PRINCIPI MODERNIH TELEKOMUNIKACIJA

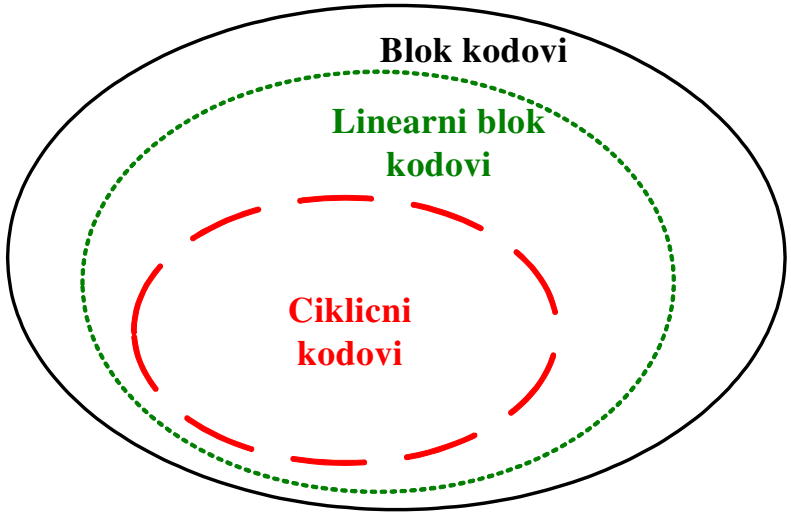
Elektrotehnički fakultet
Katedra za telekomunikacije
Beograd, 2020/2021.

Vežbe III

Linearni blok kodovi, ciklični kodovi, CRC postupak i RSA algoritam

Blok kodovi

* **Klasifikacija blok kodova**
  - ***Blok kod*** **čine kodne reči dužine *n* bita, pri čemu je jedna kodna reč pridružena svakoj mogućoj kombinaciji od *k* informacionih bita. Opisuje se tabelom preslikavanja!**
  - ***Linearni blok kod*** **je vektorski podprostor vektorskog prostora nad poljem *GF(q)* – za binarne kodove *q=2*. Opisuje se generišućom matricom!**
  - ***Ciklični kod*** **je ciklični vektorski podprostor vektorskog prostora nad poljem *GF(q)*. Opisuje se jednim polinomom!**



Zadatak 1

a) Odrediti generišuću matricu Hemingovog koda (7,4).
b) Napisati sve kodne reči ovog koda.
c) Kakva je razlika između Hemingovog rastojanja i Hemingove težine?
d) Odrediti spektar kodnih rastojanja i broj grešaka koji ovaj kod može da koriguje/detektuje!
e) Objasniti način konstrukcije Hemingovog koda (6,3)

Rešenje:

$$\boldsymbol{x} = \boldsymbol{i} \otimes \boldsymbol{G}$$

$$[z_1\ z_2\ i_1\ z_3\ i_2\ i_3\ i_4] = [i_1\ i_2\ i_3\ i_4] \otimes \begin{bmatrix} ? & ? & 1 & ? & 0 & 0 & 0 \\ ? & ? & 0 & ? & 1 & 0 & 0 \\ ? & ? & 0 & ? & 0 & 1 & 0 \\ ? & ? & 0 & ? & 0 & 0 & 1 \end{bmatrix}$$

$$z_1 = c_3 \oplus c_5 \oplus c_7 = i_1 \oplus i_2 \oplus i_4$$
$$z_2 = c_3 \oplus c_6 \oplus c_7 = i_1 \oplus i_3 \oplus i_4$$
$$z_3 = c_5 \oplus c_6 \oplus c_7 = i_2 \oplus i_3 \oplus i_4$$

Zadatak 1 – rešenje (1)

