CNS
Assignment-2

1812401160001
Vishwas Acharya

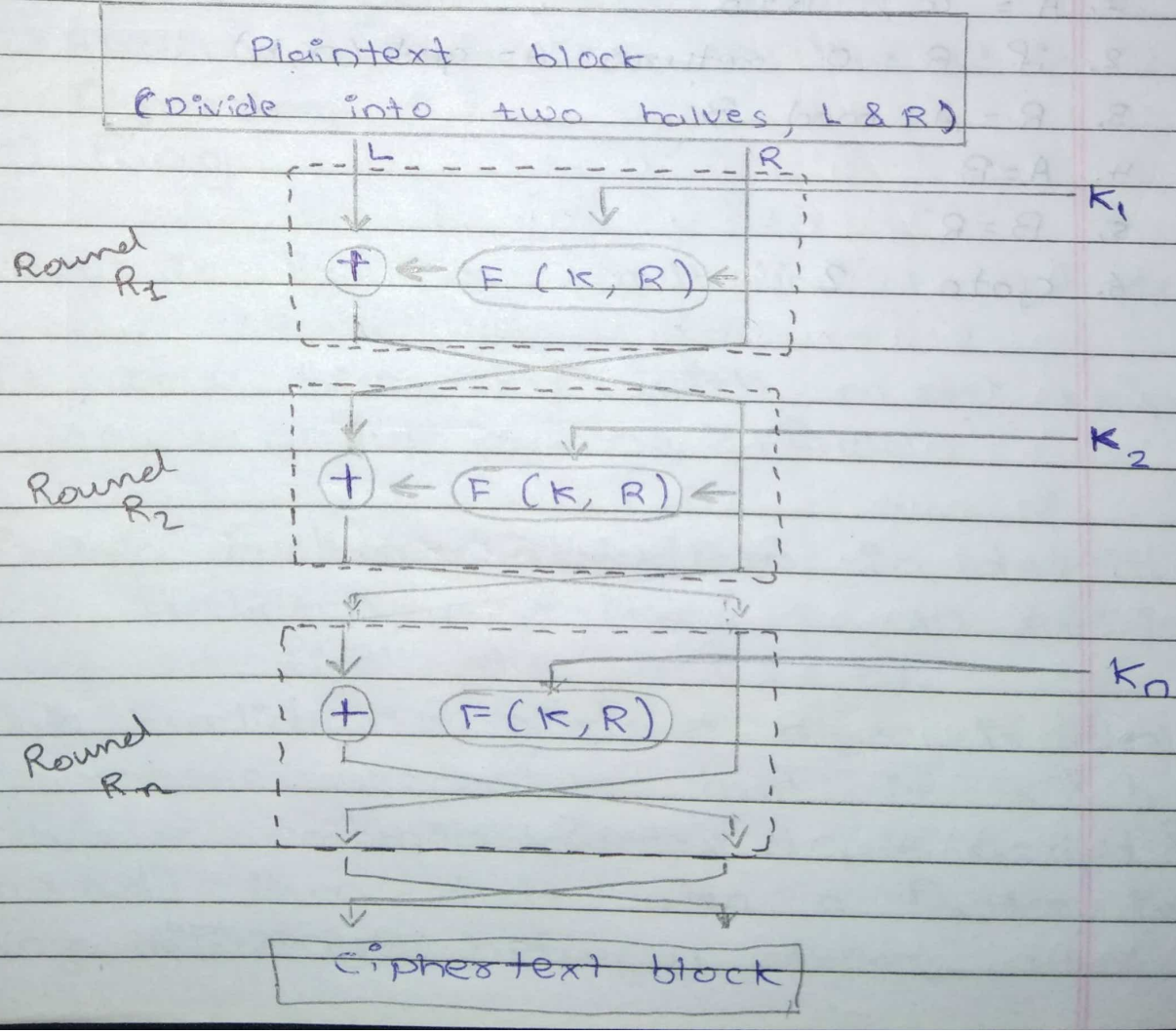
Page No.: 1
Date: / /

1) Write note on feistel cipher with figure.

