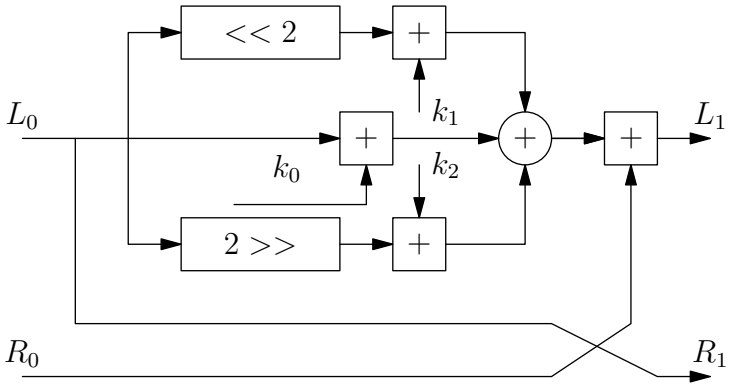
4 užduotis. Blokinių šifrų režimai su TEA



Viena TEA iteracija

Pranešimo blokai L_0, R_0 – po 8 bitus (po vieną ASCII simbolį), vienos iteracijos raktas $K = [k_0, k_1, k_2]$ – trys skaičiai (arba trys ASCII simboliai). Operacijos $<< 2, >> 2$ – cikliniai poslinkiai per 2 bitus atitinkamai į kairę ar dešinę; $+$ kvadrate – sudėtis moduliu $2^8 = 256$, $+$ apskritime – XOR.
Šifruojama atliekant tris iteracijas su raktais $K_0 = [k_0, k_1, k_2], K_1 = [k_1, k_2, k_0], K_2 = [k_2, k_0, k_1]$.
Pranešimo $M = [L_0, R_0]$ šifras yra $C = [R_3, L_3.]$
Duoti šifrai sudaryti ECB, CBC, OFB režimais. Reikia juos dešifruoti.
Patarimai, programuojantiems Python arba Sage:

```
int(str(b),2) # dvejetainės eilutės  išraiška į dešimtainį skaičių
a=int(str(11110),2)
print(a)
30

getBin = lambda x, n: x >= 0 and str(bin(x))[2:].zfill(n) or "-"
         + str(bin(x))[3:].zfill(n)
print(getBin(3,10)) #-- skaičiaus 3 10 bitų ilgio dvejetainė išraiška
0000000011

#Cikliniai eilučių postūmiai per n bitų
def rotate_right(l,n):
    return l[-n:] + l[:-n]
def rotate_left(l,n):
    return l[n:] + l[:n]

a^b # XOR operacija Pythono aplinkoje
a^b Sage aplinkoje - kėlimas laipsniu.
XOR operacija Sage: a^^b
```