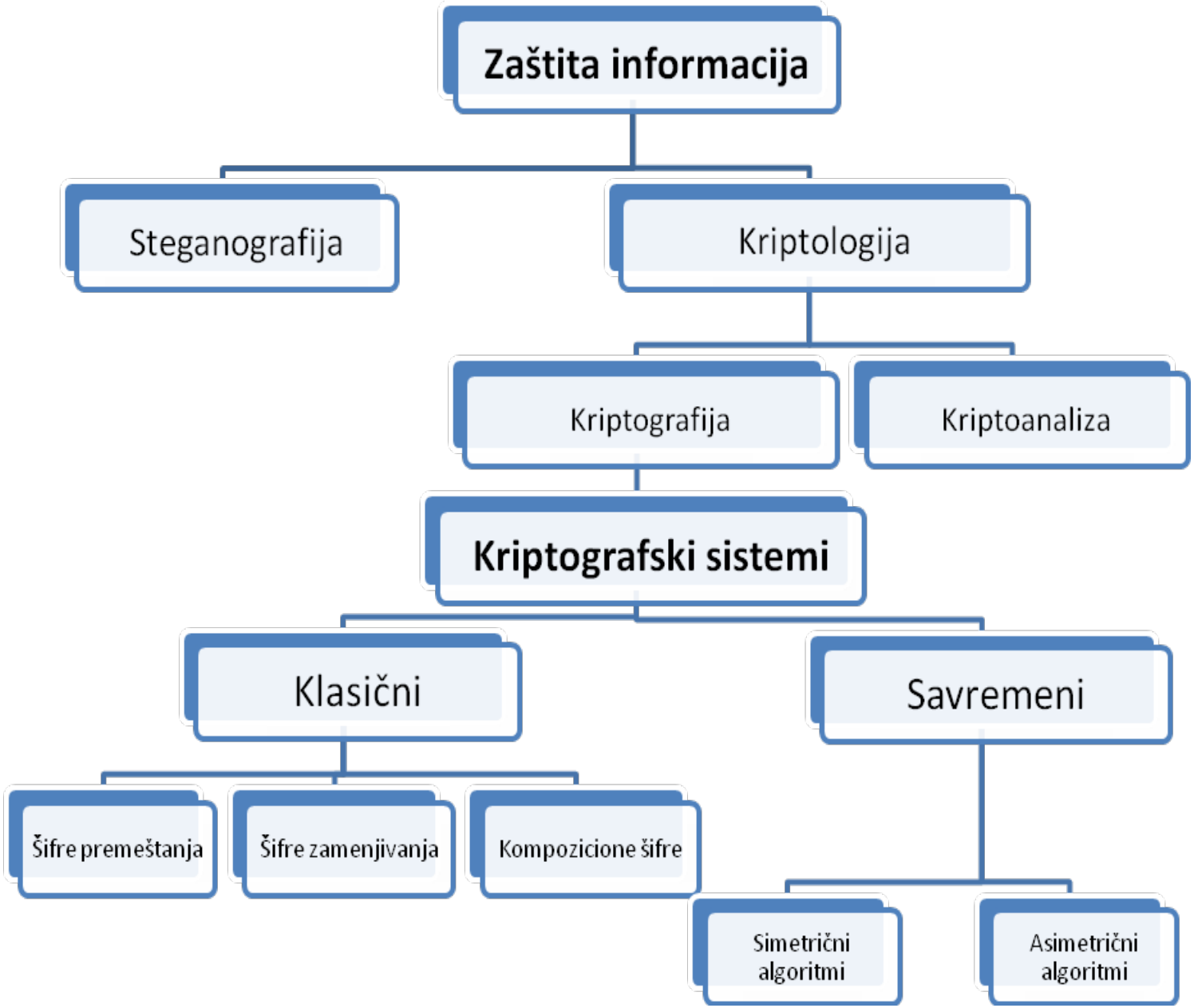
III- Osnovni kriptografski pojmovi

S A D R Ž A J

3.1 – Osnovni pojmovi

- **Kriptografija** potiče od grčkih reči ***kriptos*** i ***grafo*** - skriveno pisanje.
- Ovo je i prikladan opis poslova kojima se dobrim delom bavi naučna disciplina **kriptologija**.
- **Kriptoanaliza** - metode otkrivanja sadržaja zaštićenih informacija
- Javile su se tehnike koje izvorne informacije transformišu tako da su neupućenima praktično bezvredne što omogućava da se prenose osetljive informacije za vlasnika bez bojazni da će biti otkrivene.
- Ako vidimo jedan šifrat videćemo odmah da je reč o primeni nekog od **šifrarskih algoritama** kojim se stvorio nerazumljiv niz znakova
- Tada u pomoć priskače druga tehnika koja pored šifriranja informacija ima i osobinu prikrivanja u odnosu na nosilac – **steganografija**.
- Kriptografija je jako složeno interdisciplinarno područje
- Pre računara, kriptografija je bila blisko povezana sa lingvistikom.
- Danas se zasniva na tehničkim oblastima matematike, teorije brojeva i informacija, računske složenosti, statistike i konačne matematike.
- Ciljevi kriptografije su: **privatnost ili poverljivost**, **integritet podataka**, **autentifikacija i neporečivost**.

