Poglavje 1

Klasična kriptografija

1.1 Uvod: nekateri preprosti kriptosistemi

Osnovni namen kriptografije je omogočiti dvema človekoma, ki ju bomo imenovali Anita in Bojan, da se sporazumevata preko nezaščitenega kanala, tako da nasprotnik Oskar ne more razumeti, o čem se pogovarjata. Ta zveza je lahko na primer telefonska linija ali računalniška mreža. Sporočilo, ki ga želi Anita posredovati Bojanu, imenovali ga bomo čistopis, je lahko Angleško besedilo, številski podatki ali karkoli – njegova struktura je nekaj povsem poljubnega. Anita s pomočjo vnaprej določenega ključa čistopis zašifrira in dobljeni tajnopis pošlje po kanalu. Oskar, ki s pomočjo prisluškovanja vidi tajnopis, ne more določiti čistopisa, medtem ko Bojan, ki pozna šifrirni ključ, lahko dešifrira tajnopis in rekonstruira čistopis.

To lahko opišemo bolj formalno v matematičnem jeziku.

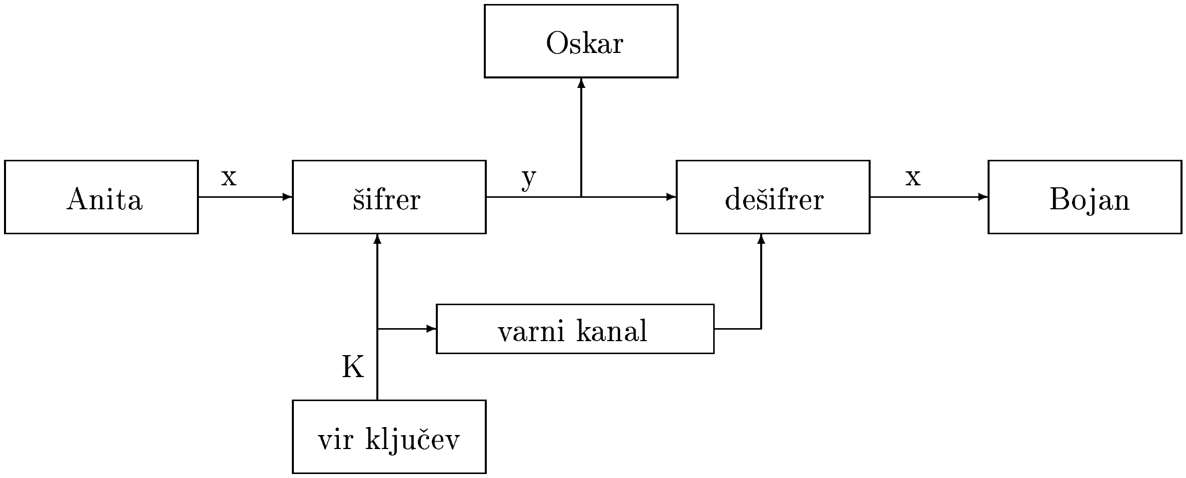
Definicija 1.1 *Kriptosistem je peterica* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, za katero velja:*

1. $\mathcal{P}$ *je končna množica možnih čistopisov*
2. $\mathcal{C}$ *je končna množica možnih tajnopisov*
3. $\mathcal{K}$ *je končna množica možnih ključev*
4. *Za vsak ključ* $K \in \mathcal{K}$ *obstaja šifrirni postopek* $e_K \in \mathcal{E}$ *in dešifrirni postopek* $d_K \in \mathcal{D}$*. Vsaka* $e_K : \mathcal{P} \to \mathcal{C}$ *in* $d_K : \mathcal{C} \to \mathcal{P}$ *sta taki funkciji, da velja* $d_K(e_K(x)) = x$ *za vsak čistopis* $x \in P$*.*

Najpomembnejša je lastnost 4. Pove nam, da če čistopis x zašifriramo s pomočjo e_K in tako dobljeni tajnopis dešifriramo z d_K, dobimo nazaj originalni čistopis x.

