4. Kriptográfia, titkosítás

4.1. Feladat

Fejtse meg az alábbi üzenetet, amelyet Caesar egyik kémje küldött magának a nagy Caesarnak Pannóniából!

ORJNE RGURV QRFBS ZNEPU

Megoldás:

A leggyakoribb betűk az R (4 db előfordulással) és az N, E, U (mind-mind 2 db előfordulással).

Próbálkozzunk olyan Caesar rejtjelezőkkel, amelyek e betűhöz az R-t, N-t, E-t, illetve az U-t rendelik[1]. Ha e → R, akkor az eltolás értéke 13 karakternyi. Ebben az esetben a visszafejtett szöveg az alábbi lesz:

BEWARE THE IDES OF MARCH

Letter	AAIW	Meaker	Garrett	French	Spanish	Gadsby
A	8.15	8.05	7.73	9.42	12.69	10.96
B	1.37	1.62	1.58	1.02	1.41	2.14
C	2.21	3.20	3.06	2.64	3.93	2.66
D	4.58	3.65	3.24	3.38	5.58	4.12
E	12.61	12.31	11.67	15.87	13.15	0.00
F	1.86	2.28	2.14	0.95	0.46	2.15
G	2.36	1.61	2.00	1.04	1.12	3.61
H	6.85	5.14	4.52	0.77	1.24	4.91
I	6.97	7.18	7.81	8.41	6.25	8.81
J	0.14	0.10	0.23	0.89	0.56	0.23
K	1.07	0.52	0.79	0.00	0.00	1.18
L	4.37	4.03	4.30	5.34	5.94	5.32
M	1.96	2.25	2.80	3.24	2.65	2.07
N	6.52	7.19	6.71	7.15	6.95	8.61
O	7.58	7.94	8.22	5.14	9.49	10.42
P	1.40	2.29	2.34	2.86	2.43	1.91
Q	0.19	0.20	0.12	1.06	1.16	0.05
R	5.02	6.03	5.97	6.46	6.25	4.77
S	6.05	6.59	6.55	7.90	7.60	6.97
T	9.93	9.59	9.53	7.26	3.91	8.50
U	3.22	3.10	3.21	6.24	4.63	4.16
V	0.78	0.93	1.03	2.15	1.07	0.31
W	2.49	2.03	1.69	0.00	0.00	2.80
X	0.13	0.20	0.30	0.30	0.13	0.04
Y	2.11	1.88	2.22	0.24	1.06	3.18
Z	0.07	0.09	0.09	0.32	0.35	0.11

4.2. Feladat

Az alábbi szöveget affin rejtjelezővel titkosították. Mi lehetett az eredeti angol nyelvű üzenet?

GWNQZ ADGTR BILZT WGWBM NENNO WBOKE BIIEJ GGWNA NQNAN NWBDT ZMNOZ GGWND
NHROK RONLZ TWGWB MNENN ORJGD ZKNGW NERSE JGBTB ZOWNW BDLBK NGWNK NHZDZ
ROBTB ZODGJ DBGGW NNOKR QGWNK BVPNK ZKOGK NQNOK GWNLP NIINO RJTWZ HBOGE
NHAZG ZHBIR QGWNA NQNAN NEJGZ HBOEN HAZGZ HBIRQ LVKNQ NOKNA DORGK NQNOK
ZOTZG PNIIG WNVPN ANURR AYYYY

Megoldás:

Affin rejtjelezők esetében a titkosítás, illetve a titkosított szöveg visszafejtése az alábbi összefüggésekkel adható meg:

$$\text{Enc}: x \mapsto ax + b \pmod{m}$$

$$\text{Dec}: x \mapsto a^{-1}(y - b) \pmod{m},$$

[1] A feladat mellett található táblázat mutatja az egyes betűk előfordulási gyakoriságát az angol (különböző könyvek alapján) és egyéb nyelveken.

ahol a^{-1} az a multiplikatív inverze $\bmod m$, azaz $aa^{-1} \equiv 1 \pmod m$, és m az ábécé mérete. A második összefüggés átírható az alábbi módon:

$$\mathrm{Dec}(x) \equiv a^{-1}(y-b) \equiv a^{-1}y - a^{-1}b \equiv \tilde{a}y + \tilde{b} \pmod m.$$

