0.1 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:**

   ```
   EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
   QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
   OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
   GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
   ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
   IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
   ```

   NASVET: F pomeni w.

   (b) **Vigenerjev tajnopis:**

   ```
   KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
   DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
   QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
   SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
   GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
   PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
   FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
   CWHJVLNHIQIBTKHJVNPIST
   ```

   (c) **Afini tajnopis:**

   ```
   KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP
   KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKP
   BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF
   ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK
   IVKSCPICBRKIJPKABI
   ```

   (d) **Neznan tajnopis:**

   ```
   BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVT
   DVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXM
   MASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQ
   OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC
   GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLR
   FFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWM
   NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUM
   ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUU
   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 $x = (x_1, \dots x_m) \in \mathcal{P}$ in $K = (L, b) \in \mathcal{K}$ izračunamo $y = e_K(x) = (y_1, \dots, y_m$ s formulo $y = xL + b$. Torej, če je $L = (l_{i,j})$ in $b = (b_1, \dots, b_m)$, je

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

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:

`LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA`
`XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV`

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:

MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW

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:

    ```
    IYMYSILONRFNCQXQJEDSHBUIBCJUZBOLFQYSCHATPEQGQ
    JEJNGNXZWHHGWFSUKULJQACZKKJOAAHGKEMTAFGMKVRDO
    PXNEHEKZNKFSKIFRQVHHOVXINPHMRTJPYWQGJWPUUVKFP
    OAWPMRKKQZWLQDYAZDRMLPBJKJOBWIWPSEPVVQMBCRYVC
    RUZAAOUMBCHDAGDIEMSZFZHALIGKEMJJFPCIWKRMLMPIN
    AYOFIREAOLDTHITDVRMSE
    ```

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