Anita in Bojan bosta uporabljala naslednji protokol za uporabo specifičnega kriptosistema. Najprej si izbereta naključni ključ $K \in \mathcal{K}$. To naredita takrat, ko sta skupaj in ju Oskar ne opazuje, ali ko imata dostop do zašcitenega kanala (v tem primeru ne rabita biti skupaj). Recimo, da želi Anita kasneje Bojanu poslati sporočilo preko nezaščitenega kanala. Predpostavimo, da je to sporočilo niz

$$x = x_1 x_2 \ldots x_n$$



Slika 1.1: Komunikacijski kanal

za neko naravno število $n \geq 1$ in za $x_i \in \mathcal{P}$, $1 \leq i \leq n$. Vsak x_i je zašifriran s pomočjo šifrirnega postopka e_K, ki ga določa vnaprej izbran ključ K. Torej Anita izračuna $y_i = e_K(x_i)$, $1 \leq i \leq n$ in dobljeni tajnopis

$$y = y_1 y_2 \ldots y_n$$

pošlje preko kanala. Ko Bojan sprejme $y_1 y_2 \ldots y_n$, ga dešifrira s pomočjo dešifrirnega postopka d_K in na ta način dobi čistopis $x_1 x_2 \ldots x_n$. Oglej sliko 1.1, ki predstavlja komunikacijski kanal.

Jasno je, da mora biti vsaka šifrirna funkcija e_K injektivna, sicer tajnopisa ne bi mogli enolično dešifrirati. Na primer, če

$$y = e_K(x_1) = e_K(x_2),$$

kjer je $x_1 \neq x_2$, potem Bojan ne more vedeti, ali naj y dešifrira kot x_1 ali kot x_2. Opazi, da če je $\mathcal{P} = \mathcal{C}$, je vsaka šifrirna funkcija permutacija. Torej, če sta množici čistopisov in tajnopisov enaki, potem vsaka šifrirna funkcija zgolj premeša (permutira) elemente te množice.

1.1.1 Pomični tajnopis

V tem razdelku bomo opisali **pomični tajnopis**, ki temelji na modularni aritmetiki. Najprej navedimo nekaj osnovnih definicij modularne aritmetike.

Definicija 1.2 *Naj bosta a in b celi števili in m naravno število. Potem pišemo $a \equiv b \pmod{m}$, če m deli $b - a$. Izraz $a \equiv b \pmod{m}$ se prebere kot "a je kongruenten b po modulu m". Število m se imenuje modul.*

Délimo a in b z m, pri čemer dobimo celoštevilske kvociente in ostanke, kjer so ostanki med 0 in $m-1$, t.j. $a = q_1 m + r_1$ in $b = q_2 m + r_2$, kjer je $0 \leq r_1, r_2 \leq m-1$. Ni težko videti, da je $a \equiv b \pmod{m}$ natanko tedaj, ko je $r_1 = r_2$. Z oznako $a \bmod m$ bomo označevali ostanek pri deljenju a z m, t.j. vrednost r_1 zgoraj. Torej je $a \equiv b \pmod{m}$ natanko tedaj, ko je $a \bmod m = b \bmod m$. Če a nadomestimo z $a \bmod m$ pravimo, da smo a okrajšali po modulu m.

OPOMBA. V mnogih programskih jezikih je $a \bmod m$ definirano kot število med $-m+1$ in $m-1$ z enakim predznakom kot a. Na primer, $-18 \bmod 7$ bi bilo -4 namesto 3, kot je zgoraj definirano. Za naše namene je primerneje definirati $a \bmod m$ kot nenegativno število. ⧫

Sedaj lahko definiramo aritmetiko po modulu m: $\mathbb{Z}_m$ definiramo kot množico $\{0, \ldots, m-1\}$, opremljeno z dvema operacijama, $+$ in $\times$. Seštevanje in množenje v $\mathbb{Z}_m$ delujeta enako kot pravo seštevanje in množenje s to razliko, da se rezultati okrajšajo po modulu m.

