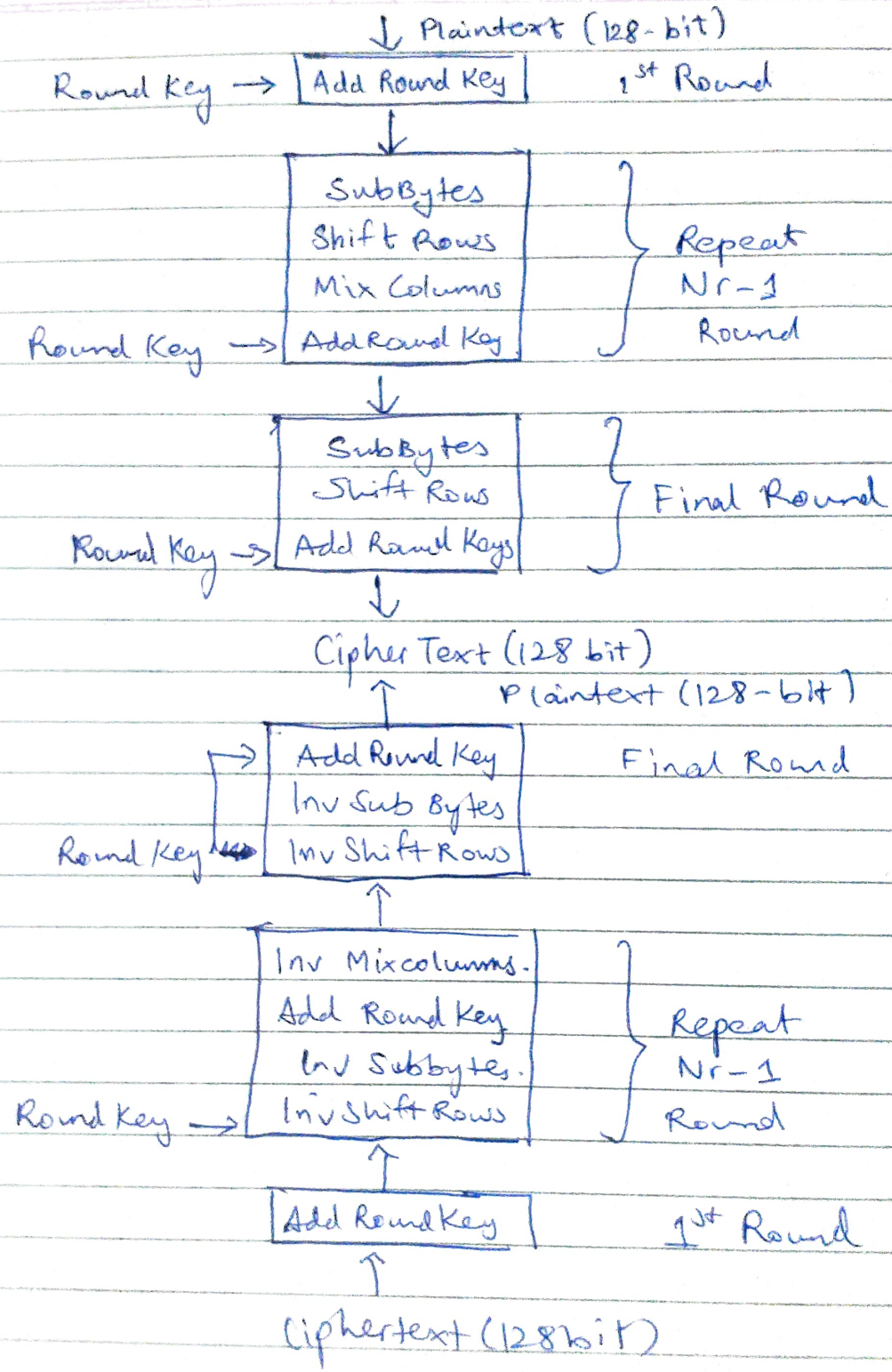
Sudesh Pawar
F17111037
BE Comp A

ICS A4

1) Explain working of AES in detail.

→ The Advanced Encryption Standard (AES Algorithm) is a symmetric key cryptographic algorithm.

- The plaintext given is divided into 128-bit block as consisting of 4x4 matrix of bytes.
- Therefore, the first 4 bytes of a 128-bit input block occupy the first column in 4x4 matrix of bytes. Next 4 bytes occupy second column & so on
- AES operates on 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 & decryption process.
- The no. of rounds are 10, for the case when the encryption key is 128 bits long.
- Before any round based processing for encryption can begin each byte of that state combined with the round key using bitwise XOR operation, Nr stands for no. of rounds.
- AES divide plaintext into 16 bytes blocks & treats each block as 4x4 state array.
- It then performs 4 operations in each round consists of several processing steps like substitution step, a row-wise permutation step, a column-wise mixing step & the addition of the round key.
- Except for last round in each case, all other rounds are identical


Plaintext (128-bit)
Round Key
Add Round Key
1st Round
SubBytes
Shift Rows
Mix Columns
Add Round Key
Repeat Nr-1 Round
Round Key
SubBytes
Shift Rows
Add Round Keys
Final Round
Round Key
Cipher Text (128 bit)
Plaintext (128-bit)
Add Round Key
Inv Sub Bytes
Inv Shift Rows
Final Round
Round Key
Inv Mixcolumns.
Add Round Key
Inv Subbytes.
Inv Shift Rows
Repeat Nr-1 Round
Round Key
Add Round Key
1st Round
Ciphertext (128bit)

2) Explain operation in key expansion process in AES algorithm.

→ The AES key expansion algorithm takes as input, a 4-byte (16 byte) key & produces a linear array of 44 words (176 bytes). This is sufficient to provide a 4-word round key for the initial AddRoundKey stage & each of the 10 rounds of the cipher. The key is copied into the first four words of the expanded key is filled in 4 words at a time. Each added word w[i] depends on the immediately preceding words w[i-1], & the word four positions back, w[i-4] in 3 out of 4 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 between AES / DES Algorithm.

	DES	AES
i)	It takes 64 bit plaintext as an input & creates 64 bit ciphertext	It allows data length of 192, 128 & 256 bits
ii)	In DES plaintext message is divided into size 64 bits block each & encrypted using 56-bit key at initial level.	AES divide plaintext into 16 byte blocks & treats each block as a 4x4 state array & supporting 3 different lengths.
iii)	Different versions of DES are double DES/Triple DES is added	AES doesn't have a future version

iv) DES doesn't use Mix Column Shift rows method during encryption & decryption process.

v) DES, double DES & Triple DES are vulnerable to brute force attacks.

iv) AES uses mix column, shift rows method during encryption & decryption process.

v) AES also are vulnerable to brute force attacks