KRIPTOLOGIJA – PROJEKAT

KRIPTOANALIZA VIGENEREOVE ŠIFRE POMOĆU INDEKSA KOINCIDENCIJE

Student : Tarik Džaka

POJMOVI I DEFINICIJE

Definirajmo prvo *Vigenèreovu šifru:*

Definicija 1. Neka *je* m fiksan prirodan broj. Za ključ $K = (k_1, k_2, \dots, k_m)$ definiramo:

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m),$$

$$d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m),$$

gdje su sve operacije u $\mathbb{Z}_{26}$.

Definicija 2. Neka je $x = x_1x_2 \dots x_n$ niz od *n* slova. *Indeks koincidencije* od *x*, u oznaci $I_c(x)$, definira se kao vjerovatnost da su dva slučajna elementa iz *x* jednaka.

NEFORMALNI OPIS POSTUPKA

Prvi korak je određivanje dužine ključne riječi.Postoji više načina za ovo, ali nas sada interesuje metod koji koristi indeks koincidencije. Ako pretpostavimo da je dužina ključne riječi jednaka m, tada je svako m-to slovo šifrirano sa istim slovom ključa. To znači da će, kada posmatramo grupu svih slova na pozicijama koje daju jednak ostatak po modulu m, indeks koincidencije te grupe biti približan indeksu koincidencije nekog otvorenog teksta na jeziku na kojem je napisana poruka, obzirom da se pomjeranjem svakog slova u otvorenom tekstu neće promjeniti indeks koincidencije. Prema tome, možemo za različito m, odnosno različite dužine ključa, izračunati indeks koincidencije od svake grupe, i ocijeniti za koje m dobijamo da je prosječni indeks koincidencije od svih grupa najbliži indeksu koincidencije za jezik na kojem je napisana otvorena poruka. Onda ćemo za to m pretpostaviti da je dužina ključa jer je to najvjerovatnije.
Drugi korak jeste otkrivanje slova ključa. Opet ćemo podjeliti slova šifrirane poruke u grupe u zavisnosti od ostatka pozicije slova po modulu m. Svakom bloku onda odgovara jedno slovo iz ključa, samo trebamo otkriti koje. Ukoliko bi probali svako slovo abecede, očekujemo da će samo za slovo koje je zaista korišteno za šifrovanje ovoga bloka proizvesti slova sa frekvencijama sličnim kao u bilo kakvom otvorenom tekstu na jeziku poruke. Ovo nam omogućava da isprobamo sva slova, i ponovo nađemo ono slovo koje je najvjerovatnije proizvelo trenutni blok. Ako ovako postupimo za svaki blok, dobit ćemo sva slova ključa. Naravno, nije zagarantovana tačnost ovoga ključa, ali je vrlo vjerovatno tačan, pogotovo ukoliko je šifrirani tekst velik, jer veći tekst povlači i manje odstupanje indeksa koincidencija i frekvencija slova od prosječnih. Puno detaljniji i matematički precizniji opis postupka može se naći na linkovima ispod.

KORISNI LINKOVI

http://e.math.hr/old/vigenere/index.html
http://e.math.hr/old/vigenere/vigjs.html
https://www.youtube.com/watch?v=FdRwxAYq894