Na primer, da hočemo izračunati 11×13 v $\mathbb{Z}_16$. V celih številih je $11 \times 13 = 143$. Da bi reducirali 143 po modulu 16, preprosto na dolgo zdelimo: $143 = 8*16+15$, torej je $143 \bmod 16 = 15$, zato je $11 \times 13 = 15$ v $\mathbb{Z}_16$.

Te definicije seštevanja in množenja v $\mathbb{Z}_m$ zadoščajo večini znanih pravil aritmetike. Spodaj je podan seznam teh lastnosti, ki jih navajamo brez dokaza:

1. $\mathbb{Z}_m$ je *zaprta za seštevanje*, t.j. za vsaka $a, b \in \mathbb{Z}_m$ je $a + b \in \mathbb{Z}_m$
2. seštevanje je *komutativno*, t.j. za vsaka $a, b \in \mathbb{Z}_m$ je $a + b = b + a$
3. seštevanje je *asociativno*, t.j. za vse $a, b, c \in \mathbb{Z}_m$ je $(a + b) + c = a + (b + c)$
4. 0 je *enota za seštevanje*, t.j. za vsak $a \in \mathbb{Z}_m$ je $a + 0 = 0 + a = 0$
5. *Nasprotni element* poljubnega elementa $a \in \mathbb{Z}_m$ je $m - a$, t.j. $a + (m - a) = (m - a) + a = 0$ za vsak $a \in \mathbb{Z}_m$
6. $\mathbb{Z}_m$ je *zaprta za množenje* t.j. za vsaka $a, b \in \mathbb{Z}_m$ je $ab \in \mathbb{Z}_m$
7. množenje je *komutativno*, t.j. za vsaka $a, b \in \mathbb{Z}_m$ je $ab = ba$
8. množenje je *asociativno*, t.j. za vse $a, b, c \in \mathbb{Z}_m$ je $(ab)c = a(bc)$
9. 1 je *enota za množenje*, t.j. za vsak $a \in \mathbb{Z}_m$ je $1 \times a = a \times 1 = a$
10. Množenje in seštevanje povezuje *distributivni zakon*, t.j. za poljubne $a, b, c \in \mathbb{Z}_m$ je $(a + b)c = (ac) + (bc)$ in $a(b + c) = (ab) + (ac)$.

Lastnosti 1, 3-5 povejo, da je $\mathbb{Z}_m$ *grupa* za seštevanje. Ker velja tudi lastnost 2, je $\mathbb{Z}_m$ *abelova* grupa.

Lastnosti 1-10 pokažejo, da je $\mathbb{Z}_m$ dejansko *kolobar*. Videli bomo še mnogo primerov grup in kolobarjev v nadaljevanju knjige. Znani primeri kolobarjev so cela števila, $\mathbb{Z}$, realna števila, $\mathbb{R}$, in kompleksna števila $\mathbb{C}$. Ti kolobarji so vsi neskončni, naša pozornost pa bo skoraj povsem namenjena samo končnim kolobarjem.

Ker v $\mathbb{Z}_m$ obstajajo nasprotni elementi, lahko v $\mathbb{Z}_m$ tudi odštevamo. Za $a, b \in \mathbb{Z}_m$ definiramo $a - b = a + m - b \bmod m$. Lahko pa bi kar izračunali $a - b$ kot v celih številih in nato reducirali po modulu m.

Na priemer, da izračunamo $11 - 18$ v $\mathbb{Z}_{31}$, izračunamo $11 + 13 \bmod 31 = 24$. Lahko pa najprej odštejemo 18 od 11, dobimo -7 in nato izračunamo $-7 \bmod 31 = 24$.

Slika 1.2 predstavlja **pomični tajnopis**. Definiran je nad $\mathbb{Z}_{26}$, saj angleška abeceda vsebuje 26 črk, lahko pa bi bil definiran nad $\mathbb{Z}_m$ za poljuben m. Enostavno je videti, da **pomični tajnopis** ustreza definiciji tajnopisa zgoraj, t.j. $d_K(e_K(x)) = x$ za vsak $x \in \mathbb{Z}_{26}$.

