**AES (Advanced Encryption Standard)**

* Rajnish

2101CS18

AES is a symmetric key encryption algorithm used to secure data. It works with 128, 192, or 256-bit keys and processes data in 128-bit blocks.

**Working Mechanism: Step-by-Step**

**Input and Key Preparation**

* **Input Block:** The plaintext is divided into 128-bit (16-byte) blocks.
* **Key Expansion:** The key is expanded into multiple round keys using a process called the **Key Schedule.** The number of round keys depends on the key length:
  + 10 rounds for 128-bit keys.
  + 12 rounds for 192-bit keys.
  + 14 rounds for 256-bit keys.

**Initial Round**

The plaintext is XORed with the first round key:

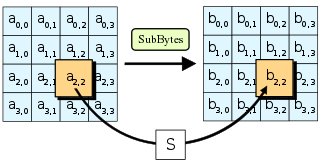
* **AddRoundKey:** Each byte of the plaintext is XORed with the corresponding byte of the round key.

**Main Rounds**

Each main round consists of the following four operations:

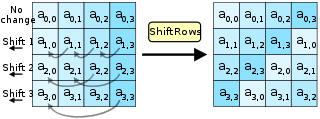
**a. SubBytes (Byte Substitution)**

* Each byte in the 4x4 state matrix is replaced using a substitution box (S-Box), which is a precomputed lookup table designed to provide non-linearity and resistance to attacks.



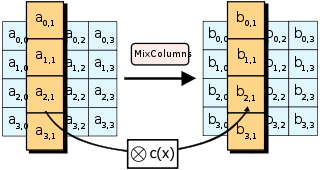
**b. ShiftRows**

* Rows of the state matrix are shifted cyclically:
  + Row 0: No shift.
  + Row 1: 1-byte left shift.
  + Row 2: 2-byte left shift.
  + Row 3: 3-byte left shift.



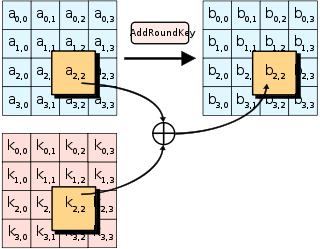
**c. MixColumns**

* Each column of the state matrix is transformed using a mathematical function that mixes the bytes to increase diffusion.  
  *(Note: The MixColumns step is omitted in the final round.)*



**d. AddRoundKey**

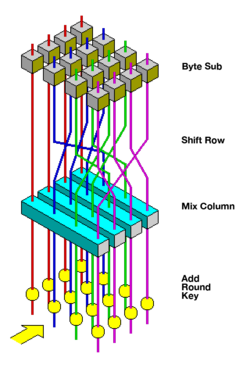
* The current state is XORed with the corresponding round key.



**Final Round**

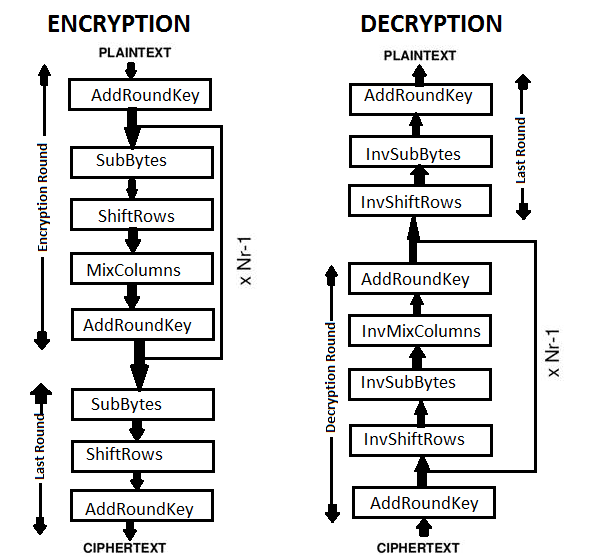
The final round excludes the **MixColumns** step and only performs:

1. **SubBytes**
2. **ShiftRows**
3. **AddRoundKey**



**Output**

After the final round, the state matrix is transformed into a ciphertext block. This process repeats for all 128-bit blocks of plaintext.



**Advantages of AES**

1. **Security:**
   * AES is resistant to known cryptographic attacks like differential and linear cryptanalysis.
   * Larger key sizes (192-bit, 256-bit) provide stronger security.
2. **Efficiency:**
   * AES is fast and efficient in both hardware and software implementations.
   * It is widely used in various applications, including TLS/SSL, VPNs, and file encryption.
3. **Standardized:**
   * AES is a globally recognized encryption standard adopted by the U.S. government (FIPS PUB 197).
4. **Flexibility:**
   * AES supports multiple key lengths (128, 192, 256 bits), allowing scalability for different security requirements.
5. **Lightweight:**
   * Suitable for resource-constrained devices due to its computational efficiency.

**Drawbacks of AES**

1. **Symmetric Key Distribution:**
   * Both the sender and receiver must securely exchange the secret key, which can be challenging without a secure channel.
2. **Performance with Large Data:**
   * Encrypting/decrypting large volumes of data can introduce latency.
3. **Quantum Vulnerability:**
   * Although not broken, AES might be less secure against quantum attacks (Grover's algorithm can reduce effective key strength).
4. **Single Point of Failure:**
   * If the secret key is compromised, the entire communication is vulnerable.
5. **Block Size Limitation:**
   * AES operates on fixed 128-bit blocks, which may require padding schemes or block chaining modes (e.g., CBC, GCM) to handle data of varying lengths securely.

***PERFORMANCE:***  
  