3.1-Osnovni pojmovi steganografije



3.2-Osnovni pojmovi steganografije

- **Steganografija** je proces prikrivanja tajne poruke, ali ne i činjenice da dve strane međusobno komuniciraju.
- Istorijski gledano ona se najduže primenjuje kod prikrivanja poruka
- Izvodi se ugradnjom **tajne poruke** u neki prenosni medijum **nosilac**
- Nosilac je skup podataka koji je sastavni deo uobičajne komunikacije i kao takav ne privlači posebnu pažnju na sebe.
- Tajna poruka ne sme da poremeti osnovnu poruku koja se šalje
- Pogodni primeri nosioca su: tekst, slike, audio i video zapisi.
- Nosilac je datoteka u kojoj će se nalaziti skrivena poruka.
- Steganografski medijum (**stego-datoteka**) je celina dobijena "ugrađivanjem" tajne poruke u prenosni medijum.
- Osnovni cilj je da se tajna poruka pošalje a da o tome znaju samo pošiljalac i primalac tj. onaj kome je poruka namenjena
- Steganografske tehnike se mogu podeliti na
  1. **lingvističke** (*linguistic steganography*)
  2. **tehničke** (*technical steganography*)

3.2- Lingvistička steganografija

- Primer **lingvističke steganografije** je **nulta šifra** (***null cipher***), koja shodno prethodnoj klasifikaciji pripada skrivenim šiframa
- Ovde umetnutu tajnu poruku moguće je izdvojiti iz steganografskog medijuma samo ako je poznata tačna metoda iskorišćena za njeno umetanje u prenosni medijum.
- **Nulta šifra** se koristi za skrivanje informacija tako što se definiše neki skup pravila (na primer: „**čitaj svaku četvrtu reč**“).
- Ova metoda omogućava skrivanje tajnih poruka u svakodnevnim porukama bez upotrebe komplikovanih algoritama ili alata.

Primer:

“A**P**PARENTLY N**E**UTRAL'S P**R**OTEST I**S** T**H**OROUGHLY D**I**SCOUNTED A**N**D I**G**NORED. I**S**MAN H**A**RD H**I**T. B**L**OCKADE I**S**SUE A**F**FECTS P**R**ETEXT F**O**R E**M**BARGO O**N** B**Y**PRODUCTS, E**J**ECTING S**U**ETS A**N**D V**E**GETABLE O**I**LS.”

Uzimanjem **drugog slova** iz svake reči dobija se tajna poruka:

“**PERSHING SAILS FROM N.Y. JUNE 1**”

3.2 – Tehnička steganografija

- Dve najčešće korišćene metode za sakrivanje poruke u datotekama su:

1. **Umetanje** (*injection*) - bitovi poruke koju želimo da sakrijemo se umeću u datoteku nosioca – na primer, na kraj datoteke. Na ovaj način dolazi do povećanja veličine datoteke što se lako može otkriti.
2. **LSB supstitucija** - audio-video zapisi i slike sadrže određeni broj bitova koji se mogu zameniti drugim bitovima a da pri tome kvalitet informacija koje nosi datoteka ostane na zadovoljavajućem nivou.

- LSB supstitucija se lako primjenjuje na slike velike rezolucije sa mnogo detalja, ili na audio datoteke sa velikim bitrate-om.
- U steganografiji se najčešće koristi 24-bitni BMP format slike.
- Boja piksela je predstavljen kao kombinacija crvene, zelene i plave RGB boja.
- Svaka od ovih boja predstavljena je jednim bajtom(8 bita).
- Kombinacija po jednom bajtu crvene, zelene i plave daje 3 bajta (24 bita) koji predstavljaju 1 piksel.
- Svaki piksel može uzeti jednu od 2^{24} (oko **16.7×10^6**) nijansi.

3.2 – Tehnička steganografija

- **Primer** LSB supstitucije: *potrebno je sakriti slovo A u sliku*.
- ASCII ekvivalent slova A je 65 (dekadno) – **01000001** binarno.
- Za skrivanje su dovoljna 3 piksela. Neka su ti pikseli:

  pix1: (00100111, 11101001, 11001000)
  pix2: (00100111, 11001000, 11101001)
  pix3: (11001000, 00100111, 11101001).

