TKK DN1

Janez Justin, 63180016

March 17, 2021

1 Vigenerjeva šifra

1.1 Encrypt

Besedilo in ključ sta predstavljena kot niz znakov, ki ju pretopim v dva seznama števila. Število dobim kot: ASCII vrednost znaka − 65.
Sedaj se lahko zapeljem preko vseh elementov številske predstavitve besedila in izračunam i-ti element kriptograma na sledeč način:

$$kriptogram[i] = besedilo[i] + ključ[j](mod 26)$$

kjer je j enak ostanku pri deljenju i z dolžino ključa. Tako dobim številsko predstavitev kriptograma. Vsem elementom kriptograma prištejem 65 in upoštevam ASCII vrednosti, da dobim kriptogram predstavljen kot niz.

1.2 Decrypt

Podobno storim za dekriptiranje sporočila, le da za izračun besedila uporabljam sledečo enačbo:

$$besedilo[i] = kriptogram[i] - ključ[j](mod 26)$$

1.3 Dolžina ključa

Razdalja med dvema ponovljenima nizoma predstavlja možno ponovitev šifriranja enakega podniza v originalnem besedilu z istim delom ključa. To poveča možnost, da dolžina ključa deli razdaljo med podnizoma.
Za določanje dolžine ključa poiščem ponavljajoče se nize dolžine 3 in razdalje med njimi. Za vsak ponovljen niz poiščem delitelje razdalje. Za vsakega delitelja si hranim število ponovitev v seznamu fiksne dolžine, za katero upam, da je večja od dejanske dolžine ključa (v oddani kodi je dolžina seznama 50). Ta seznam uredim padajoče po velikosti in si zapomnim kam se je premaknil posamezen indeks. Za indekse, ki se je premaknil na začetna mesta urejene tabele, trdim, da imajo največjo možnost, da so dolžina ključa.

1.4 Iskanje ključa

Tu izkoristim dejstvo, da se črke v angleščini pojavljajo z določeno frekvenco. Uporabim tudi poznavanje dolžine ključa iz prejšnje točke.
Za dolžino ključa d razdelim kriptogram na d podtekstov. i-ti tekst se začne i-tem mestu kriptograma in vzame vsak naslednji d-ti znak v besedilu. Naprimer za kriptogram=ABCDEF, $d = 2$ dobim besedili ACE in BDF.
Vsako besedilo lahko sedaj obravnavam kot Cesarjevo šifro. S pomočjo frekvenčne analize pogledam pri katerem zamiku besedila $z_i \in \{1, 2...26\}$ se i-to besedilo najbolje prilega porazdelitvi črk v angleški abecedi. Ko to storim za vsak $i <= d$, lahko sestavim seznam $[z_1, z_2, ...z_d]$, ki ga pretopim v besedilo, enako kot to storim s kriptogramom v točki 1.1.

1.5 Rezultat

Kriptogram priložen v navodilih se prevede v:
ITHASLONGBEENAGRAVEQUESTIONWHETHERANYGOVE RNMENTNOTTOOSTRONGFORTHELIBERTIESOFITSPEOPL ECANBESTRONGENOUGHTOMAINTAINITSEXISTENCEING REATEMERGENCIESONTHISPOINTTHEPRESENTREBELLIO NBROUGHTOURREPUBLICTOASEVERETESTANDTHEPRES IDENTIALELECTIONOCCURRINGINREGULARCOURSEDURI NGTHEREBELLIONADDEDNOTALITTLETOTHESTRAINTHE STRIFEOFTHEELECTIONISBUTHUMANNATUREPRACTICA LLYAPPLIEDTOTHEFACTSINTHECASE
s ključem: **MATH**
Napogostejša dolžina ključa, ki jo program zazna je 2, vendar se izkaže, da je dejanska dolžina 4 (napaka je lahko pričakovana, ker vsako število deljivo s 4, bo deljivo tudi s 2). Zato sem zahteval še uporabnikov vnos, ki potrdi, če je besedilo smiselno. Če ni smiselno, potem program poskusi z naslednjo najbolj verjetno dolžino ključa.