* **Generišuća matrica**

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

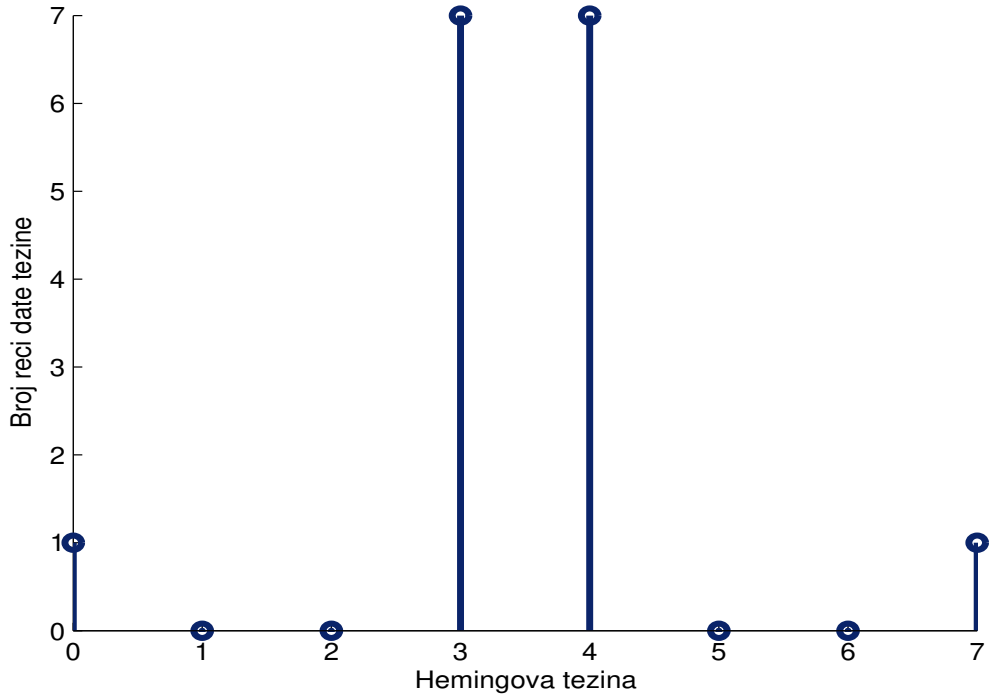
b) Ovaj kod ima 2^4=16 kodnih reči, one su:

x_1=0000000	x_2=1101001	x_3=0101010	x_4=1000011
x_5=1001100	x_6=0100101	x_7=1100110	x_8=0001111
x_9=1110000	x_{10}=0011001	x_{11}=1011010	x_{12}=0110011
x_{13}=0111100	x_{14}=1010101	x_{15}=0010110	x_{16}=1111111

Zadatak 1 – rešenje (2)

* Pošto je svaka kodna reč zbir dve druge kodne reči, rastojanja između pojedinih kodnih reči mogu se odrediti i preko Hemingovih težina.

* Broj kodnih reči sa određenim Hemingovim rastojanjima (težinama) predstavlja spektar kodnih rastojanja datog koda



$d=3,$

$d \geq 2e_c+1$

$e_c=1,$

$d \geq e_c+e_d+1$

$e_d=1.$

Zadatak 1 – rešenje (3)

* **Hemingov kod (6,3) - generišuća matrica**

$$G_{(6,3)} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

* **Proces kodovanja:**

$$[z_1\ z_2\ i_1\ z_3\ i_2\ i_3] = [i_1\ i_2\ i_3] \otimes G_{(6,3)}$$

* **Zaštitni biti:**

$$z_1 = i_1 \oplus i_2$$
$$z_2 = i_1 \oplus i_3$$
$$z_3 = i_2 \oplus i_3$$

Zadatak 2

a) Odrediti generišuću matricu Hemingovog koda (10,6).

b) Objasniti rad deinterlivinga i dekodera, ako se deinterliving obavlja na tri kodne reči, za primljenu sekvencu: $r = (0110011100010010000000000000)$

Rešenje:

1	0 0 0 **1**	z_1
2	0 0 **1** 0	z_2
3	0 0 1 1	i_1
4	0 **1** 0 0	z_3
5	0 1 0 1	i_2
6	0 1 1 0	i_3
7	0 1 1 1	i_4
8	**1** 0 0 0	z_4
9	1 0 0 1	i_5
10	1 0 1 0	i_6
~~11~~	~~1 0 1 1~~	~~i_7~~
~~12~~	~~1 1 0 0~~	~~i_8~~
~~13~~	~~1 1 0 1~~	~~i_9~~
~~14~~	~~1 1 1 0~~	~~i_{10}~~
~~15~~	~~1 1 1 1~~	~~i_{11}~~

$$z_1 = i_1 \oplus i_2 \oplus i_4 \oplus i_5$$
$$z_2 = i_1 \oplus i_3 \oplus i_4 \oplus i_6$$
$$z_3 = i_2 \oplus i_3 \oplus i_4$$
$$z_4 = i_5 \oplus i_6$$

