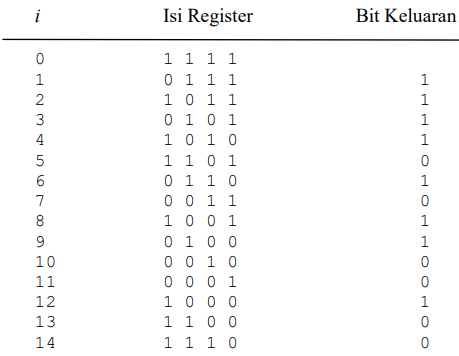
**Pertemuan I Kriptografi modern**

0000=0,0001=1,0010=2,0011=3,0100=4,0101=5,0011=6,0111=7,1000=8,1011=9,1010=A,1011=B,1100=C, 1101=D, 1101=E, 1111=F (Hex), kalau plainteksnya tidak cukup dibagi sesuai blok maka ditambah 000 disebelah kirinya (padding bits)

**Pertemuan II Stream Cipher**

Keystream generator. Ada contohnya yg xor-kan bit 1 dngan bit 4 untuk dapat nilai ke-5 nilai ke-6 dari bit 2 dengan bit 5 untuk dapat nilai ke-6 dst. (kalau 4-bit yg disuruh)

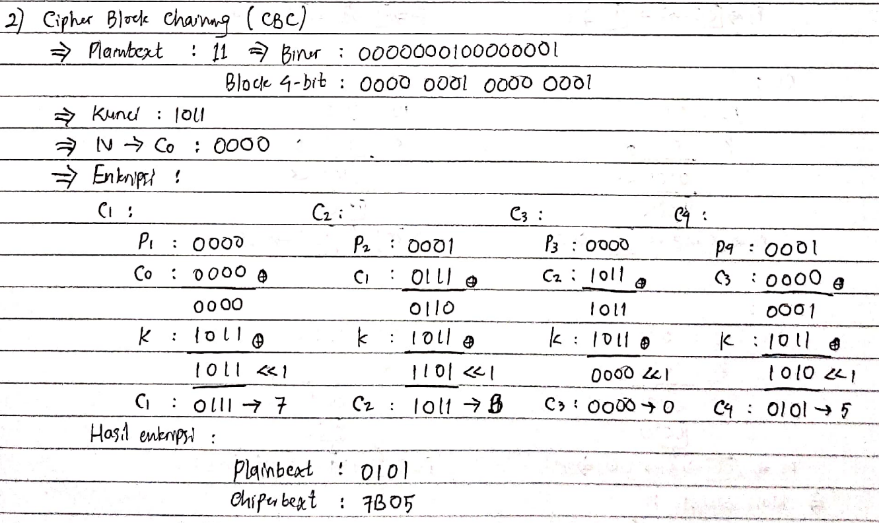
* FSR (Feedback Shift Register): terdiri dari dua bagian:register geser (n bit) dan fungsi umpan balik. Contoh FSR adalah LFSR (Linear Feedback Shift Register)

 LFSR 4-bit diinisialisasi dengan 1111

**RC4 -> RC4 memproses data dalam ukuran byte, bukan dalam bit. Key-Scheduling Algorithm (KSA) dan Pseudo-random generation algorithm (PRGA).**

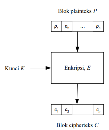
**Key-Scheduling Algorithm (KSA)**

J -> 0, i-> 0 /iterasi 1

J -> (j + S[i] + K[i mod Length(K)]) mod 256, swap(S[i], S[j])

**Pseudo-random generation algorithm (PRGA) (dibawah ini yg pake titik berarti baris baru)**

i -> 0 j -> 0. idx -> 0. i -> (i + 1) mod 256. j -> (j + S[i]) mod 256. swap(S[i], S[j]) {Pertukarkan nilai S[i] dan S[j]}. t -> (S[i] + S[j]) mod 256. u -> S[t] (keystream ). c -> u xor P[idx] {enkripsi}

**A5 -> untuk mengenkripsi transmisi sinyal percakapan dari standard telepon seluler GSM (Group Special Mobile).**

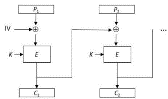
**Block Cipher -> Panjang blok cipherteks = panjang blok plainteks. Skema**

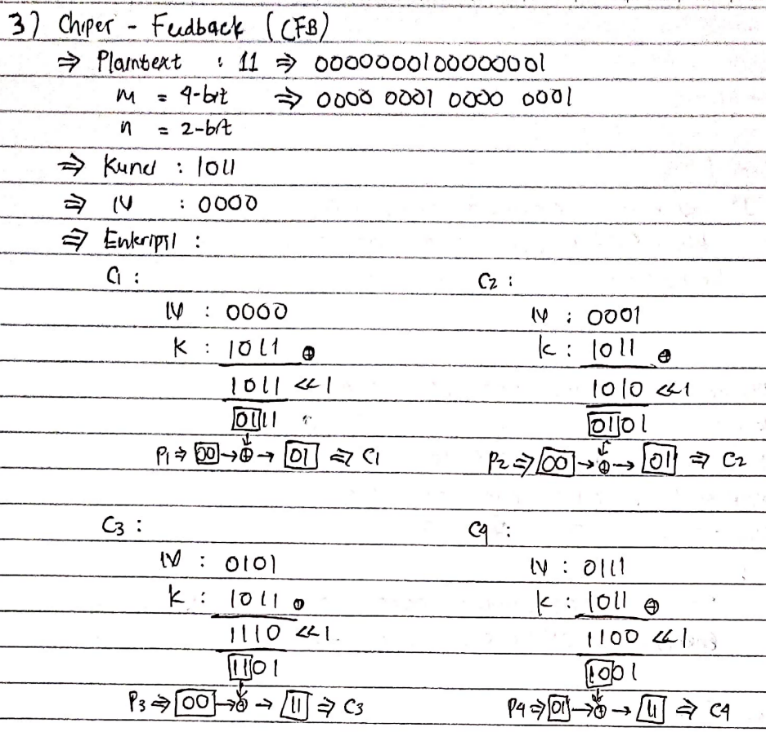
1. **ECB (Electronic Code Book) -> INDEPENDEN**

