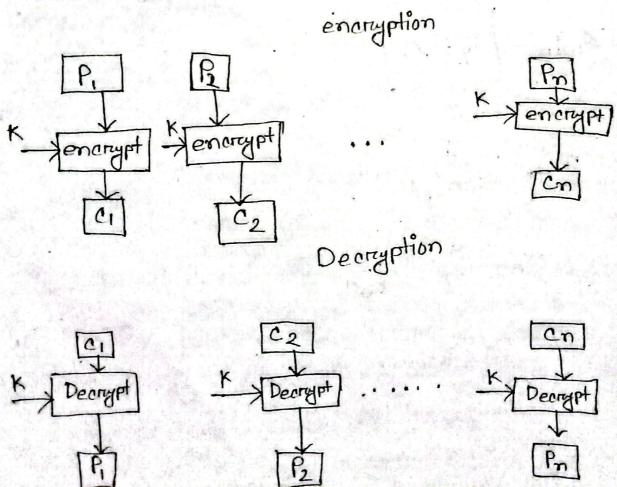
Electronic Code Book (ECB):

The electronic codebook is the easiest block cipher mode of functioning. It is easier because of the direct encryption of each block blocks of input plaintext and output is in the form of blocks of encrypted ciphertext.

Rode Block:



Advantages of using ECB

-> Panallel energyption of blocks of bits in possible thus it is a faster way of energyption.

-> Simple way of block aphen.

Disadvantages of using ECB:

-> Prione to cryptanalysis since there is a dinect relationship between plaintext and ciphentex

Jentical plaintext blocks produce identical ciphentext blocks, which can neveal patterns.

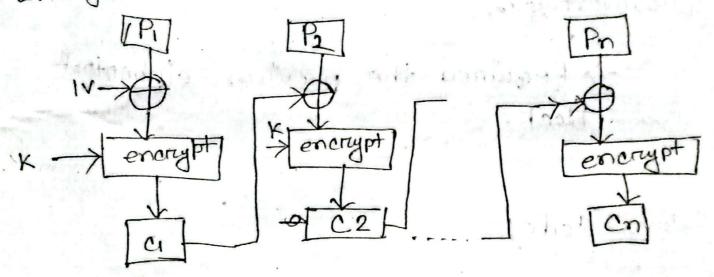
Java cade:

import Javax. crypto. Ciphen;
import Javax. crypto. Key Grenerator;
import Javax. crypto. Secret Key;
import Javax. crypto. Ciphen Inputstream.
import Javax. crypto. Ciphen Output Stream.
import Javax. crypto io. File Inputstream.
import Javax. crypto io. File Inputstream.
import Javax. crypto io. File Inputstream.
import Java. o ecunity. key;

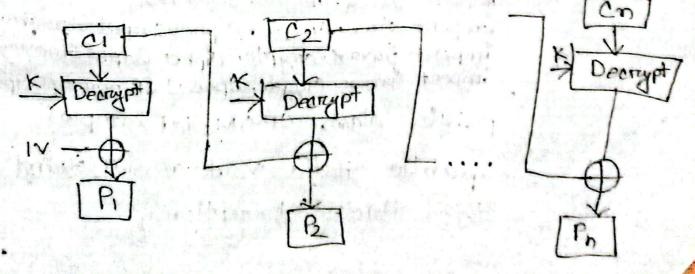
public class ECBMode Example } public static voide main (strange Jangs throws exception { Reygeneratori Keygeneratori = keygenerator get Instance (A) Section key sectrolkey= keygenenaton. generatekey(); ciphen ciphen = Ciphen get Instance ("AES) ECB/PKSS5Padding Ciphen init (Ciphen . Encrypt-mode, secket) byte [] encrypted = cipher.do Final ("This is a test. System. out. println ("En crypted:"+ new string (encrypted)); cipherz init (Cipherz DECRYPT_Mode, secrettey),
byte[] descrypted = cipherz idofinal (encrypted); System.out. prantln ("Decrypted:"+new string (decrypted)). (decrypted)); }

advancement made on ECB since ECB compromises some security near mements. In

Block Diagram; Energption



Decryption



Advantage:

TOBC works well for imput greater than b bits.

many atooks and in

TCBC is a good authentication mechanism.

Disadvantages:

Hock.

Java Code:

import Javax. crypto. Ciphen;
import Javax. crypto. Key Greneraton;
import Javax. crypto. Secre key;
import Jax. crypto. Ciphen Input Stream;
import Javax. crypto. Ciphen Output Stream;
import Javax. crypto. Ophen Output Stream;
import Javax. crypto. opec. I v Panameter Spec;
public class CBCMode Examples

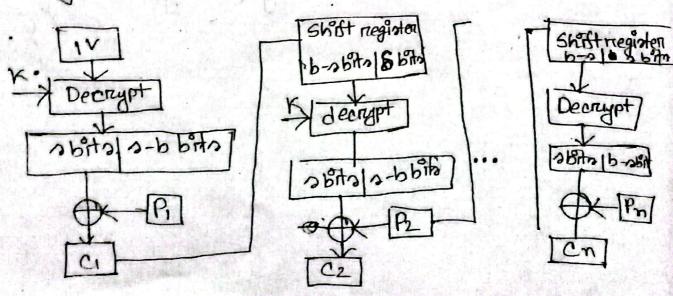
public Static Void main (String[]
args] throws Exception {

Keygenerator KeyGrenerator = KeyGrenerator getInsiene byte[] "v = new byte [16]; IN parameter Spec in Parameter Spec = new Informa-meter Spec (in); Ciphen aiphen = Ciphen.get Irvatornee ("AES"); Ciphen . init (ciphen . Encrypt . Encrypt mode); byte [] encrypted = Ciphen · dofinal (* Things a tot) igystem.out. printin ("Encrypted (aBC): "+ new string (encrypted)); Ciphen · int (Ciphen · Decrypt-mode, secret key); byte[] decrypted = ciphen.dofinal (Energyte System.out. println (" Decrypted (CBC): "+ new String (decrypted));

CEB:

In this mode the ciphen is given as feedback to the next block of encryption with some new supecifications:

Block Diagram: Enaryption Shift negisten Short negisten क्षित्र विभिन्न क्ल otide offderd Energy encrypt encrypt 10 py 10 20 py क किरी किन्त किरीव 200 0-9 Pull Po X cn Dearyption. Shift negisted



Advantages:

-> Since, there is some data loss due to the use of shift register, thus it is difficult

-> Can do handle data streams of any size Disadvantages:

-> Slightly more complex and can propegate етспотов.

Java Code:

import. Javax. crypto . cipheri; import. Gavan. cypto. Keygeneratori; import. Javax. crypto. secret key; import. Javax. opec. Ivparameter;

Public Class CFB Mode Example {

public static Void Main (string[] ango)

Keygenerator Keygenerator = Keygenetaton get Instance (" ARS"); Secretkey sectet key = kggeneraton gene-raton (1;

byte [] iv = new byte [16];

Ivpariameterspec = new Ivpariapmeter (iv);

ciphen ciphen = ciphen getInstance (AES");

ciphen ciphen = ciphen getInstance (AES");

byte []encrypted = ciphen dofinal (This");

ciphen init (ciphen Decrypt - mode);

3 ystem out printin (Descrypted (CFB):"

+ new string (decrypte);

and the transfer of the results that the re-

Plant of the distribution of the string of