1. program pergeseran bit :

import java.util.Scanner;

public class Bit{

public static void main(String[] args){

Scanner data = new Scanner(System.in);

System.out.print("Input angka: ");

int n = data.nextInt();

System.out.print("Input jumlah pergeseran: ");

int a = data.nextInt();

System.out.println();

String biner = Integer.toBinaryString(n);

System.out.println("biner dari "+n+": "+biner);

System.out.println(n+" >> "+a+": "+(n >> a)+" ("+Integer.toBinaryString(n >> a)+")");

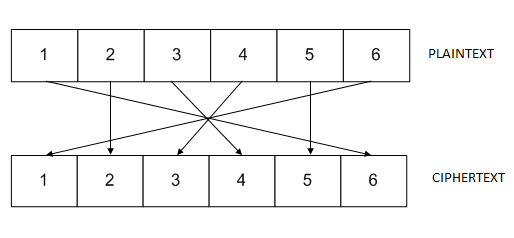
System.out.println(n+" << "+a+": "+(n << a)+" ("+Integer.toBinaryString(n << a)+")");

}

}

4. Teknik enkripsi adalah memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap,namun posisinya yang diacak.

Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama. Plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi, sebagai berikut :



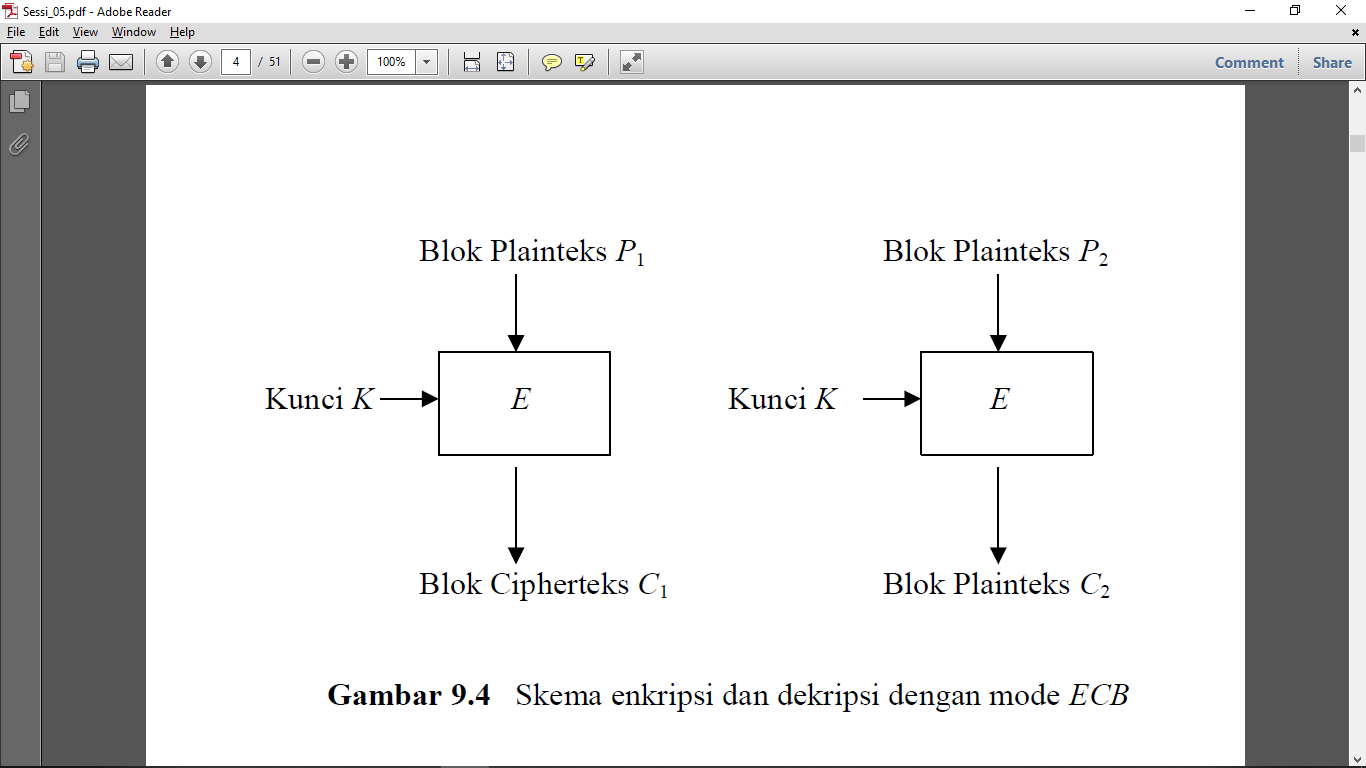
5. a. Electronic Code Book (ECB)

Setiap blok plainteks Pi dienkripsi secara individual dan independen menjadi blok cipherteks Ci. Pada ECB, blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama.