Cnth: Plainteks: 10100010001110101001. Bagi plainteks blok 4-bit.

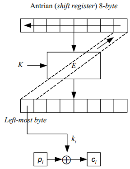
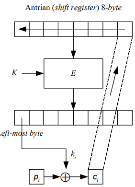
(notasi HEX :A23A9). Kunci (juga 4-bit): 1011. Di xor-kan plainteks 4-bit dengan kunci lalu hasilnya di <<1. Nah itumi hasil cipherteksnya (kasih notasi hex juga). (dmetode ini diberlakukan **padding bits 0 semua, 1 semua, ato selang seling**)

1. **CBC (Cipher Block Chaining) -> KETERGANTUNGAN ANTAR BLOK, skemanya:**

**-> initialization vector (IV). Cntoh: ada plainteks, 4-bit, kunci sama IV. P1 xor IV. Hasilnya xor Kunci baru <<1 itumi cipherteksnya**



1. **CFB (Cipher-Feedback) 4. OFB (Output-Feedback)**

****Xi=IV, m=ukuran blok, yg sblah kirinya

n=panjang unit keatas

ciphernya yng naik keatas



**5.Counter Mode -> Nilai counter harus berbeda dari setiap blok yang dienkripsi. Pada mulanya, untuk enkripsi blok pertama, counter diinisialisasi dengan sebuah nilai. Selanjutnya, untuk enkripsi blok-blok berikutnya counter dinaikkan nilainya satu.**

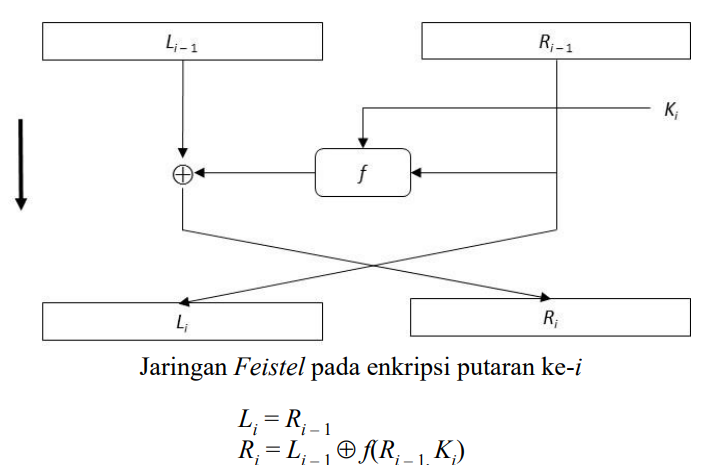
**Prinsip-prinsip Perancangan Cipher Blok, Kunci utama=eksternal, kunci putaran=internal**

**1. Prinsip Confusion dan Diffusion dari Shannon**. -> Prinsip ini menyembunyikan hubungan apapun yang ada antara plainteks,cipherteks, dan kunci. Prinsip **confusion** membuat kriptanalis frustasi untuk mencari pola-pola statistik yang muncul pada cipherteks. One-Time Pad adalah contoh algoritma yang confuse. Confusion dapat direalisasikan dengan menggunakan algoritma substitusi yang kompleks. **Diffusion**: Mode CBC dan CFB menggunakan prinsip ini. Pada algoritma DES, diffusion direalisasikan dengan menggunakan operasi permutasi.

**2. Cipher berulang (iterated cipher) ->** Ci= f(Ci – 1, Ki). i = 1, 2, …, r (r adalah jumlah putaran).

Ki= upa-kunci (subkey) pada putaran ke-I, f = fungsi transformasi (di dalamnya terdapat operasi substitusi, permutasi,dan/atau ekspansi, kompresi). Plainteks dinyatakan dengan C0 dan cipherteks dinyatakan dengan Cr.

**3.Jaringan Feistel (Feistel Network)**

****

**4. Kotak-S (S-box) ->** matriks yang berisi substitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain. Pada kebanyakan algoritma cipher blok, kotak-S memetakan m bit masukan menjadi n bit keluaran, sehingga kotak-S tersebut dinamakan kotak mxn S-box. Cth: 6x4 S-box yang berarti memetakan 6 bit masukan menjadi 4 bit keluaran. b1,b2,b3,b4,b5,b6 -> b1b6 baris, b2b3b4b5->kolom (DES)