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Zadatak 2

Deinterliving:

$$r = (011001110001001000000000000000)$$

$$\downarrow$$

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} \rightarrow r^{(I)} \\ \rightarrow r^{(II)} \\ \rightarrow r^{(III)} \end{matrix}$$

1 2 3 4 5 6 7 8 9 10

Dekoder:

$$s_1 = r_1 \oplus r_3 \oplus r_5 \oplus r_7 \oplus r_9 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 1$$
$$s_2 = r_2 \oplus r_3 \oplus r_6 \oplus r_7 \oplus r_{10} = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 1$$
$$s_3 = r_4 \oplus r_5 \oplus r_6 \oplus r_7 = 0 \oplus 1 \oplus 0 \oplus 0 = 0$$
$$s_4 = r_8 \oplus r_9 \oplus r_{10} = 0 \oplus 0 \oplus 0 \oplus 0 = 0$$

Lokacije greške:

- prva reč $S^{(I)} = 3$, $\hat{i}^{(I)} = (000000)$
- druga reč $S^{(II)} = 2$, $\hat{i}^{(II)} = (100000)$
- treća reč $S^{(III)} = 2$, $\hat{i}^{(III)} = (010000)$

Zadatak 3

a) ***Odrediti kodnu reč koja se pojavljuje na izlazu kodera, ako je na njegovom ulazu sekvenca (1101), a kod je opisan polinomom $g(x)=1+x^2+x^3$.***

b) ***Ako na ulaz dekodera stigne primljena reč (0001000), izvršiti dekodovanje ako je kod je opisan polinomom $g(x)=1+x^2+x^3$.***

Rešenje:

* Poruka (1101) se prvo prebaci u informacioni polinom, pa se obavi množenje generišućim polinomom

$$(i_0 i_1 i_2 i_3) = (1101) \rightarrow i(x) = x^3 + x + 1$$
$$(g_0 g_1 g_2 g_3) = (1011) \rightarrow g(x) = x^3 + x^2 + 1$$

$$c(x) = i(x)g(x) = x^3(x^3 + x^2 + 1) + x(x^3 + x^2 + 1) + x^3 + x^2 + 1$$
$$= x^6 + x^5 + \cancel{x^3} + x^4 + \cancel{x^3} + x + x^3 + x^2 + 1$$
$$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (1111111)$$

Zadatak 3 - rešenje

* **Poruka *r*=(0001000) se prvo prebaci u primljeni polinom, pa se obavi deljenje generišućim polinomom i odredi ostatak**

$$r = (0001000) \rightarrow r(x) = x^3$$

$$g(x) = x^3 + x^2 + 1$$

$$s(x) = rem(r(x) / g(x)) = 1 + x^2 = (101)$$

* **Dobijeni ostatak ima jednu od osam vrednosti i predstavlja sindrom**

* **Sindrom *s*=(000) ukazuje da nije bilo greške pri prenosu, dok preostalih sedam kombinacija jednoznačno ukazuje na poziciju greške.**

Množenje i deljenje na nivou koeficijenata

* **Množenje sa $g(x)=x^4+x^3+1$**
  (bez pisanja polinoma po x)

$$
\begin{array}{r}
10001100101 \\
\times\quad 11001 \\
\hline
10001100101 \\
00000000000 \\
00000000000 \\
10001100101 \\
10001100101 \\
\hline
110000100011101
\end{array}
$$

* **Deljenje – kodna reč bez greške, tj. sa greškom pri prenosu**

$$
\begin{array}{l}
110000100011101 : 11001 = 10001100101 \\
11001 \\
\quad 10100 \\
\quad 11001 \\
\quad\ 11010 \\
\quad\ 11001 \\
\quad\quad 11111 \\
\quad\quad 11001 \\
\quad\quad\ 11001 \\
\quad\quad\ 11001 \\
\quad\quad\ 00000
\end{array}
$$

$$
\begin{array}{l}
110000100\mathbf{1}11101 : 11001 = 10001100110 \\
11001 \\
\quad 10100 \\
\quad 11001 \\
\quad\ 11011 \\
\quad\ 11001 \\
\quad\quad 10111 \\
\quad\quad 11001 \\
\quad\quad\ 11100 \\
\quad\quad\ 11001 \\
\quad\quad\ 01011
\end{array}
$$

