Assignment No - 3

Aim - Write a Java / C / C++ / python program to implement AES Algorithm.

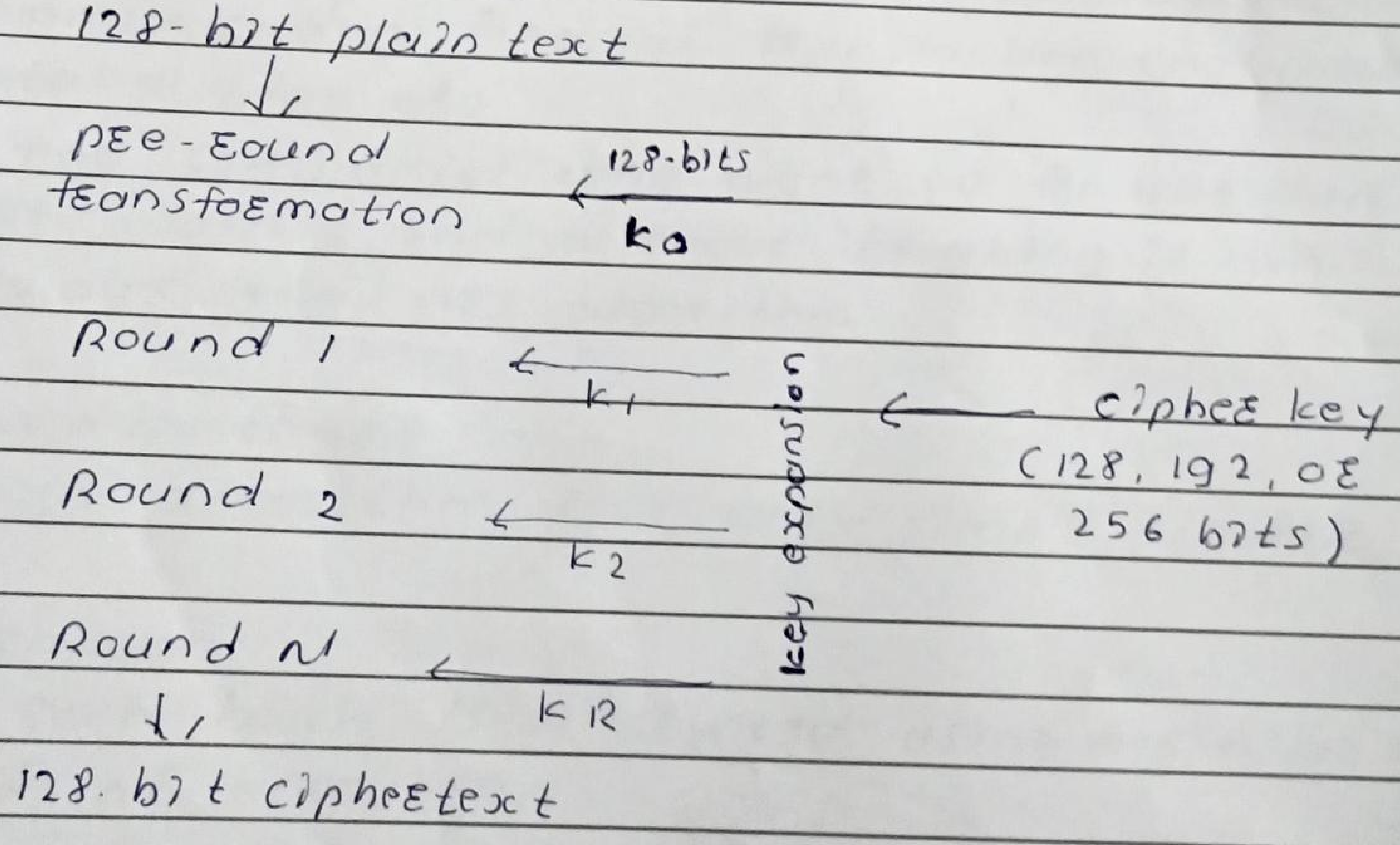
Theory - The most popular and widely used symmetric encryption algorithm is advanced encryption standerd (AES). AES is 6 times faster than the triple DES.

Operation of AES -

- AES is an iterative rather than feistel cipher. It is based on substitution - permutation Network. It includes a series of linked operations Some of which involve replacing inputs by specific outputs involve and others involve shuffling bits around (permutations)
- AES performs all its computations on bytes rather bits Hence AES treats the 128 bits of a plaintext block as 16 bytes.
- The AES is a symmetric - keys block cipher published by the National Institute of standard and technology.
- AES was created for the U.S government with additional voluntary free use in Public or private commercial or non-commercial programs that provide encryption services
- However nongovernmental organizations choosin to use AES are subject to limitation created by U.S export control. AES is found at least

six time faster than triple DES

- Every version uses different key size which can be 128, 192, or 256 bits depending on the number of rounds but the round keys are always 128 bits. AES uses 10 rounds keys are always 128 bits keys, 12 rounds for 192 bit keys and 14 around for 256-bit keys. It can be observed from the following
- These 16 bytes are arranged in four columns and four rows for processing as a matrix It comprises of a series of linked operations some of which involve replacing inputs by specific outputs (substitution) and others involve shuffling bit around.



Date : 12 / 1 /20

Encryption process.

At encryption site, each round comprises of four transformations that are invertible the transformation are

1] SubBytes (substitution)
2] Shift Rows (permutation)
3] Mix columns (mixing)
4] Add Round keys (key adding)

Advantages.

- The encrypted data cannot be decrypted without a valid secrete key.
- AES is the most common security algorithm used world wide for various purpose like wireless communication finacial transfaction encrypted data storage etc.
- The companies who want to transfer their data safetly and without breaking it can always the AES algorithm.

Disadvantages.

AES algorithm uses very simple algebric formula.

- Each block is encrypted using a similar kind of encryption.
- AES can be difficult to implement with the software.

Algorithm -

1. Derive the set of round keys from the cipher key
2. Initialize the state array with the block data
3. Add the initial round key to the starting state array.
4. perform nine rounds of state manipulation
5. perform the length and final round of the state manipulation
6. Copy the final state array as the encrypted data.
7. Stop.

Conclusion.

We learned how to encrypt and decrypt input data like strings files objects and password based data using the AES algorithm in Java.