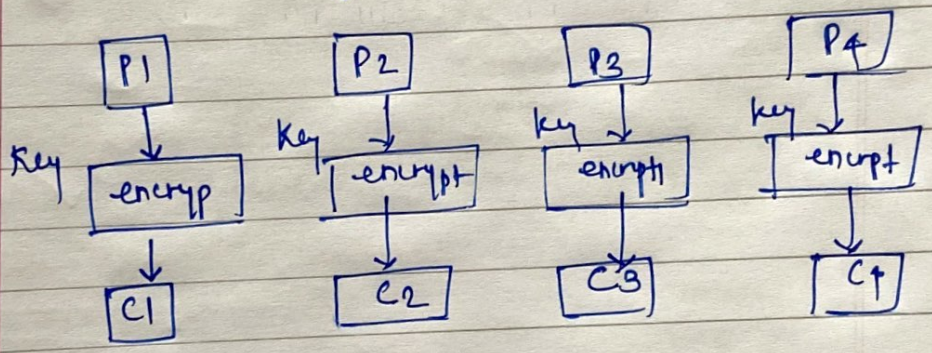
Rebecca Dias
19
18202
TE CMPN A

Assignment Test A

Q. Explain any 2 modes of operation of block cipher.

→ ① Electronic Code Book mode (ECB)

i) Easiest block cipher mode of operation
ii) Plain text is divided into the blocks, each of 64 bit
iii) Same key is used to encrypt each block.



iv) The cipher text is again divided into blocks, each of 64 Bit and each block is decrypted independently one at a time to obtain the corresponding plain text block.
v) The same key is used to decrypt each block which was used to encrypt each block.

advantages
i) Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption
ii) Simple way of block cipher

Disadvantages
i) Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

② Cipher Block Chaining mode (CBC).

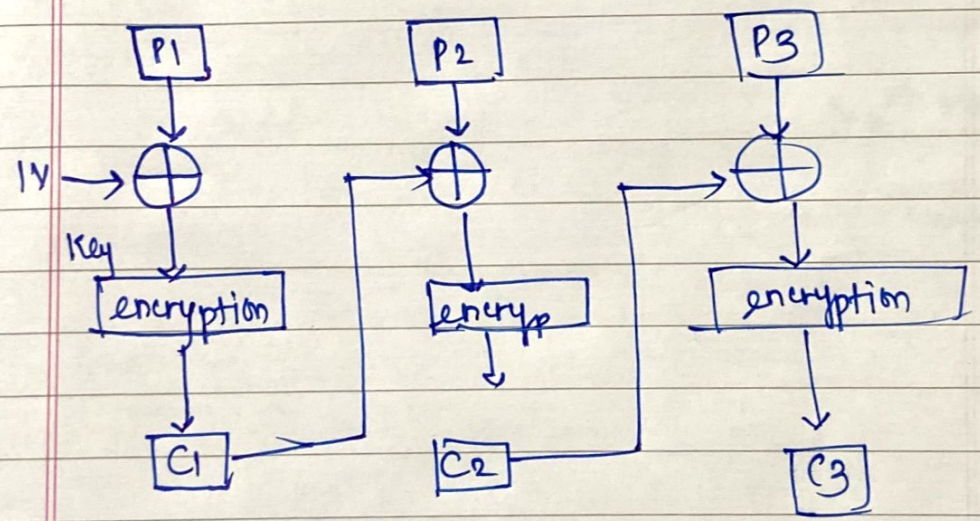
i) CBC confirms that even if the plain text has repeating blocks its encryption won't produce same cipher block

ii) chaining has been added to the block cipher

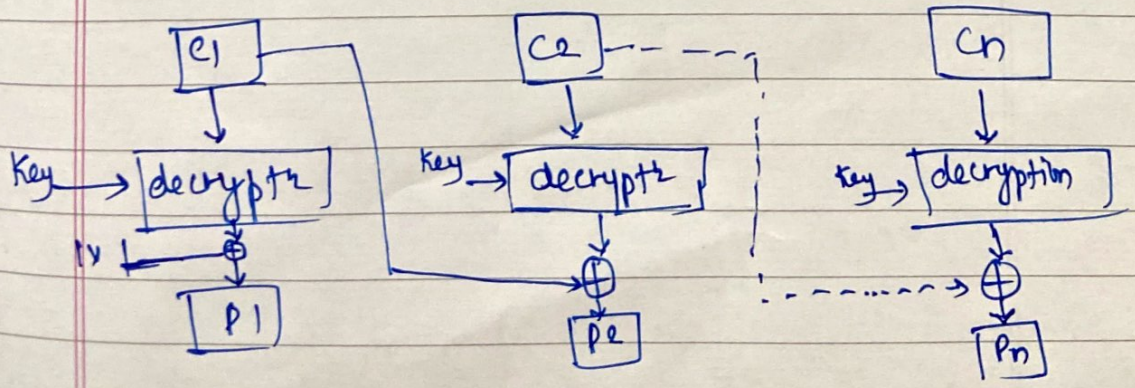
iii) for this, the result obtained from the encryption of the first plain text block is fed to the encryption of the next plaintext box.

iv) since, during the encryption of first plain text block, no previous plain text block is available so a random block of text is generated called Initialization vector.

encryption



decryption



advantages

i) CBC works well for input greater than 8 bits

ii) CBC is a good authentication mechanism

iii) Better resistive nature towards crypandy than ECB.

dis advantages

i) parallel encryptim is not possible since every encryptim requires previous cipher.