Ans :- Feistel Cipher is not a specific of block cipher.

- It is a design model from which many different block ciphers are derived.
- DES is just one example of a Feistel Cipher.
- A cryptographic system based on Feistel Cipher structure uses the same algorithm for both encryption and decryption.

- Figure:



1. Encryption Process:

↳ The encryption process uses the fiestel structure consisting multiple rounds of processing of the plaintext, each round consisting of a substitution step followed by a permutation step.

2. Decryption Process:

↳ It's same as encryption process with the only difference is that the subkeys used in encryption are used in reverse order.

3. Numbers of Rounds:

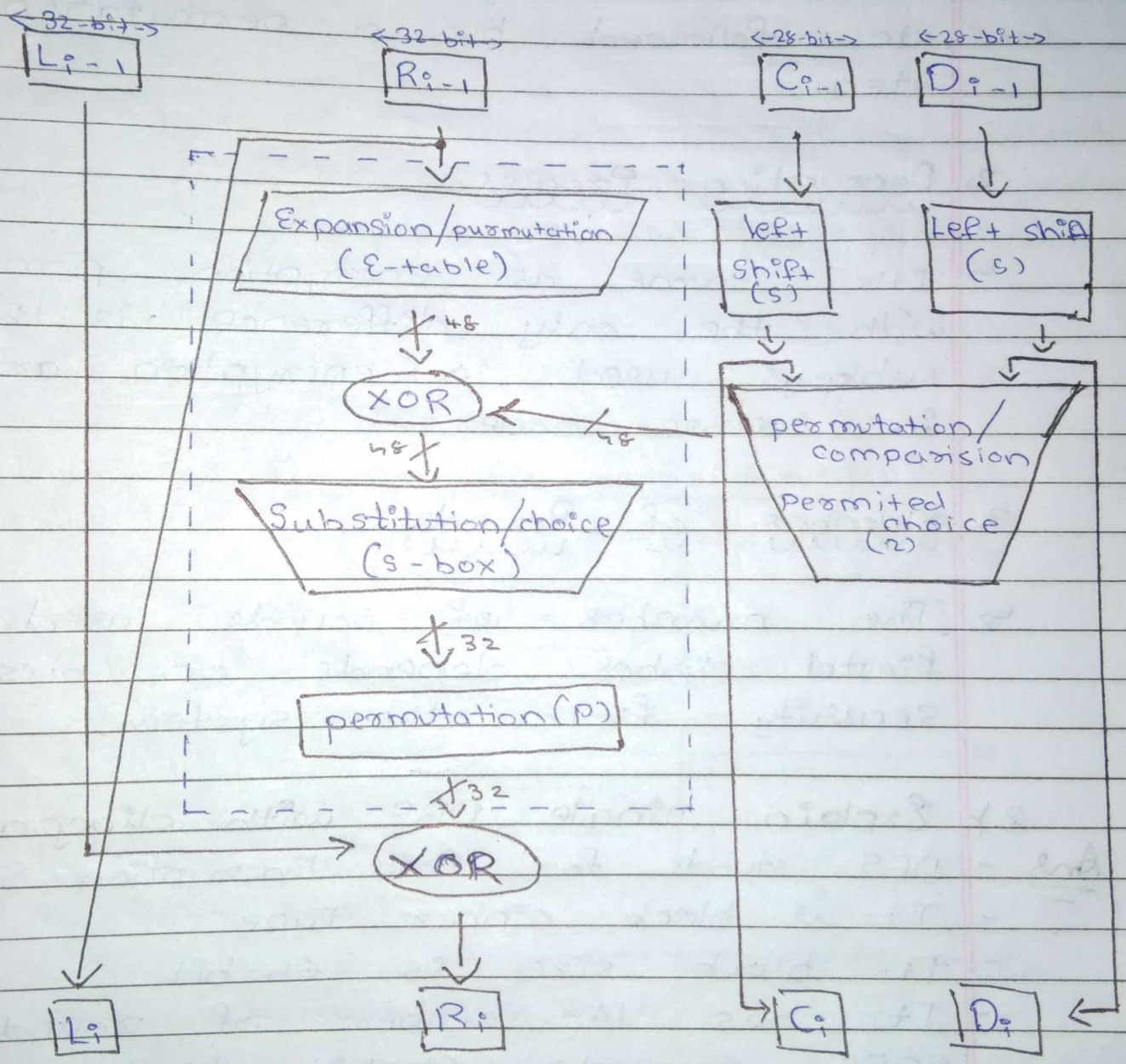
↳ The number of rounds used in fiestel cipher depends on desired security from the system.