- Nakon umetanja binarne vrednosti slova A dobijamo sledeće vrednosti:

  pix1: (00100110**, 11101001, 11001000)** – izmenjen 1/24 bita
  pix2: (00100110**, 11001000, 1110100**0**)** – izmenjena 2/24 bita
  pix3: (11001000, 00100111, 11101001) – nema promene

- Samo su 3 od 9 najmanje značajnih bitova promenili vrednost.
- Najveća promena je na drugom pikselu jer se menjaju dve nijanse
- U odnosu na 16,7 miliona mogućih nijansi ova promena predstavlja zanemarlivu promenu koje ljudsko oko ne može da detektuje.
- U proseku se primenom ove metode promeni oko polovine najmanje značajnih bitova slike.

3.2 – Tehnička steganografija

- Postavlja se pitanje **kako se slovo A rekonstruiše** iz ove poruke?
- Jednostavnim iščitavanjem najmanje značajnih bitova svake boje ovog piksela dobijamo: prvi piksel daje **010**, drugi **000** i treći **011** (pri čemu su od trećeg piksela neophodna samo prva dva najmanje značajna bita)

pix1: (00100110, 11101001, 11001000) ⇨ **010**
pix2: (00100110, 11001000, 11101000) ⇨ **000**
pix3: (11001000, 00100111, 11101001) ⇨ **011**

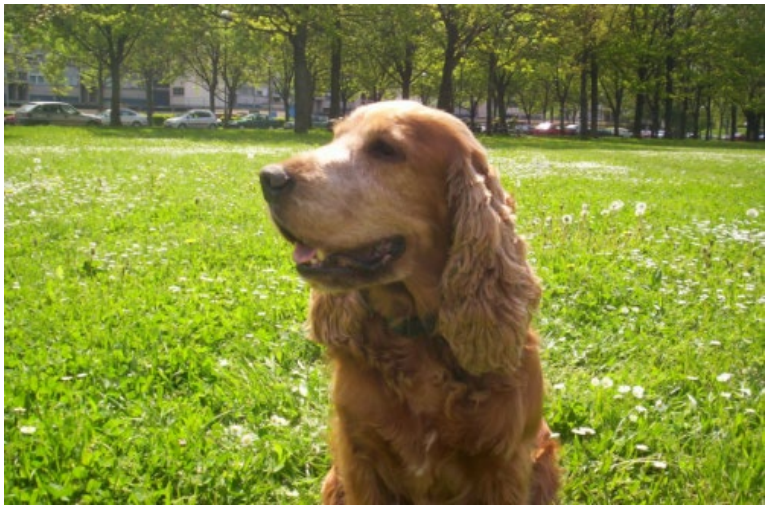
- Kada primalac poruke ove bitove spoji dobije **01000001**, tj slovo A.

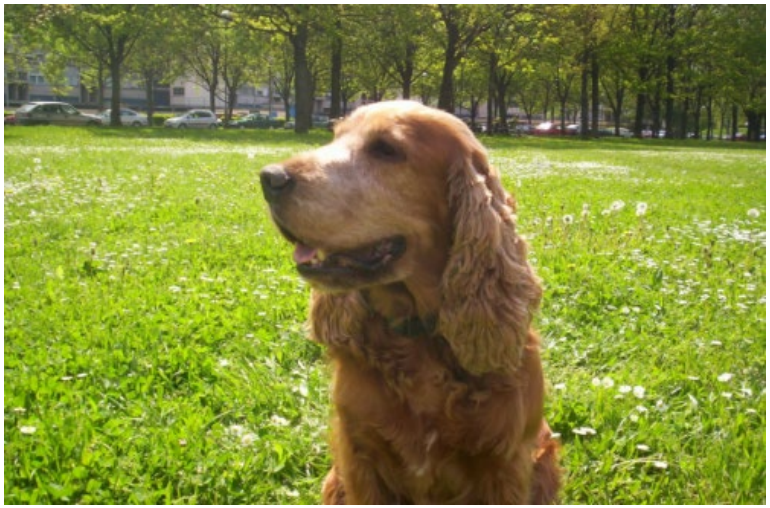
1. Ukoliko se ugrađuje poruka, najpre se bira pogodan nosilac.
2. Nakon izbora pogodnog nosioca (slike) bira se podskup najmanje značajnih bitova koji će biti iskorišćeni za supstituciju (broj bitova u odabranom skupu odgovara broju bitova poruke).
3. Tada se nekim redosledom svaki odabrani bit zamenjuje bitom poruke.
4. Najjednostavnije je redom smeštati bitove poruke u LSB bitove piksela
5. Da bi rekonstruirao poruku, primalac mora da zna koji je podskup LSB bitova za njega interesantan, tj. koji bitovi nose skrivenu poruku.
6. Tehnikom obrnutom od umetanja "**izvlači**" najmanje značajne bitove, slaže ih redom i dobija poruku.