Zadatak 4

a) *Objasniti postupak dobijanja sistematskog cikličnog koda za slučaj kada je* $g(x)=1+x+x^3$

b) *Formirati kodnu reč kada je i=(1010).*

c) *Ispisati sve kodne reči ovog koda.*

d) *Objasniti cikličnu proveru redundanse (CRC) na primeru kada je i=(01100111) a generišući polinom je* $g(x)=x^4+x^3+1$.

e) *Objasniti princip rada CRC kodera i CRC dekodera, koristeći blok šemu.*

Postupak za dobijanje sistematskog cikličnog koda

* Treba najpre informacioni polinom pomnožiti sa x^{n-k}, tako da se dobija nov informacioni polinom

$$i^*(x) = x^{n-k}i(x) = i_{k-1}x^{n-1}+\ldots+i_1x^{n-k-1}+i_0x^{n-k}.$$

* Sada ovaj rezultat treba podeliti generišućim polinomom $g(x)$ koji je stepena n-k. Očigledno da će ostatak biti stepena n-k-1 (tj. da će imati ukupno n-k koeficijenata)

$$r(x) = r_{n-k-1}x^{n-k-1}+\ldots+r_1x+r_0.$$

* Kodna reč se sada dobija oduzimanjem ostatka $r(x)$ od polinoma $i^*(x)$,

$$c(x) = x^{n-k}i(x)+r(x).$$

* Ovome polinomu odgovara kodni vektor

$$(i_{k-1},\ldots,i_1,i_0, r_{n-k-1},\ldots,r_1,r_0)$$

gde su informacioni biti neizmenjeni, a preostali biti su ustvari provere na parnost, čime je dobijen sistematski kod.

Zadatak 4 – rešenje (1)

Poruke	Kodni vektori	Kodni polinomi
(0 0 0 0)	0 0 0 0 0 0 0	0 = 0•g(x)
(1 0 0 0)	1 1 0 1 0 0 0	1+x+x^3 = 1•g(x)
(0 1 0 0)	0 1 1 0 1 0 0	x+x^2+x^4 = x•g(x)
(1 1 0 0)	1 0 1 1 1 0 0	1+x^2+x^3+x^4 = (1+x)•g(x)
(0 0 1 0)	1 1 1 0 0 1 0	1+x+x^2+x^5 = (1+x^2)•g(x)
(1 0 1 0)	0 0 1 1 0 1 0	x^2+ x^3+x^5 = x^2•g(x)
(0 1 1 0)	1 0 0 0 1 1 0	1+x^4+x^5 = (1+x+x^2)•g(x)
(1 1 1 0)	0 1 0 1 1 1 0	x+x^3+x^4+x^5 = (x+x^2)•g(x)
(0 0 0 1)	1 0 1 0 0 0 1	1+x^2+x^6 = (1+x+x^3)•g(x)
(1 0 0 1)	0 1 1 1 0 0 1	x+x^2+x^3+x^6 = (x+x^3)•g(x)
(0 1 0 1)	1 1 0 0 1 0 1	1+x+x^4+x^6 = (1+x^3)•g(x)
(1 1 0 1)	0 0 0 1 1 0 1	x^3+x^4+x^6 = x^3•g(x)
(0 0 1 1)	0 1 0 0 0 1 1	x+x^5+x^6 = (x+x^2+x^3)•g(x)
(1 0 1 1)	1 0 0 1 0 1 1	1+x^3+x^5+x^6 = (1+x+x^2+x^3)•g(x)
(0 1 1 1)	0 0 1 0 1 1 1	x^2+ x^4+x^5+x^6 = (x^2+x^3)•g(x)
(1 1 1 1)	1 1 1 1 1 1 1	1+x+x^2+x^3+x^4+x^5+x^6 = (1+x^2+x^5)•g(x)

$X^3(x^2+1)$

$X^3+x+1)$

$= x^2$

Zadatak 4 – rešenje (2)

* **Binarnu poruku i=(01100111) treba kodovati CRC kodom kod koga je generišući polinom dat izrazom $g(x)=x^4+x^3+1$.**
* **Vektor koji odgovara generišućem polinomu dobija se iz**

$$g(x) = x^4 + x^3 + 1 = g_0 x^0 + g_1 x^1 + g_2 x^2 + g_3 x^3 + g_4 x^4 \rightarrow g = (10011)$$

