Name : Tejas Redkar
PRN : 1032210937
Panel - C
Roll No : PC-44

A
1/12/23

ICS Lab A3

* FAQ's

Q1) What is S-AES algorithm & 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 & to help students & beginners understand the basic principles of AES encryption without the complexity of the full AES Algorithm.

S-AES typically uses a smaller no. of rounds & a smaller key size compared to the standard AES.

Q2) 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 & 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 algo is symmetric

Q3) 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 ciphertext which represents the encrypted data.

Q4) Explain Decryption in S-AES

Ans 1) Initial Round : The ciphertext 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 & substitution operations from the encryption process.

3) The decryption process concludes ~~th~~ with the reverse of the initial round.

A

1/12/23