Klasična kriptografija

dr Jasmina Novaković

3. KLASIČNA KRIPTOGRAFIJA

- U ovom delu razmatraju se klasični algoritmi šifrovanja koji su zasnovani na tajnom ključu, što znači da pripadaju grupi algoritama za simetrično šifrovanje.
- Posebno se obrađuju klasične substitucione šifre koje slova originalnog teksta zamenjuju drugim slovima, brojevima ili simbolima.
- Analizira se primena transpozicionih algoritama kod kojih se ne radi zamena slova u originalnoj poruci, već se vrši promena redosleda slova u originalnoj poruci.
- Poseban deo posvećen je produkcionim algoritmima koji predstavljaju prelaz od klasičnih ka modernim šiframa.

Nakon proučavanja ovog dela, trebalo bi da možete da:

- objasnite šta su klasični algoritmi šifrovanja;
- objasnite klasične substitucione šifre;
- razumete šta su transpozicioni algoritmi;
- objasnite šta su produkcioni algoritmi.

Simetrično šifrovanje

- Simetrično šifrovanje je šifrovanje tajnim ključem, pri čemu je ključ za šifrovanje identičan ključu za dešifrovanje.
- Simetrični šifarski sistemi karakterišu se relativno velikom brzinom rada i jednostavnom implementacijom.

Cezarova šifra

- Cezarova šifra je jedna od najranije poznatih šifri.
- Ova šifra je dobila ime po Juliju Cezaru, koji je ovu šifru koristio u vojnim operacijama.
- Cezarova šifra je tip šifre **zamenjivanja (substitucije)** u kome se svako slovo otvorenog teksta menja odgovarajućim slovom azbuke, pomerenim za određeni broj mesta.

Monoalfabetske šifre

- Kod monoalfabetske šifre slova originalnog teksta se zamenjuju drugim slovima, brojevima ili simbolima, tako da se umesto samo pomeranja, vrši **permutacija** svih slova alfabeta i primenjuje se na otvoreni tekst.
- Na ovaj način se svako slovo originalnog teksta preslikava u različito slovo kodiranog teksta.

Playfair-ova šifra

- Playfair-ova šifra omogućava da se radi sa **matricama 5x5 ili 6x6**.
- Matrica 5x5 ima 25 slova, jedno slovo se izgubilo od ukupno 26 koliko ih ima u engleskoj abecedi, a po dogovoru je to slovo J.

Vižnerova šifra

- Vižnerova šifra je **najjednostavnija polialfabetska šifra**.
- Kod polialfabetskih šifara se postiže veća sigurnost tako što se koriste višestruki alfabeti šifara.
- Polialfabetske šifre otežavaju kriptoanalizu jer treba pogoditi više alfabeta, a zaravnjuje distribuciju učestalosti.
- Vižnerova šifra predstavlja **višestruku upotrebu Cezarove šifre**.

One-Time Pad

- Kod One-Time Pad metode šifrovanja algoritam ključa je simetričan.
- Pri tome, ključ i poruka imaju **istu veličinu**.
- Za ovu metodu šifrovanja, ključ se pronalazi slučajnim putem. Kod ove metode, svaki ključ upotrebljava se **samo jednom**.

Transpozicioni algoritmi

- Kod transpozicionog algoritma se ne radi zamena slova u originalnoj poruci, već se vrši **promena redosleda slova u originalnoj poruci**.
- Koristeći transpozicioni algoritam, šifrovana poruka ima identičnu frekvenciju korišćenja slova kao i originalna poruka.