

Devanshu Surana

PC-23, Panel C

1032210755

ICS Lab A3

P4
30/11/23

FAQ's

1. What is S-AES algorithm and how it is different from AES algorithm?

Ans. Simplified AES (S-AES) is a reduced-round version of the AES algorithm. S-AES is designed for educational purposes and to help students and beginners understand the basic principles of AES encryption without the complexity of the full AES algo. S-AES typically uses a smaller number of rounds and a smaller key size compared to the standard AES.

2. Explain Key generation in S-AES.

Ans. Key generation in S-AES:

1. Key Selection: In S-AES, we have to select shortest key often 8-bits in length. This key will be used for both encryption and decryption.
2. Key Expansion: Key expansion is a critical process that generates round keys for each round of encryption from the original key.
3. Encryption Key: The selected short key is used directly for the initial round of encryption in S-AES.
4. Decryption Key: We can use the same short key for decryption as well since the algorithm is symmetric.

3. Explain Encryption in S-AES.

- Ans.
1. Initial Round: The plaintext is combined with the first part of the key using simple bitwise XOR operation.
 2. i) Substitution: Each byte of the data is substituted with a corresponding value from a fixed S-box.
ii) Permutation: The bytes are rearranged.
 3. In the last round, the remaining part of the key is combined with the data using another XOR operation.
 4. Output: The result of the final round is the cipher text, which represents the encrypted data.

4. Explain Decryption in S-AES.

- Ans.
1. Initial Round: The cipher text is combined with the last part of the key using a XOR operation to reverse the final round of encryption.
 2. The main rounds of decryption reverse the permutation and substitution operations from the encryption process.
 3. The decryption process concludes with the reverse of the initial round. The remaining part of the key is XORed with the key data to obtain the original plaintext.
The result of the final round of decryption should be the original plaintext, which matches the input data before encryption.

✓