A titkosított szövegben a két leggyakoribb betű az N és a G. Válasszuk őket e-nek és t-nek. Ekkor $\mathrm{Dec}(13) = 4$ és $\mathrm{Dec}(6) = 19$. Ebből az affin rejtjelezőre az alábbi egyenleteket írhatjuk:

$$\tilde{a} \cdot 13 + \tilde{b} \equiv 4 \pmod{26},$$

illetve

$$\tilde{a} \cdot 6 + \tilde{b} \equiv 19 \pmod{26}.$$

A másodikból kivonva az elsőből $7\tilde{a} \equiv -15 \pmod{26}$-t kapunk. Így $\tilde{a} \equiv 15(-15) \pmod{26}$, azaz $\tilde{a} = 9$. Ezt behelyettesítve a másik egyenletbe $6(9) + \tilde{b} \equiv 19 \pmod{26}$. Ebből pedig $\tilde{b} \equiv 19 - 6(9) \equiv -35 \equiv 17 \pmod{26}$.

Így már meghatározható a rejtjelező által használt összerendelés:

A → r, B → a, C → j, D → s, E → b, F → k, G → t, H → c, I → l, J → u, K → d, L → m, N → e, O → n, P → w, Q → f, R → o, S → x, T → g, U → p, V → y, W → h, X → q, Y → z, Z → i,

és a nyílt szöveg is:

```
thefi rstgo almig hthav ebeen handb allbu tther efere ehasg iveni tthes
econd onemi ghtha vebee nouts ideth eboxb utaga inheh asmad ethed ecisi
onaga instu satth eendo fthed aywed idntd efend themw ellen oughi cantb
ecrit icalo fther efere ebuti canbe criti calof mydef ender snotd efend
ingit wellt heywe repoo rzzzz
```

4.3. Feladat

Adva van a $x^4 + x + 1$ polinom.

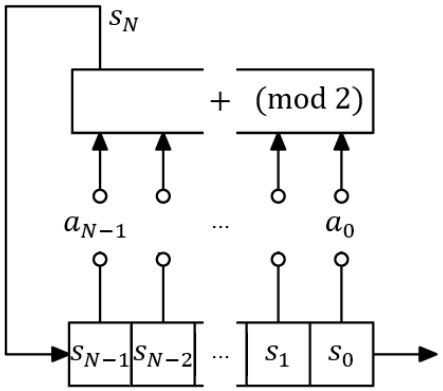
a) Rajzolja fel azt a LFSR-t, amelynek ez a polinom a karakterisztikus polinomja!

b) Határozza meg a karakterisztikus polinomhoz tartozó feedback polinomot!

c) Határozza meg a shift regiszter kimeneti szekvenciáját, ha kezdeti értéke 1001!

d) Határozza meg a shift regiszter periódusát minden nem nulla kezdeti érték esetére!

Megoldás:



a) Az ábra alapján könnyen beláthatjuk, hogy:

$$s_{N+k} = \sum_{i=0}^{N-1} a_i s_{k+i}.$$

Legyen $\boldsymbol{L}$ egy lineáris operátor (shiftelés), amelyre

$$\boldsymbol{L}(s_{N-1}, \dots, s_1, s_0) = (s_N, \dots, s_2, s_1).$$

Ekkor

$$\begin{aligned}
&\sum_{i=0}^{N-1} a_i \boldsymbol{L}^i(s_{N-1}, \dots, s_1, s_0) \\
&\quad = a_0 \boldsymbol{L}^0(s_{N-1}, \dots s_1, s_0) + a_1 \boldsymbol{L}^1(s_{N-1}, \dots s_1, s_0) + \cdots + a_{N-1} \boldsymbol{L}^{N-1}(s_{N-1}, \dots s_1, s_0) \\
&\quad = a_0(s_{N-1}, \dots s_1, s_0) + a_1(s_N, \dots s_2, s_1) + \cdots + a_{N-1}(s_{2N-2}, .., s_N, s_{N-1}) \\
&\quad = \left((a_0 s_{N-1} + a_1 s_N + \cdots), \dots, (a_0 s_1 + a_1 s_2 + \cdots), (a_0 s_0 + a_1 s_1 + \cdots)\right) \\
&\quad = \left(\sum_{i=0}^{N-1} a_i s_{i+N-1}, \dots, \sum_{i=0}^{N-1} a_i s_{i+1}, \sum_{i=0}^{N-1} a_i s_i\right) \\
&\quad = (s_{2N-1}, \dots s_{N+1}, s_N) \\
&\quad = \boldsymbol{L}^N(s_{N-1}, \dots, s_1, s_0)
\end{aligned}$$