Enkripsi : Ci = EK(Pi)

Dekripsi : Pi = DK(Ci)

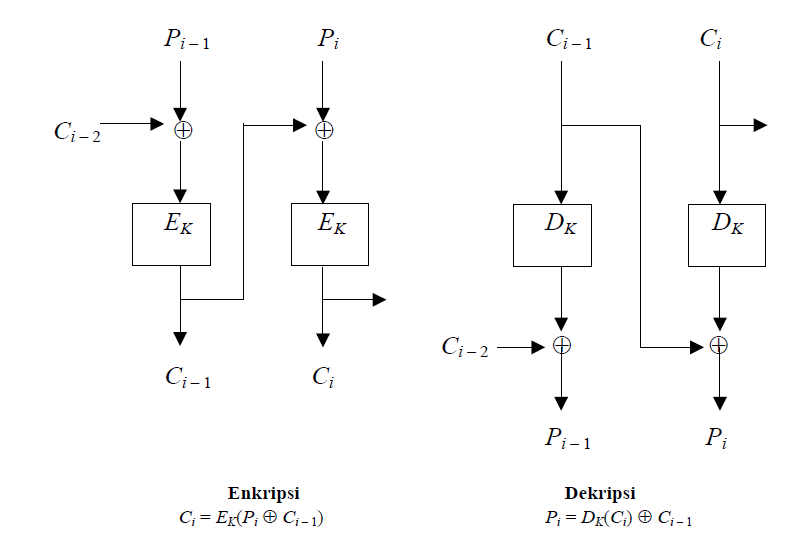
Pi dan Ci masing-masing blok plainteks dan cipherteks ke-*i*.



Skema enkripsi dan dekripsi dengan mode ECB

b. Cipher Block Chaining (CBC)

CBC bertujuan untuk membuat ketergantungan antar blok. Setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya. Hasil enkripsi blok sebelumnya di umpan balikkan ke dalam enkripsi blok yang current. Blok-blok plainteks yang sama tidak menghasilkan cipherteks yang sama sehingga kriptanalisis menjadi lebih sulit.

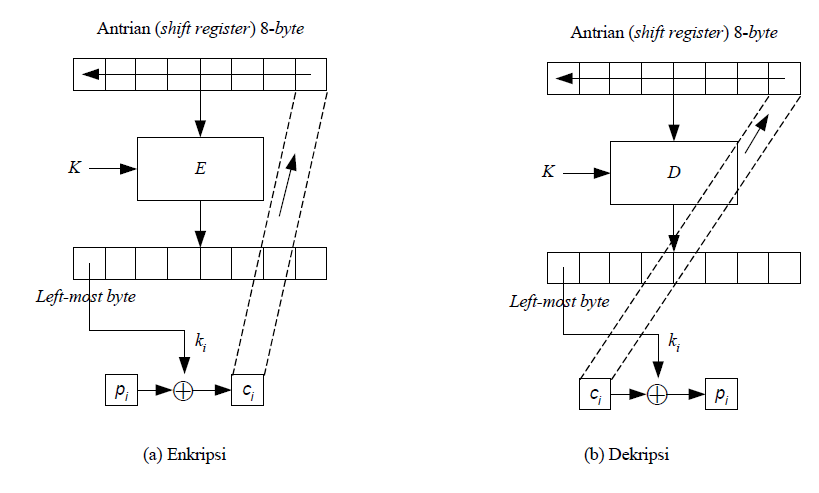


Skema enkripsi dan dekripsi dengan mode CBC

c. Cipher-Feedback (CFB)

* CFB digunakan untuk mengatasi kelemahan pada mode CBC jika diterapkan pada komunikasi data (ukuran blok yang belum lengkap).
* Data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok.
* Unit yang dienkripsikan dapat berupa bit per bit (seperti cipher aliran).
* Bila unit yang dienkripsikan satu karakter setiap kalinya, maka mode CFB nya disebut CFB 8bit.
* CFB *n*-bit mengenkripsi plainteks sebanyak *n* bit setiap kalinya, *n* ≤ m (m = ukuran blok).

Skema mode CFB 8-bit yang bekerja pada blok 64 bit :



d. Output Feedback (OFB)

Mode *OFB* mirip dengan mode *CFB*, kecuali *n*-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan di antrian. Dekripsi dilakukan sebagai kebalikan dari proses enkripsi.

Skema mode OFB 8-bit yang bekerja pada blok 64 bit :

