Jessica Braganza
BE comp 2
F17112151

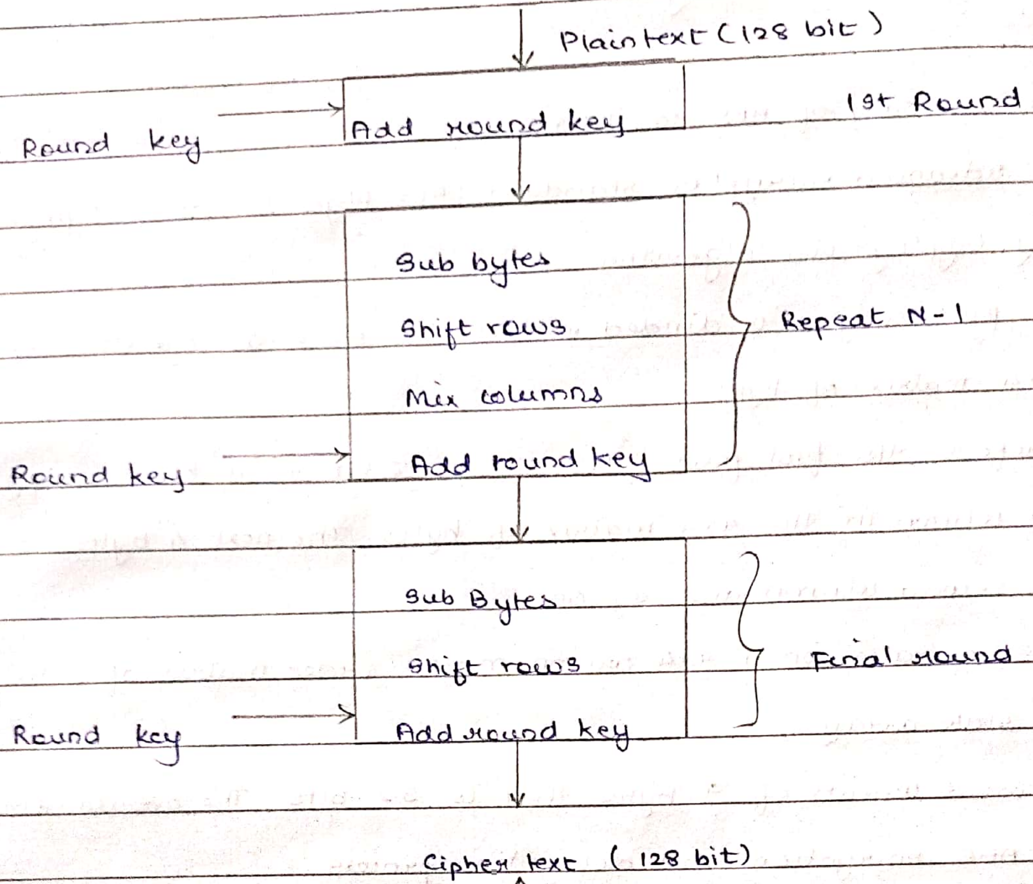
PAGE NO :
DATE :