2 Hillova šifra

2.1 Encrypt

Besedilo in kjluč tudi tu predstavim kot dve besedili. Besedilo na isti način kot v prejšnji nalogi pretvorim v številski seznam, kjer dodam 0 na konec, če besedilo ni sode dolžine. Tekst "ABCD" pa pretvorim v matriko A=$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, kjer so črke številska predstavitev njihovih velikih črk. Po pretvorbi iz besedila v matriko program preveri, da ima matrika determinanto v $\mathbb{Z}_{26}^*$.
Za vsak $x_i = [b_{2i}, b_{2i+1}]^T$, kjer je b besedilo in $i < \frac{len(b)}{2}$ poračunam $c_i = A * x_i$. Vektorji c_i zloženi v seznam: $[c_1^T, c_2^T, ...]$ predstavljo številsko predstavitev kriptograma, ki ga pretvorim v niz(enako kot pri 1.1).

2.2 Decrypt

Postopek je enak točki 2.1, le da namesto matrike A uporabljam matriko A^{-1}, ki jo dobim po enačbi:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2.3 Iskanje ključa

Ključ iščem s pregledom vseh možnih matrik velikosti 2x2, ki imajo ustrezno determinanto. Za vsako ustrezno matriko poračunam kakšno besedilo dobim iz poznanega kriptograma. Nad tem besedilom izvedem kriptoanalizo in shranim ključ matrike, če se frekvenca besedila dovolj ujema. Ključ z najboljšim ujemanjem predstavim kot ključ kriptograma.
Ker uporabljam napad z grobo silo je program časovno zahteven, vendar se za matrika 2x2 izvede v približno minuti, kar vzmamem za sprejemljiv čas. V primeru večjih dimenzij matrike program ne bi deloval. Prvič, ker je napisan z mislijo, da bodo ključi matrike velikosti 2x2. Drugič, ker že za 3x3 matrike obstaja 646108188922667329893224 1 možnih matrik, kar bi bilo s trenutno tehnologijo težko pregledati.

2.4 Rezultat

Kriptogram priložen v navodilih se prevede v:
**ITISAVERYPOORTHINGWHETHERFORNATIONSORINDIVID
UALSTOADVANCETHEHISTORYOFGREATDEEDSDONEINT
HEPASTASANEXCUSEFORDOINGPOORLYINTHEPRESENTB
UTITISANEXCELLENTTHINGTOSTUDYTHEHISTORYOFTHE
GREATDEEDSOFTHEPASTANDOFTHEGREATMENWHODID
THEMWITHANEARNESTDESIRETOPROFITTHEREBYSOAST
ORENDERBETTERSERVICEINTHEPRESENTINTHEIRESSEN
TIALSTHEMENOFTHEPRESENTDAYAREMUCHLIKETHEME
NOFTHEPASTANDTHELIVEISSUESOFTHEPRESENTCANBEF
ACEDTOBETTERADVANTAGEBYMENWHOHAVEINGOODF
AITHSTUDIEDHOWTHELEADERSOFTHENATIONFACEDTHE
DEADISSUESOFTHEPASTSUCHASTUDYOFLINCOLNSLIFEWI
LLENABLEUSTOAVOIDTHETWINGULFSOFIMMORALITYAN
DINEFFICIENCYTHEGULFSWHICHALWAYSLIEONEONEAC
HSIDEOFTHECAREERSALIKEOFMANANDOFNATIONITHEL
PSNOTHINGTOHAVEAVOIDEDONEIFSHIPWRECKISENCOU
NTEREDINTHEOTHERA**
s ključem: **ZAFD** oziroma A=$\begin{bmatrix} 25 & 0 \\ 5 & 3 \end{bmatrix}$