2Y Explain single DES with diagram.

Ans
- DES stands for Data Encryption Satandard.
- It is block cipher Type.
- Its block size is 64-bit.
- It has 16 number of rounds.
- SDES encrypts 64-bit blocks using a 56-bit key and produces a 64-bit cipher text.
- DES is based on the two fundamental

attributes of cryptography
↳ substitution (aka confusion)
↳ Transposition (aka diffusion)

- Figure:



3) Write about AES with example.

Ans - AES stands for Advanced Encryption Standard.
- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the AES.
- It is found at least six time faster than triple DES.
- A replacement for DES was needed as its key size was too small.
- With increasing computing power, it was considered vulnerable against exhaustive key search attack.
- Triple DES was designed to overcome this drawback but it was found slow.

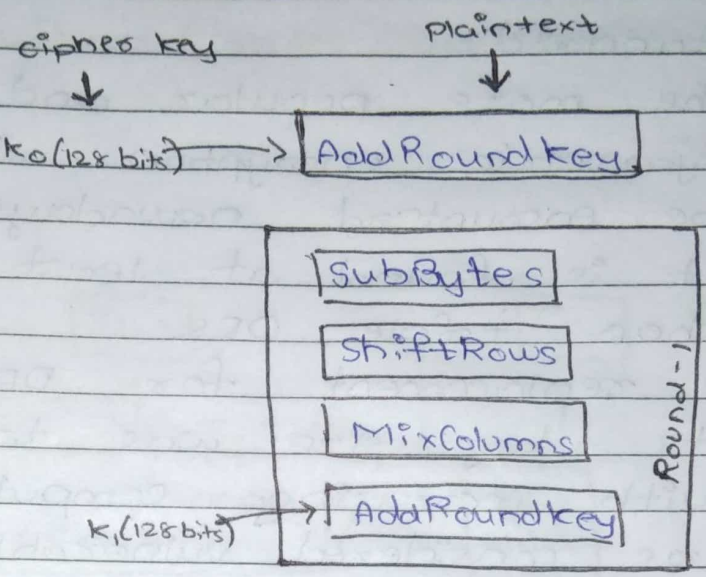
• Features:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details.
- Software implementable in C and Java

• Encryption Process

↳ Here, we ristrict to description of a typical round of AES encryption.
↳ Each round comprise of four sub-processes.

- The first round process is depicted below-



- Decryption Process

↳ The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

↳ Each Round consists of the four processes conducted in the reverse order

  ↳ Add round key
  ↳ Mix columns
  ↳ Shift rows
  ↳ Byte substitution

↳ Since sub-processes in each round are in reverse manner, unlike for a feistel cipher, those algorithm needs to be separately implemented, although they are very close related.

4.1 Write down the difference between block cipher and stream cipher.

Ans - Both cipher difference is given below:

BLOCK Cipher	STREAM Cipher
• It converts the plain text into cipher text by taking plain text's block at a time.	• It converts the plain text into cipher text by taking 1 byte of plain text at a time.
• It uses either 64 bits or more than 64 bits	• While stream chiper uses 8 bits.
• The complexity of block cipher is simple	• While stream cipher is more complex.
• Block cipher uses confusion as well as diffusion	• While stream cipher uses only confusion
• In block cipher, reverse encrypted text is hard	• While in stream cipher, reverse encrypted text is easy
• Algo. modes are: ECB & CBC	• Algo. modes are CFB & OFB
• It works on transposition techiques like caesar, Polygram substitution cipher, etc...	• It works on substitution techniques like railfence, Columnar transposition, technique, etc..