* **Polinom koji odgovara poruci koja se prenosi**

$$i=(01100111) \rightarrow i(x)=x^7+x^6+x^5+x^2+x$$

* **Kodna reč na osnovu postupka**

$$c(x) = i(x)x^{n-k} + rem\left\{\frac{i(x)x^{n-k}}{g(x)}\right\} = i(x)x^4 + r(x)$$

a ovde je

$$i(x)x^4 = x^{11} + x^{10} + x^9 + x^6 + x^5 \rightarrow i^* = (00001100111)$$

$$r(x) = rem\left\{\frac{i(x)x^4}{g(x)}\right\} = x^2 + x \rightarrow (0110)$$

$$c(x) = i(x)x^4 + r(x) = x^{11} + x^{10} + x^9 + x^6 + x^5 + x^2 + x \rightarrow c = (01100111001111)$$

Zadatak 4 – rešenje (3)

* **Ako je greška prikupljena na liniji oblika e=00000000101, za poslatu poruku c primljena poruka će biti :**

$$c = (011001100111)$$

$$e = (100100000000)$$

$$y = (111101100111)$$

* **Ako ostatak pri deljenju sa $g(x)$ bude ravan nuli smatra se da je kodna reč ispravno preneta (poslata kodna reč je uvek deljiva generišućim polinomom!). U svakom drugom slučaju smatra se da je došlo do greške pri prenosu.**
* **U posmatranom slučaju dele se polinomi koji odgovaraju sekvencama (111101100111) i (11001) :**

$$rem\left\{\frac{y(x)}{g(x)}\right\} = x^3 + 1 \;\Rightarrow\; r = [1001] \neq [0000]$$

pa je detektovana greška pri prenosu, ali ne i na kojoj poziciji se nalazi greška i da li je pri prenosu postojala jedna ili više grešaka.

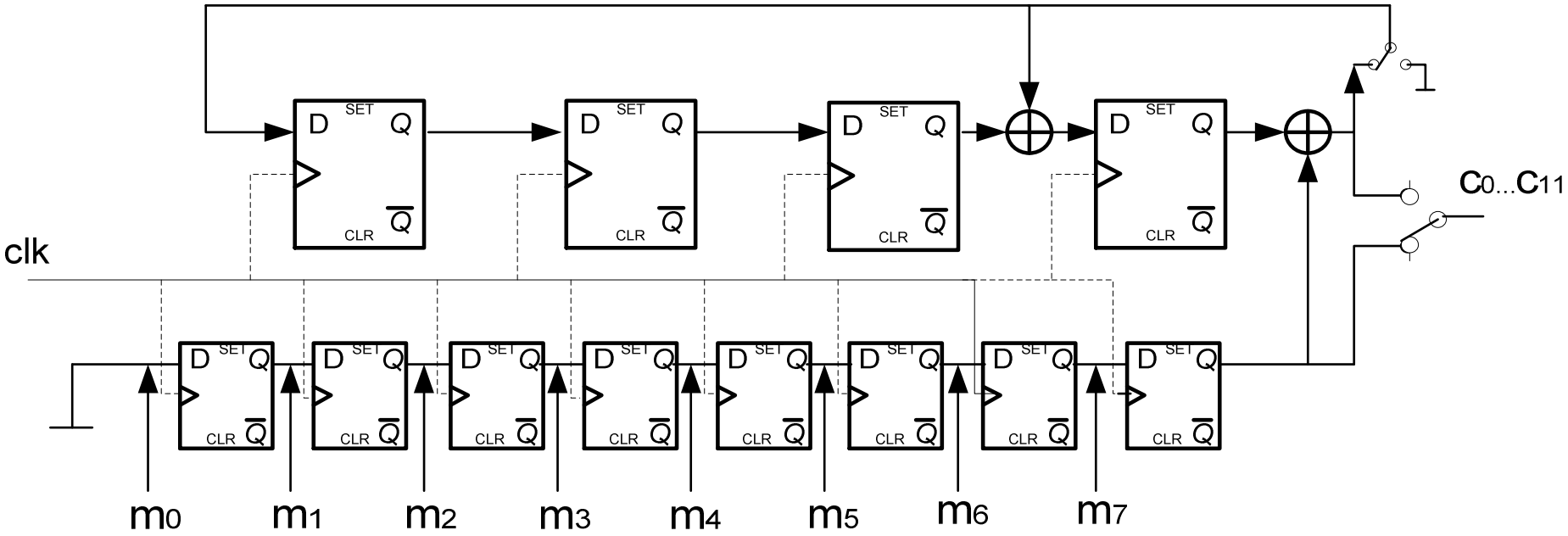
Zadatak 4 – rešenje (4)

