Kriptografija

Kriptografija je veda o zapisovanju in branju tajnih sporočil. Tajna sporočila se že od antike uporabljajo v diplomaciji in vojski. S sodobnim načinom komunikacij postajajo tudi stalnica običajnih državljanov. Dostop do naše elektronske pošte ima vzdrževalec strežnika, kjer imamo poštni predal. Če običajna pošta niti ni zanimiva za morebitnega izsiljevalca, tega ne moremo reči za dostop do bančnega računa ali pri plačevanju s kartico preko medmrežja. Ali in kako so ti podatki zaščiteni? Takšna vprašanja si zastavlja kriptografija.
Mi se ne bomo ukvarjali s posebno zapletenimi načini kodiranja, saj bomo zakodirano sporočilo želeli tudi prebrati, ne da bi zato porabili preveč dragocenega časa.
Metode šifriranja sporočil lahko v grobem delimo v dve skupini. Transpozicijsko šifriranje ne spreminja črk ,ampak le njihov vrstni red. Substitucijsko šifriranje pa zamenja črke (številke in druge znake) med seboj ali pa z drugimi označbami.
V tem prispevku se bomo ukvarjali z enostavnim substitucijskim načinom – s t. i. pomično šifro. Le-ta je znana tudi kot Cezarjeva šifra, Julij Cezar jo je namreč uporabljal pri državniških opravkih.
V vseh primerih se bomo ukvarjali le z velikimi črkami slovenske abecede. Ključ je število, ki nam pove, za koliko mest bomo premaknili osnovno abecedo. Recimo, da je ključ 5. Nova abeceda (in pod njo stara) je zdaj

T U V Z Ž A B C Č D E F G H I J K L M N O P R S Š
A B C Č D E F G H I J K L M N O P R S Š T U V Z Ž

Kodiranje poteka takole: Če je v sporočilu A, ga zamenjamo z E, B zamenjamo s F.... Črko iz zgornje vrstice zamenjamo s črko iz spodnje vrstice. Besedo PARALELOGRAM spremeni postopek v UEVERJRTLVES.
Prijatelj, ki mu pošiljamo sporočilo, mora seveda poznati ključ. On bo dekodiral besedilo takole: Če je v sporočilu A ga zamenja s T, če je B ga zamenja z U ... Črko iz spodnje vrstice zamenja s črko iz zgornje.
Seveda se s prijateljem lahko dogovorita, da bosta ključe menjavala vsak dan (v tednu).
Tretja oseba, ki ne pozna ključa, ima kar nekaj dela, da razvozlja zakodirano besedilo. Toda ko enkrat ključ odkrije, hitro lahko prebere nadaljnja besedila. Pri dešifriranju je ugodno, če poznamo področje pogovora (če gre npr. za matematiko, obstaja lahko samo ena beseda, ki ima 12 črk).
V nalogi bomo šifrirali 10 matematičnih pojmov, po dva zaporedna z istim ključem. Poišči matematične pojme, če so šifrirani takole:
ZNSJAVERE, AVNPTAŠNP, VHALN, SČGKŽGC, ŽLVLRČ, LRZHJTČO, ZLDZL, ŽMAUEČHJRSH, FOCTOEŽAČE, UAE

Rešitve so na strani 18!

Izidor Hafner