OPOMBA. V primeru, ko je $K = 3$, se tajnopis pogostokrat imenuje **Cezarjev tajnopis**, saj je dokazano, da ga je uporabljal Julij Cezar. ⧫

Pomični tajnopis (z modulom 26) uporabljamo tako, da povežemo posamezne črke angleške abecede z ostanki po modulu 26 na naslednji način: $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$. Ker bomo te

Naj bo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. Za $0 \leq K \leq 25$ definirajmo

$$e_K(x) = x + K \bmod 26$$

in

$$d_K(y) = y - K \bmod 26$$

$(x, y \in \mathbb{Z}_{26}.)$

Slika 1.2: Pomični tajnopis

zveze rabili v večih primerih, jih zapišimo v tabeli:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Prikažimo uporabo na preprostem primeru.

Primer 1.1
Recimo, da je ključ za **Pomični tajnopis** enak $K = 11$ in da je čistopis

`wewillmeetatmidnight.`

Najprej pretvorimo čistopis v zaporedje števil z uporabo zgoraj opisanih zvez, da dobimo

$$\begin{array}{cccccccccc} 22 & 4 & 22 & 8 & 11 & 11 & 12 & 4 & 4 & 19 \\ 0 & 19 & 12 & 8 & 3 & 13 & 8 & 6 & 7 & 19 \end{array}$$

Sedaj vsakemu številu prištejemo 11 in pokrajšamo po modulu 26. Dobimo

$$\begin{array}{cccccccccc} 7 & 15 & 7 & 19 & 22 & 22 & 23 & 15 & 15 & 4 \\ 11 & 4 & 23 & 19 & 14 & 24 & 19 & 17 & 18 & 4 \end{array}$$

Preostane nam še, da številke pretvorimo nazaj v črke. Tajnopis se potem glasi:

`HPHTWWXPPELEXTOYTRSE.`

Bojan dešifrira tajnopis tako, da ga najprej pretvori v zaporedje števil, odšteje 11 po modulu 26 in dobljeno pretvori nazaj v črke. $\diamondsuit$

OPOMBA. V zgornjem primeru smo čistopis zapisali z malimi črkami, tajnopis pa z velikimi. To pisavo bomo uporabljali tudi v prihodnje. $\blacklozenge$

Če hočemo, da ima kriptosistem praktično vrednost, mora imeti določene lastnosti. Neformalno navedimo dve taki lastnosti.

1. Vsak šifrirni postopek e_K in vsak dešifrirni postopek d_K se more enostavno izvesti.
2. Nasprotnik ne more določiti niti ključa K, ki je bil uporabljen, niti čistopisa x, če ima samo tajnopis y.

Druga lastnost na nek način definira pojem ,,varnosti". Postopek računanja ključa K iz danega tajnopisa y se imenuje *kriptoanaliza.* (Te pojme bomo v nadaljevanju natančneje definirali.) Opazimo, da če Oskar lahko ugotovi ključ K, potem lahko dešifrira tajnopis y na enak način kot Bojan, z uporabo d_K. Torej je ugotavljanje ključa K vsaj tako zehtevno kot ugotavljanje čistopisa x.

Vidimo, da **Pomični tajnopis** (po modulu 26) ni varen, saj ga lahko kriptoanaliziramo z očitno metodo *požrešnega iskanja ključa.* Ker je vseh možnih ključev samo 26, je enostavno poizkušati vse možne dešifrirne postopke d_K, dokler ne dobimo ,,smiselnega" čistopisa. To je prikazano v naslednjem primeru.

Primer 1.2
Na danem tajnopisu

```
JBCRCLQRWCRVNBJENBWRWN
```

zaporedoma preizkušamo dešifrirne postopke d_0, d_1, itd. Dobimo naslednje:

```
jbcrclqrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlwfklqwlphvdyhvqlqh
cuvkvejkpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine
```

Na tem mestu smo našli čistopis in lahko nehamo. Ključ je $K = 9$. ◊

V povprečju bomo našli čistopis po uporabi $26/2 = 13$ dešifrirnih pravil.