* **Sabiranjem sekvence grešaka sa poslatom kodnom reči na prijemu može se desiti sa se opet primi jedna od kodnih reči.**
* **U tom slučaju dekoder će smatrati da nije bilo grešaka pri prenosu. Koliko je ovo verovatno?**
  - Kodna reč je dužine n bita pa u dekoder može doći ukupno 2^n svih mogućih kombinacija kodnih reči.
  - Koder može da emituje samo 2^k kombinacija kodnih reči dužine n. Informacione reči na ulazu kodera su dužine k pa je za svaku kombinaciju od k bita na ulazu preostalih n-k bita u kodnoj reči jednoznačno određeno.
  - Od 2^n mogućih reči na ulazu dekodera samo 2^k su kodne reči. Stoga je verovatnoća da greška ne bude detektovana utoliko manja što je n-k veće (verovatnoća ovakvog događaja je 2^{k-n} ali treba uzeti u obzir i činjenicu da nisu sve sekvence grešaka jednako verovatne!) ali je tada umanjen i kodni količnik.

Zadatak 4 – rešenje (5)

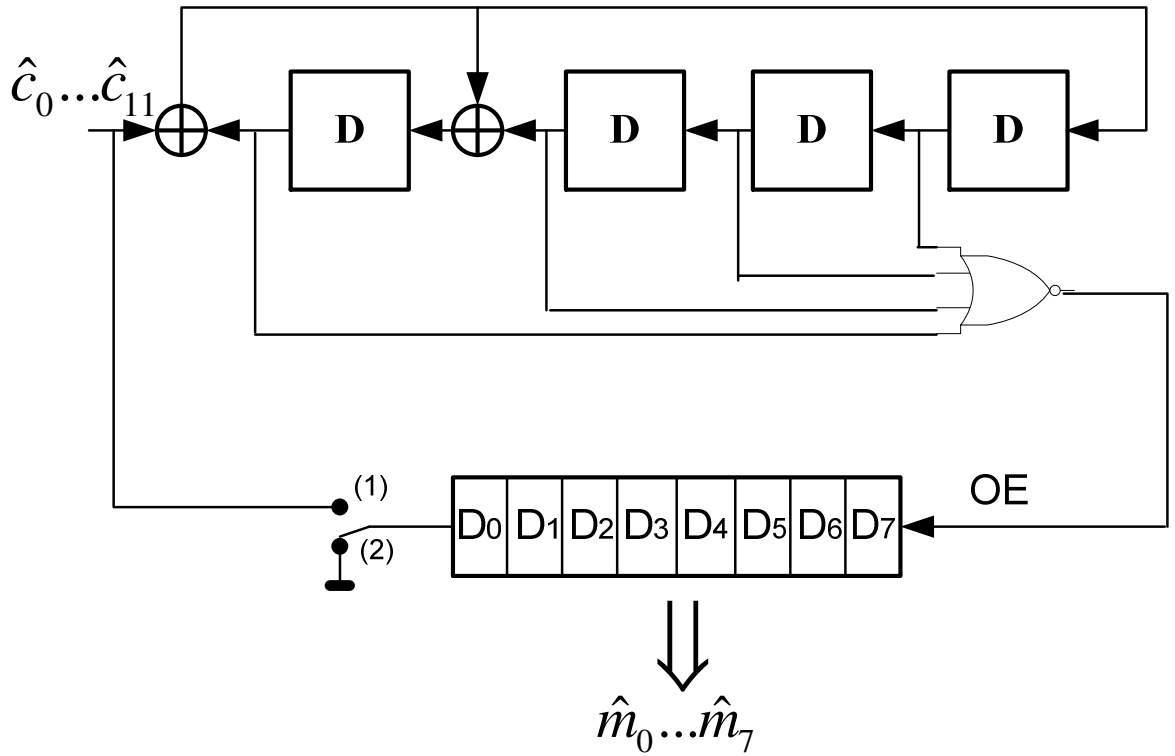
* U prvih k=8 taktova iščitavaju se donji biti a gore se obavlja deljenje. Nakon k taktova ostatak je izračunat i nalazi se u gornjem registru. Prekidači idu u položaj (2) a na izlaz se iščitava ostatak od n-k=4 bita.