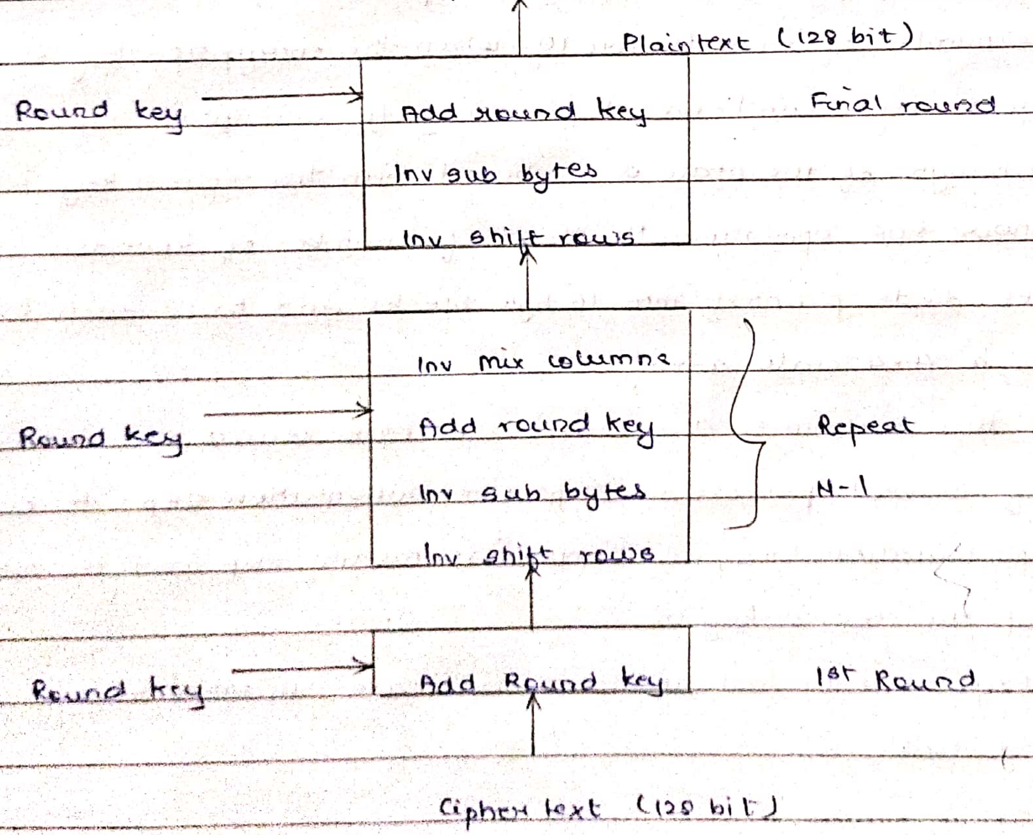
ICS Assignment 4

1) Explain working of AES in detail.

Ans. - The advanced encryption standard (AES Algorithm) is a symmetric key cryptographic algorithm.

- The plaintext given is divided into 128 bit block as consisting of a 4x4 matrix of bytes.
- Therefore, the first four bytes of a 128 bit input block occupy the first column in the 4x4 matrix of bytes. The next 4 bytes occupy the second column and so on.
- AES operates on a 4x4 column major order matrix of bytes called as state array.
- A word consists of 4 bytes that is 32 bits. The overall structure of AES encryption and decryption process.
- The number of rounds are 10 when the encryption key is 128 bits.
- Before any round-based processing for encryption can begin, each byte of the state is combined with the round key using bitwise XOR operation. Nr stands for number of rounds.
- AES divide plaintext into 16 byte blocks and treats each block as a 4x4 state array.
- It then performs 4 operations in each round and consists of several processing steps like substitution step. A row-wise permutation step, a column-wise mixing step and the addition of the round key.
- Except for the last round in each case, all other rounds are identical.





2) Explain operation in key expansion process in AES algorithm

Ans. The AES key expansion algorithm takes input a 4 byte (16 byte) key and produces a linear array of 44 words (176 bytes).

- This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher.
- The key is copied into the first four words ~~by~~ of the expanded key.
- The remainder of the expanded key is filled in 4 words at a time.
- Each added word w[i] depends on the immediately preceding word w[i-1], and the word four positions back, w[i-4] in three out of four cases a simple XOR is used.
- For a word whose position in the w array is a multiple of 4, a more complex function is used.

3) Differentiate AES and DES algorithm.

	DES	AES
i)	It takes 64 bit plaintext as a input and creates 64 bit ciphertext	It allows the data length of 192, 128 and 256 bits.
ii)	In DES plaintext message is divided into size 64 bit block each and encrypted using 56 bit key at the initial level.	AES divide plaintext into 16 byte blocks as a 4x4 state array and supporting 3 different key lengths 128, 192 and 256 bits
iii)	Different versions of DES are double DES and triple DES is added	AES doesn't have any future version.
iv)	DES doesn't use Mix column, shift rows method during encryption and decryption process	AES uses Mix column, shift rows method during encryption and decryption process.

v)	DES, double DES and triple DES are vulnerable to brute force attacks.	AES also are vulnerable to brute force attacks.