- Vižnerova šifra
- Opis
- Kritpoanaliza
- Varijante

Kriptologija 1

Vižnerova šifra

- Vižnerova šifra je metod šifrovanja azbučnog teksta korišćenjem serije Cezarovih šifara, zasnovanih na slovima ključa. Ovo je prosti oblik šifre polialfabetske zamene.
- Metod je prvi opisao Đovan Batista Belazo (ital. Giovan Battista Bellaso)
- U 19. veku je ta šema pogrešno pripisana Blezu de Vižneru (franc. Blaise de Vigenère), tako da je sad poznata kao „Vižnerova šifra“.

Opis

- Kod Cezarove šifre, svako slovo alfabeta se pomera za neki broj mesta; na primer, sa pomakom 3, slovo A postaje D, B postaje E itd.

- Vižnerova šifra se sastoji od niza nekoliko Cezarovih šifara sa različitim pomacima.

- Otvoreni tekst: ATTACKATDAWN
- Ključ: LEMONLEMONLE
- Šifrat: LXFOPVEFRNHR

Kritpoanaliza

- **Kaziskijev test** koristi činjenicu da će pojedine česte reči verovatno biti šifrovane istim slovima ključa, pa će se u šifratu pojaviti ponovljene grupe slova.
- **Fridmanov test** za razbijanje šifre upotrebio "indeks podudarnosti", koji meri neravnomernost frekvencije slova šifre.
- **Kod frekventne analize** kada se odredi dužina ključa, šifrat se deli u sekcije tako da svaka sekcija odgovara ključu za jedno slovo. Svaki deo je ekvivalentan šifratu jedne Cezarove šifre.

Varijante

- Varijanta Vižnerove šifre uzastopni ključ (engl. running key) je takođe nekad smatrana kao neprobojna. Ova verzija kao ključ koristi blok teksta dužine otvorenog teksta. Pošto je ključ dugačak kao i poruka, testovi Kaziskog i Fridmena više ne vrede - ključ se ne ponavlja.

- Ako se koristi ključ koji je potpuno slučajan, ako je dugačak kao poruka i koristi se samo jednom, Vižnerova šifra je teoretski neprobojna.

- U tom slučaju ključ, a ne šifra, obezbeđuje kriptografsku otpornost, i ti sistemi se zajednički zovu "jednokratna beležnica" (engl. one-time pad), nevezano za za to koja šifra je primenjena.

Univerzitet Singidunum

Hvala na pažnji !