**
- Till date there is not a single evidence of cracking this algorithm.

How AES Works?

STEP 01: Text decoding and padding



How AES Works?

STEP 02: Key Splitting

AES-128 key (ThatsMyKungFu!23)

```
54 68 61 74 73 4D 79 4B 75 6E 67 46 75 21 32 33
```

key matrix (column-wise)

```
54 73 75 75
68 4D 6E 21
61 79 67 32
74 4B 46 33
```

1. round 0: XOR the plaintext state with the key

```
68 XOR 54 = 3C
6C XOR 73 = 1F
6F XOR 75 = 1A
00 XOR 75 = 75
..............
...
```

→

```
3C 1F 1A 75
04 21 6E 21
61 79 67 32
74 4B 46 33
```

2. round 1-9: Each of these has 4 operations

2.1. SubBytes

Each byte is replaced using a substitution box (S-box).
This adds non-linearity – makes the relationship between plaintext and ciphertext complex.

```
3C → row 3, column C → EB
1F → row 1, column F → C0
1A → row 1, column A → A2
75 → row 7, column 5 → 6F
.....
```

→

```
EB C0 A2 6F
F2 FD 9F FD
EF E1 85 23
AD CD 5A B3
```

2.2. ShiftRow

```
Row 0: no shift → EB C0 A2 6F
Row 1: left shift 1 byte → FD 9F FD F2
Row 2: left shift 2 bytes → 85 23 EF E1
Row 3: left shift 3 bytes → B3 AD CD 5A
```

→

```
EB C0 A2 6F
FD 9F FD F2
85 23 EF E1
B3 AD CD 5A
```

How AES Works?

STEP 02: Key Splitting

2.3. MixColumns
Each column of 4 bytes is transformed using matrix multiplication in $GF(2^8)$. This mixes data vertically - so each output byte depends on all bytes in the column.

2.4. AddRoundKey
XOR the state with the round key derived from the original key using Key Expansion.

e4cfa39b4ec88890f4e76fd92a08ec6b

How AES Works?

e4cfa39b4ec88890f4e76fd92a08ec6b

This is our encrypted text

Challenges for AES algorithm

- Although AES is very secure, its performance can be affected on low-power or small devices due to complex mathematical operations.
- If the encryption key is weak, reused, or exposed, the entire security system can be compromised.
- AES is vulnerable to side-channel attacks, such as timing or power analysis, if the implementation is not properly secured.
- Managing and distributing encryption keys safely remains a major challenge in large systems.
- Quantum computing, in the future, may pose a potential threat to AES if not upgraded to quantum-resistant standards.

Conclusion

The Advanced Encryption Standard (AES) is one of the most reliable and widely used encryption algorithms in the world. It provides a high level of security, efficiency, and flexibility for protecting sensitive data. Despite some implementation and key management challenges, AES remains the global standard for securing digital communication and information. It is expected to continue playing a vital role in data protection until more advanced encryption methods are developed.