Zgornji primer nakazuje, da je potreben pogoj za varnost kriptosistema nepraktičnost požrešnega iskanja ključev, t.j. prostor ključev mora biti zelo velik. Vendar pa velik prostor ključev ni zadosten pogoj za varnost.

1.2 Naloge

1. Spodaj so podani štirje tajnopisi, dobljeni s pomočjo zamenjalnega, Vigenerjevega in afinega tajnopisa, za enega pa postopek šifriranja ni podan. V vseh primerih je potrebno določiti čistopis.

   Podaj jasen opis postopka, ki si ga uporabil v vsakem od primerov. Opis naj vsebuje statistično analizo in izračune, ki si jih opravil.

   Prva dva čistopisa sta vzeta iz "The Diary of Samuel Marchbanks", Robertson Davies, Clark Irwin, 1947; četrti pa je vzet iz "Lake Wobegon Days", Garrison Keillor, Viking Penguin, Inc., 1985.

   (a) **Zamenjalni tajnopis:**

   ```
   EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLW      GYICO XYSIP JCK
   QPKUGKMGOLICGINCGACKSNISACYKZSCK      XECJC KSHYS XCG
   OIDPKZCNKSHICGIWYGKKGKGOLDSILKGO      IUSIG LEDSP WZU
   GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPX      EZGAC GNFGL KNS
   ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUE      KUZCS OCFZC CNC
   IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
   ```

NASVET: F pomeni w.

(b) **Vigenerjev tajnopis:**

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVF   DETDG ILTXR GUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXI   ZAKFT LEWRP TYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPK   QDYHJ VDAHC TRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIA   SPRJA HKJRJ UMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCE   BSHCT JRWXB AFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTI   OVKCG GHJVL NHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCD   YGZWP FDTKF QIY
CWHJVLNHIQIBTKHJVNPIST
```

(c) **Afini tajnopis:**

```
KQEREJEBCPPCJCRKIEACUZBKRVPKRBCI   BQCAR BJCVF CUP
KRIOFKPACUZQEPBKRXPEIIEABDKPBCPF   CDCCA FIEAB DKP
BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDC   CJCID FUIXP AFF
ERBICZDFKABICBBENEFCUPJCVKABPCYD   CCDPK BCOCP ERK
IVKSCPICBRKIJPKABI
```

(d) **Neznan tajnopis:**