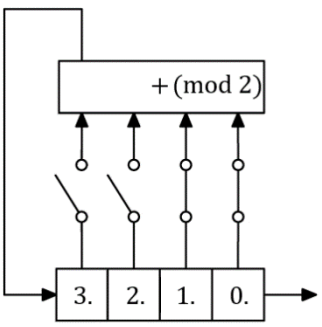
azaz

$$\boldsymbol{L}^N(s_{N-1}, \dots, s_1, s_0) = \textstyle\sum_{i=0}^{N-1} a_i \boldsymbol{L}^i(s_{N-1}, \dots, s_1, s_0),$$

amiből

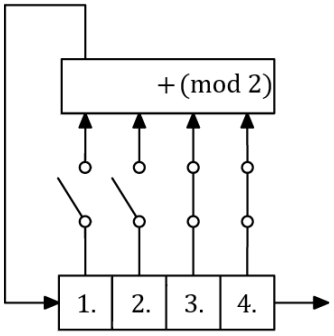
$$\left(\boldsymbol{L}^N - \sum_{i=0}^{N-1} a_i \boldsymbol{L}^i\right)(s_{N-1}, \dots, s_1, s_0) = (0, \dots, 0, 0)$$

következik. Az így kapott kifejezés bal oldalát nevezzük a LFSR karakterisztikus polinomjának.



Ezt felhasználva már könnyen felrajzolható a feladat polinomjához tartozó LFSR, mert a karakterisztikus polinomban szereplő tagok (leszámítva a legmagasabb hatványt) a visszacsatolások helyeit adják meg (ügyeljünk a shift regiszter celláinak a sorszámozására).

b) A karakterisztikus és a feedback polinom egymás reciprokai.



Azaz, ha $P(x)$a karakterisztikus polinom, akkor a feedback polinom $x \cdot P\left(\frac{1}{x}\right) = x^4 \cdot (x^{-4} + x^{-1} + 1) = 1 + x^3 + x^4$ alakú. Az ennek megfelelő LFSR-t az ábra mutatja (az x-ek kitevői ismét a visszacsatolások helyeit mutatják; ügyeljünk a cellák helyes számozására).

c) Triviális.

d) Egy N bites LSFR periódusa akkor éri el a maximális $2^N - 1$-et (és így akkor generálja a leghosszabb álvéletlen sorozatot), ha a karakterisztikus (vagy feedback) polinomja primitív. Egy N-edfokú polinomot akkor nevezünk primitívnek, ha

- irreducíbilis (azaz nem bontható fel két, nála alacsonyabb fokú polinom szorzatára),
- osztja $x^{2^{N-1}} + 1$-et, de
- nem osztja $x^d + 1$, ahol d osztója $N - 1$-nek.

Ezek az állítások most teljesülnek, ezért a periódus hossza minden nem “csupanulla” kezdeti állapot esetében $2^4 - 1$ lesz. Az ismétlődés eme maximális hosszú periódusát megfigyelhettük az előző feladatrészben is.

4.4. Feladat

Ön véletlenül meghallja a

```
0000110 1101110 1010111 1110111 0100110 1111001 0011110 0001011 0001010
1010101
```

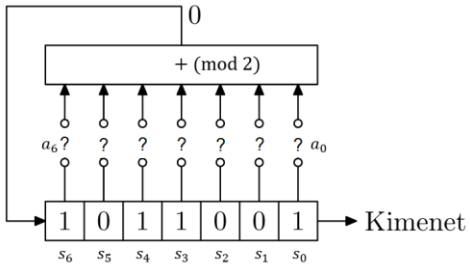
szigorúan titkos üzenetet (az üres helyek ismét csak az olvashatóságot segítik). Jó oka van feltételezni, hogy az eredeti üzenetet 7 bites ASCII kóddal kódolták, mielőtt azt egy 7-bites LFSR-el működő folyamrejtjelezővel titkosították volna. Tudja, hogy az nyílt szöveg az `Su` karakterekkel kezdődött. Fejtse vissza a teljes szöveget!