* Najjednostavnija hardverska realizacija data je na sledećoj slici (po istom principu lako je izvesti i softversku realizaciju!). Prekidači u pomeračkom registru određeni su koeficijentima generišućeg polinoma.



Zadatak 4 – rešenje (6)

* **Kada je prekidač u položaju (1) prvih *k* bita stiže u kolo za deljenje i pomerački registar. Na prijemu se računa ostatak. Ako je ostatak različit od nule OE=0 i ne dozvoljava se čitanje donjeg registra.**
* **Ako je ostatak je ravan nuli *r*(*x*)=0 tada nema greške pa je OE=1 i dekodovana informacija može da se prosledi korisniku.**



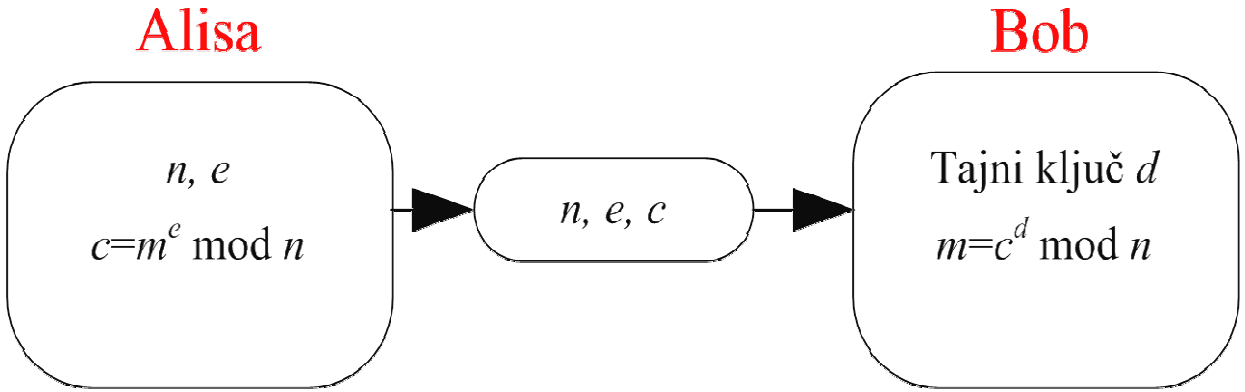
Zadatak 5

* **Objasniti RSA postupak za slučaj kada su prosti brojevi od kojih se polazi dvocifreni, a poruka koju treba kriptovati sastoji se od osamnaest decimalnih cifara.**

- Ukoliko se odabere $p = 47$ i $q = 71$, onda je $n = p \times q = 3337$.
- Ključ za šifrovanje e ne sme da ima nikakve zajedničke faktore sa

$$z = (p-1) \times (q-1) = 46 \times 70 = 3220,$$

pa se može izabrati $e = 79$ i $d = 1019$ (broj d može izračunat primenom proširenog Euklidovog algoritma). Sada se objave e i n (javni ključ) a d se zadrži u tajnosti.



Zadatak 5

Da bi se šifrovala poruka

$$m = 6882326879666683$$

ona se prvo podeli na male blokove, pa će trocifreni blokovi poslužiti u ovom slučaju:

$$m_1 = 688,\ m_2 = 232,\ m_3 = 687,\ m_4 = 966,\ m_5 = 668,\ m_6 = 003$$

- Prvi blok se šifruje stepenovanjem po modulu

$$c_1 = 688^{79} \bmod 3337 = 1570$$

Izvršavanjem iste operacije na narednim blokovima određuje se kompletna šifrovana poruka

$$c = 1570\ 2756\ 2091\ 2276\ 2423\ 158.$$

- Za dešifrovanje poruke potrebno je izvršiti isto stepenovanje, uz primenu ključa za dešifrovanje 1019, tako da se prvi blok dešifruje kao

$$m_1 = 1570^{1019} \bmod 3337 = 688$$

a i ostatak poruke se dešifruje na isti način.