```
BNVSNSIHQCEELSSKKYERIFJKXUMBGYKA   MQLJT YAVFB KVT
DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROY   GESEB UUALR WXM
MASAZLGLEDFJBZAVVPXWICGJXASCBYEH   OSNMU LKCEA HTQ
OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDV   YDHAV FJXZI BKC
GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMA   SCSPB NLHJM BLR
FFJELHWEYLWISTFVVYFJCMHYUYRUFSFM   GESIG RLWAL SWM
NUHSIMYYITCCQPZSICEHBCCMZFEGVJYO   CDEMM PGHVA AUM
ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHF   RAYIS YSGKV SUU
HYHGGCKTMBLRX
```

2. (a) Koliko je obrnljivih 2×2 matrik nad $\mathbb{Z}_{26}$?

   (b) Naj bo p praštevilo. Pokaži, da je število obrnljivih 2×2 matrik nad $\mathbb{Z}_p$ enako $(p^2-1)(p^2-p)$.

   NASVET: Ker je p praštevilo, je $\mathbb{Z}_p$ obseg. Upoštevaj dejstvo, da je matrika z elementi iz obsega obrnljiva natanko tedaj, ko so njene vrstice linearno neodvisne(t.j. ne obstaja neničelna linearna kombinacija vrstic, katere vsota bi bila ničelni vektor).

   (c) Naj bo p praštevilo in $m \geq 2$ naravno število. Poišči formulo za število obrnljivih $m \times m$ matrik nad $\mathbb{Z}_p$.

3. Včasih je koristno izbrati tak ključ, da je operacija šifriranja identična operaciji dešifriranja. V primeru Hillovega tajnopisa to pomeni, da iščemo matrike K, za katere velja $K^{-1} = K$ (take matrike imenujemo *involucijske*). Pravzaprav je Hill priporočal uporabo involucijskih matrik za ključe v njegovem tajnopisu. Določi število involucijskih matrik (nad $\mathbb{Z}_{26}$) v primeru $m = 2$.

   NASVET: Uporabi formulo iz izreka 1.3 in opazi, da za involucijsko matriko velja $\det A = \pm 1$.

4. Recimo, da nam nekdo pove, da iz čistopisa

   `breathtaking`

   dobimo tajnopis

   `RUPOTENTOSUP` ,

   kjer smo uporabili Hillov tajnopis (toda m ni podan). Določi šifrirno matriko.

5. Afini Hillov tajnopis je naslednja modifikacija Hillovega tajnopisa: naj bo m naravno število in definirajmo $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$. V tem tajnopisu ključ K predstavlja par (L, b), kjer je L $m \times m$ obrnljiva matrika nad $\mathbb{Z}_{26}$, $b \in (\mathbb{Z}_{26})^m$. Za $x = (x_1, \ldots x_m) \in \mathcal{P}$ in $K = (L, b) \in \mathcal{K}$ izračunamo $y = e_K(x) = (y_1, \ldots, y_m$ s formulo $y = xL + b$. Torej, če je $L = (l_{i,j})$ in $b = (b_1, \ldots, b_m)$, je

$$(y_1, \ldots, y_m) = (x1, \ldots, x_m) \begin{pmatrix} l_{1,1} & l_{1,2} & \cdots & l_{1,m} \\ l_{2,1} & l_{2,2} & \cdots & l_{2,m} \\ \vdots & \vdots & & \vdots \\ l_{m,1} & l_{m,2} & \cdots & l_{m,m} \end{pmatrix} + (b_1, \ldots, b_m).$$

Predpostavi, da je Oskar ugotovil, da čistopisu

adisplayedequation

ustreza tajnopis

DSRMSIOPLXLJBZULLM

in Oskar ve, da je $m = 3$. Izračunaj ključ ter opiši ves postopek.

6. Tukaj je podan način, kako lahko dešifriramo Hillov tajnopis, če poznamo samo tajnopis. Recimo, da veš, da je $m = 2$. Razbij tajnopis v bloke dolžine 2 (pare). Vsak tak par predstavlja zašifriran par čistopisa z neznano šifrirno matriko. Izberi najpogostejši par v tajnopisu in predpostavi, da je v čistopisu to eden izmed pogostejših parov, ki so navedeni pred tabelo 1.1 (na primer TH ali ST). Za vsak tak par nadaljuj kot v primeru napada s poznanim čistopisom, dokler ne najdeš pravilne šifrirne matrike.

   Primer tajnopisa, ki ga dešifriraj s pomočjo te metode:

   LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZ YVAP EWLMG QWYA
   XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPR IQSM HNOCV AXFV

7. Naslednji tajnopis je poseben primer permutacijskega tajnopisa. Naj bosta m, n naravni števili. Zapiši čistopis po vrsticah v $m \times n$ pravokotnike. Nato tvori tajnopis tako, da jemlješ stolpce teh pravokotnikov. Na primer, če je $m = 4, n = 3$, potem bi čistopis "cryptography" zašifrirali s tvorjenjem naslednjega pravokotnika:

   cryp
   togr
   aphy

   Tajnopis bi se glasil "CTAROPYGHPRY".

   (a) Opiši, kako Bojan lahko dešifrira tajnopis (pri danih vrednostih m in n)

   (b) Dešifriraj naslednji tajnopis, ki je dobljen s to metodo:

   MYAMRARUYIQTENCTORAHROYWDSOYEOUAR RGDE RNOGW

8. Obstaja osem različnih linearnih rekurzij stopnje štiri s $c_0 = 1$. Ugotovi, katere izmed teh rekurzij dajo tok ključev s periodo 15 (če je podan neničelni začetni vektor).

9. Namen naslednje naloge je, da dokažeš trditev ob koncu razdelka 1.2.5, da je $m \times m$ matrika koeficientov obrnljiva. Ta trditev je ekvivalentna trditvi, da so vrstice matrike linearno neodvisni vektorji nad $\mathbb{Z}_2$.

   Kot prej predpostavi, da je rekurzija oblike

$$z_{m+1} = \sum_{j=0}^{m-1} c_j z_{i+j} \mod 2.$$

$(z_1, \ldots, z_m)$ predstavlja začetni vektor. Za $i \geq 1$ definiraj

$$v_i = (z_i, \ldots, z_{i+m-1}).$$

Opazi, da ima matrika koeficientov za svoje vrstice natanko vektorje $v_1, \ldots, v_m$. Torej je tvoj cilj dokazati, da je teh m vektorjev linearno neodvsinih.

Dokaži naslednje trditve:

(a) Za vsak $i \geq 1$ je

$$v_{m+i} = \sum_{j=0}^{m-1} c_j v_{i+j} \mod 2.$$

(b) Naj bo h najmanjše naravno število, za katerega obstaja taka netrivialna linearna kombinacija vektorjev $v_1, \ldots, v_h$, da je njihova vsota vektor $(0, \ldots, 0)$ po modulu 2. Potem je

$$v_h = \sum_{j=0}^{h-2} \alpha_j v_{j+1} \mod 2,$$

kjer niso vsi α_j enaki nič. Opazi, da je $h \leq m+1$, saj je poljubnih $m+1$ vektorjev v m razsežnem prostoru linearno odvisnih.

(c) Dokaži, da mora tok ključev zadoščati rekurziji

$$z_{h-1+i} = \sum_{j=0}^{h-2} \alpha_j z_{j+i} \mod 2$$

za vsak $i \geq 1$.

(d) Če bi veljalo $h \leq m$, potem bi tok ključev zadoščal linearni rekurziji stopnje manj kot m, kar bi bilo protislovje. Torej mora veljati $h = m+1$ in matrika je zato obrnljiva.

10. Dešifriraj naslednji tajnopis, dobljen s pomočjo tajnopisa z lastnim ključem, z uporabo metode požrešnega iskanja ključa:

```
MALVVMAFBHBUQPTSOXALTGVWWRG
```

11. Naslednji tokovni tajnopis je modifikacija Vigenerjevega tajnopisa. S pomočjo ključa $(K_1, \ldots K_m)$ dolžine m konstruiraj tok ključev po pravilu $z_i = K_i (1 \leq i \leq m), z_{i+m} = z_i + 1 \bmod 26 (i \geq m+1)$. Z drugimi besedami, vsakič ko uporabimo ključ, zamenjamo vsako črko z njenim naslednikom po modulu 26. Na primer, če je ključ *SUMMER*, uporabimo *SUMMER* za prvih šest črk, *TVNNFS* za naslednjih šest itd.

Opiši, kako lahko uporabiš princip indeksa naključja, da najprej določiš dolžino ključa, nato pa ključ tudi dejansko poiščeš.

Preizkusi svojo metodo tako, da dešifriraš naslednji tajnopis:

```
IYMYSILONRFNCQXQJEDSHBUIBCJUZBOL      FQYSC HATPE QGQ
JEJNGNXZWHHGWFSUKULJQACZKKJOAAHGK     EMTAF GMKVR DO
PXNEHEKZNKFSKIFRQVHHOVXINPHMRTJPY     WQGJW PUUVK FP
OAWPMRKKQZWLQDYAZDRMLPBJKJOBWIWPS     EPVVQ MBCRY VC
RUZAAOUMBCHDAGDIEMSZFZHALIGKEMJJF     PCIWK RMLMP IN
AYOFIREAOLDTHITDVRMSE
```

Čistopis je iz knjige "The Codebreakers", David Kahn, Macmillan, 1967.