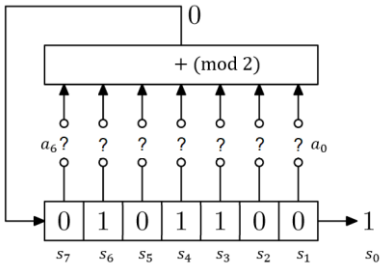
Megoldás:

A 7 bites ASCII kód a betűket, a számjegyeket és az írásjeleket 32 és 127 közötti 7 bites egész számmal kódolja. A nagybetűk a 65-90 tartományból, a kisbetűk a 97-112 tartományból kerülnek ki.

7 bites ASCII kóddal kódolva az `Su` szekvencia a `1010011 1110101` bitsorozatként írható le.

Kivonva ezt a 14 bitet a rejtjelezett szövegből megkapjuk a kulcs 14 bitjét: `1010101 0011011`. Ekkor az alábbi egyenletrendszert írhatjuk fel (lásd a működés első két lépését az ábrákon jobbra):





$$0 = a_0 + a_2 + a_4 + a_6$$

$$0 = a_1 + a_3 + a_5$$

$$1 = a_2 + a_4 + a_6$$

$$1 = a_0 + a_3 + a_5$$

$$0 = a_0 + a_1 + a_4 + a_6$$

$$1 = a_1 + a_2 + a_5$$

$$1 = a_0 + a_2 + a_3 + a_6$$

Az egyenletrendszert megoldva az

$$(a_0, \dots, a_6) = (1,1,0,1,0,0,1)$$

eredmény adódik. Így meghatározhatóak a LFSH által előállított teljes sorozat, annak ismeretében a teljes nyílt szöveg is helyreállítható: `Surrender`!

4.5. Feladat

Egyik jó ismerőse angol nyelven írt, csak nagybetűket tartalmazó szöveget küld el Önnek titkosítva. Tudja, hogy minden betűt a titkosítás előtt az 5 bites nemzetközi távíró kóddal (ITA2 variáns) lett kódolva. Ismerőse az így kapott biteket egy 4 bites lineárisa visszacsatolt léptető regiszterrel (LFSR) működő folyamrejtjelezővel titkosította. Az eredményként kapott titkosított szöveg az alábbi (az üres helyek csak az olvashatóságot segítik, azokat nem tartalmazza a titkosított üzenet):

`10111 01101 10100 00110 11000`

`11101 10000 11000 11111 01111 01011.`

A	11000
B	10011
C	01110
D	10010
E	10000
F	10110
G	01011
H	00101
I	01100
J	11010
K	11110
L	01001
M	00111
N	00110
O	00011
P	01101

Q	11101
R	01010
S	10100
T	00001
U	11100
V	01111
W	11001
X	10111
Y	10101
Z	10001
Letters	11111
Figures	11011
Line feed	01000
Carriage return	00010
Word space	00100
All space	00000

Tudja, hogy az titkosított szöveg első két betűje `th`.

a) Határozza meg a titkosításra használt shift regisztert és adja meg a kezdőállapotát!

b) Fejtse vissza a titkosított szöveget.

Megoldás:

a) A titkosított szöveg első két betűje `th`, ebből és a titkosított szövegből meghatározható a kulcs első 10 bitje: `0000100101` ⊕ `1011101101` = `1011001000`.

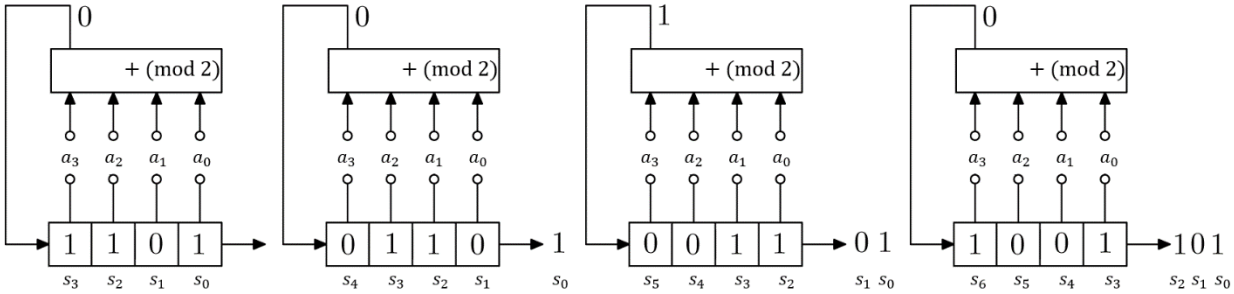
Így az alábbi egyenletek írhatóak fel:

$$0 = 1 \cdot a_0 + 0 \cdot a_1 + 1 \cdot a_2 + 1 \cdot a_3$$

$$0 = 0 \cdot a_0 + 1 \cdot a_1 + 1 \cdot a_2 + 0 \cdot a_3$$

$$1 = 1 \cdot a_0 + 1 \cdot a_1 + 0 \cdot a_2 + 0 \cdot a_3$$

$$0 = 1 \cdot a_0 + 0 \cdot a_1 + 0 \cdot a_2 + 1 \cdot a_3$$



Az egyenletrendszer egyetlen megoldása az $a_0 = a_3 = 1$ és $a_1 = a_2 = 0$. A kulcs első 8 bitje `10110010`, ezért a shift regiszter kezdeti értéke `1011`.

b) Az előbb előállított shift regiszter kimenete

`10110 01000 11110 10110 01000 11110 10110 01000 11110 10110 01000`

Összeadva a titkosított szöveggel a

`00001 00101 01010 10000 10000 00011 00110 10000 00001 11001 00011`

nyílt szöveget kapjuk, amely a távíró kóddal visszakódolva a `threeonetwo`.

4.6. Feladat

Generáljon álvéletlen számokat az RC4-es módszerrel!

Megoldás:

Az RC4 egy (pl. nem LFSR alapú folyamrejtjelzéshez használt) álvéletlenszám generátor. A számok generálására egy 256 bájtos önmagát módosító permutációs táblát használ.

A módszer első lépésként (Key Scheduling Algorithm, KSA) egy 256 byte elemű S tömböt inicializál:

```
begin ksa(with int keylength, with byte key[keylength])
    for i from 0 to 255
        S[i] := i
    endfor
    j := 0
    for i from 0 to 255
        j := (j + S[i] + key[i mod keylength]) mod 256
        swap(S[i],S[j])
    endfor
end
```

Ezek után az álvéltlenszámok generálása az alábbi pszeudokód szerint történik:

```
begin prga(with byte S[256])
    i := 0
    j := 0
    while GeneratingOutput:
        i := (i + 1) mod 256
        j := (j + S[i]) mod 256
        swap(S[i],S[j])
        output S[(S[i] + S[j]) mod 256]
    endwhile
end
```

A módszert széles körben alkalmazták (SSL, WEP), azonban eredeti verziója feltörhető.

4.7. Feladat

Alice és Bob Diffie-Hellman kulcscserét hajt végre a $p = 941$ és a $g = 627$ nyilvános paraméterekkel. Mutassa be a titkos kulcs generálását és a kulcscsere lépéseit!

Megoldás:

A Diffie-Hellman kulcscsere lépéseit az alábbi táblázat foglalja össze:

1. publikus paraméterek létrehozása	
p (nagy, 1000 bit) prím és g megválasztása	
2. titkos számítás	
Alice	**Bob**
titkos a választása	titkos b választása
$A \equiv g^a \pmod{p}$	$B \equiv g^b \pmod{p}$
3. publikus kulcscsere	
Alice elküldi A-t Bobnak $\longrightarrow$	A
B $\longleftarrow$	Bob elküldi B-t Alice-nak
4. titkos közös kulcs meghatározása	
$B^a \pmod{p}$ meghatározása	$A^b \pmod{p}$ meghatározása
a közös titkos kulcs: $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$	

Legyen Alice titkos kulcsa $a = 347$. Ekkor $A = 390 \equiv 627^{347} (\mathrm{mod}\ 941)$. Bob titkos kulcsa pedig legyen $b = 781$. Így $B = 691 \equiv 627^{781} (\mathrm{mod}\ 941)$. Alice elküldi Bobnak a 390-et, míg Bob elküldi Alice-nek a 691-et. Az $A = 390$ és $B = 691$ számok publikusak. Az $a = 347$ és $b = 781$ számok azonban továbbra is titkosak, nem kerülnek továbbításra a csatornán, ezek meghatározása A-ból és B-ből nehéz feladat.

Végezetül Alice és Bob kiszámolják a közös titkot: $470 \equiv 627^{781 \cdot 347} (\mathrm{mod}\ 941)$.