Domača naloga 1 iz Teorije kodiranja in kriptografije

Domačo nalogo rešujte samostojno. Oddati je potrebno dokument s kodo preko spletne učilnice. Rezultate lahko podate kot komentarje v kodi ali pa kot ločen dokument. Priporočeno in zaželeno je, da za programski jezik uporabite Python. V kolikor želite uporabiti kak drug jezik, najprej pišite asistentu za potrditev. Rok za oddajo je 26.3.2019. Datoteke pred oddajo združite v eno datoteko (zip, rar,...) z vašim imenom in vpisno v imenu, recimo *tilen_marc_23424123745.zip*.

1. Vigenerjeva šifra:

- Napiši programa *Encrypt(b, k)* in *Decrypt(c, k)*, ki s pomočjo Vigenerjeve šifre šifrira in dešifrira s ključem k. Predpostavi, da sta besedilo in ključ niza nad angleško abecedo brez ločil, presledkov, itd.
- Napiši program, ki za kriptogram c, za katerega vemo, da je dovolj dolgo šifrirano besedilo v angleščini, ugotovi dolžino ključa.
- S pomočjo prejšnje točke napiši program, ki za kriptogram c samodejno najde ključ in ga dešifrira.
- Preizkusi svoj program na kriptogramu iz vaj.

2. Hillov šifra:

- Napiši programa *Encrypt(b, k)*, ki s pomočjo Hillove šifre šifrira s ključem k, in *Decrypt(c, k)*, ki dešifrira. Predpostavi, da so besedila nad angleško abecedo in dimenzija matrike ključa je 2×2. Če besedilo ni večkratnik velikosti ključa, naj ga program poljubno podaljša. Ključ za šifriranje in dešifriranje naj bo isti.
- Napiši program, ki za kriptogram c, za katerega vemo, da je šifrirano besedilo v angleščini, samodejno najde ključ in ga dešifrira. Preizkusi ga na svojem primeru. Bi tvoj program še vedno deloval, če bi bile matrike višjih dimenzij?
- Preizkusi svoj program na šifri:
  STSQALWTCJMIJMTHNFEBWZTVJWMRNNHPMFICJFNWSZSXGW
  PFHHAJFBNTWZTVTHIRMRCGVRJTAFXBWDIVMFWSNSTVLXIR
  ACANWLYSIYVPJQMQNFLNMRPXSBHMWNJTIYNSZNHPHPIMNZ
  DRWBPPNSHMSBUJMUHZXJHMWPSQHHJBMHHMWMJTAFXBWDIC
  VETVLXIRANXFVETVUDWUHBWHEBMBSXHMWEEEHMANWUJUW
  WHAWWSNWZMLJXVXHWTVJTZZICACHHJTNWWTZRHWWTIYJSS
  UWSNSTVLWWWWHHPNSTVSNWWIYNSSOPFHMWEWHMHHMWNJTI
  YNSXPCQJTOQYFPBQKHMWEWHMHHMWNACHRNWHMWBSZWSIOG
  IICVETVLWWWWHHXANZRVZYWXUMVWZHDJHXAANHRUQZZOUN
  BTZTJFNSBUUMBVZSTTLHZXNWDTZELTVPPAJWTICVETVNNHPM
  FVZYWXUTVXBAJSQIUWWMHHMWNACHTGCTJIRGFCGVGSBYAPQI
  TSDWISVPPNNZMWCIRMSFRSXHMWZEENFGDVBMHSYOYJHPBHLA
  NXNNZVOSUSANTCVTVUMPSIATHYFAHEGCSPBWKNZMFWUYFIK
  XBMHHMWAAZWGJJAHSSWKVJANANXFVMAFSENLHMWBLZNDHM
  SBUJMNALWUFRSXWDMFWSVBTHLLJTYOSQWHYAGJHDJTXNNST
  VMXTVJH