3.2 – Tehnička steganografija

- Slike koje imaju velike površine istih boja nisu dobri nosioci jer se na njima promene izazvane umetanjem poruke lakše uočavaju
- Koja količina tajne informacije se može sakriti a da se ne primeti?
- Ako menjamo **3 bita** u svakom pikselu onda slika od 1024 x 768 piksela (2.25Mb). može sakriti 1024 x 768 x 3 = 2359296 b (**288Kb**).
- Ukoliko bi tajnu poruku ovom metodom skrivali u 2, 3 ili 4 najmanje značajna bita, ljudsko oko bi i dalje teško moglo da primeti razliku

Primer: *sledeće dve slike prikazuju original i stego-sliku (poruka je u sliku umetnuta tako da su 3 bita crvenog, 3 bita zelenog i 2 bita plavog kanala zamenjeni bitovima poruke).*



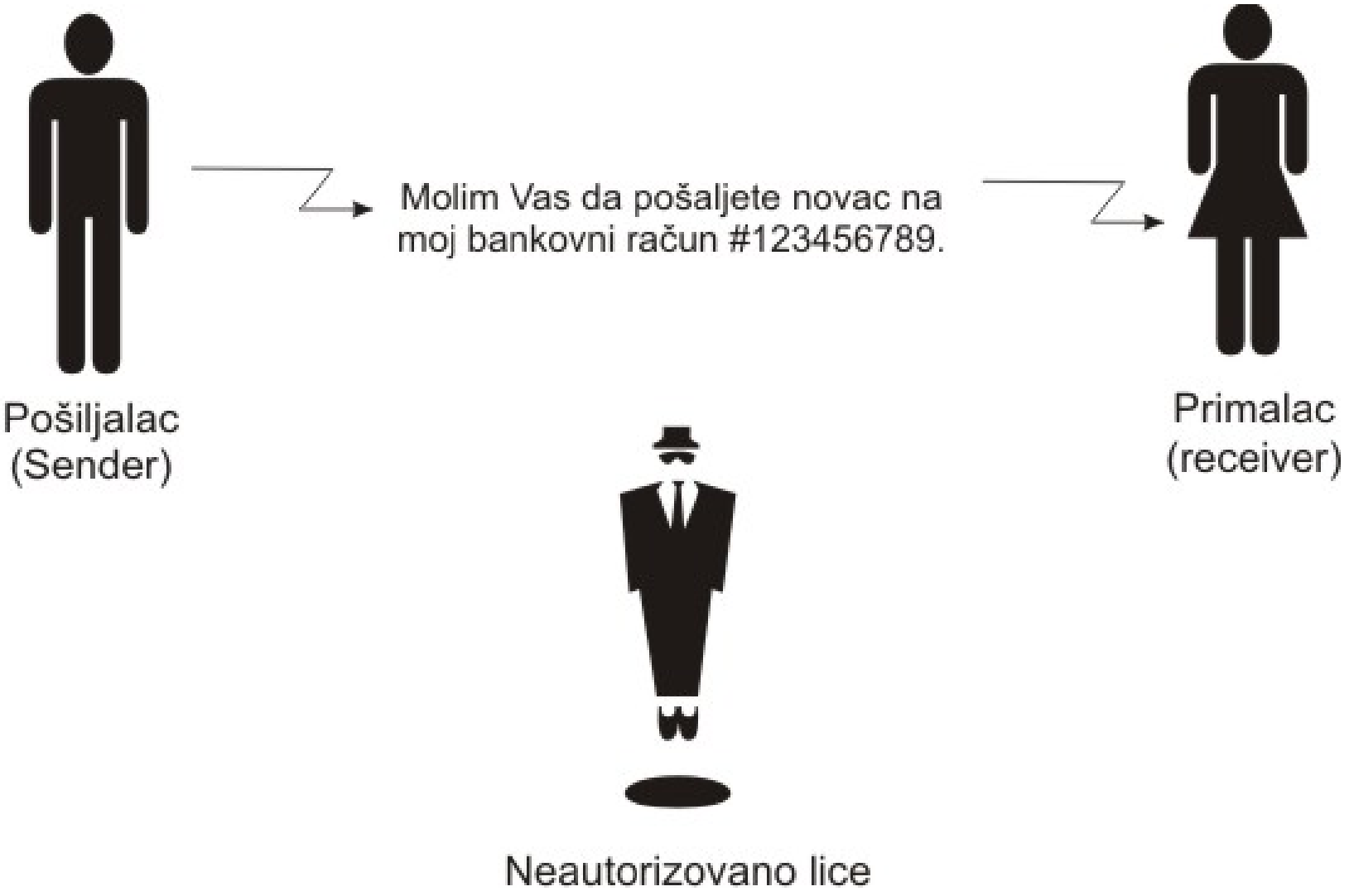


3.2 – Primena steganografije

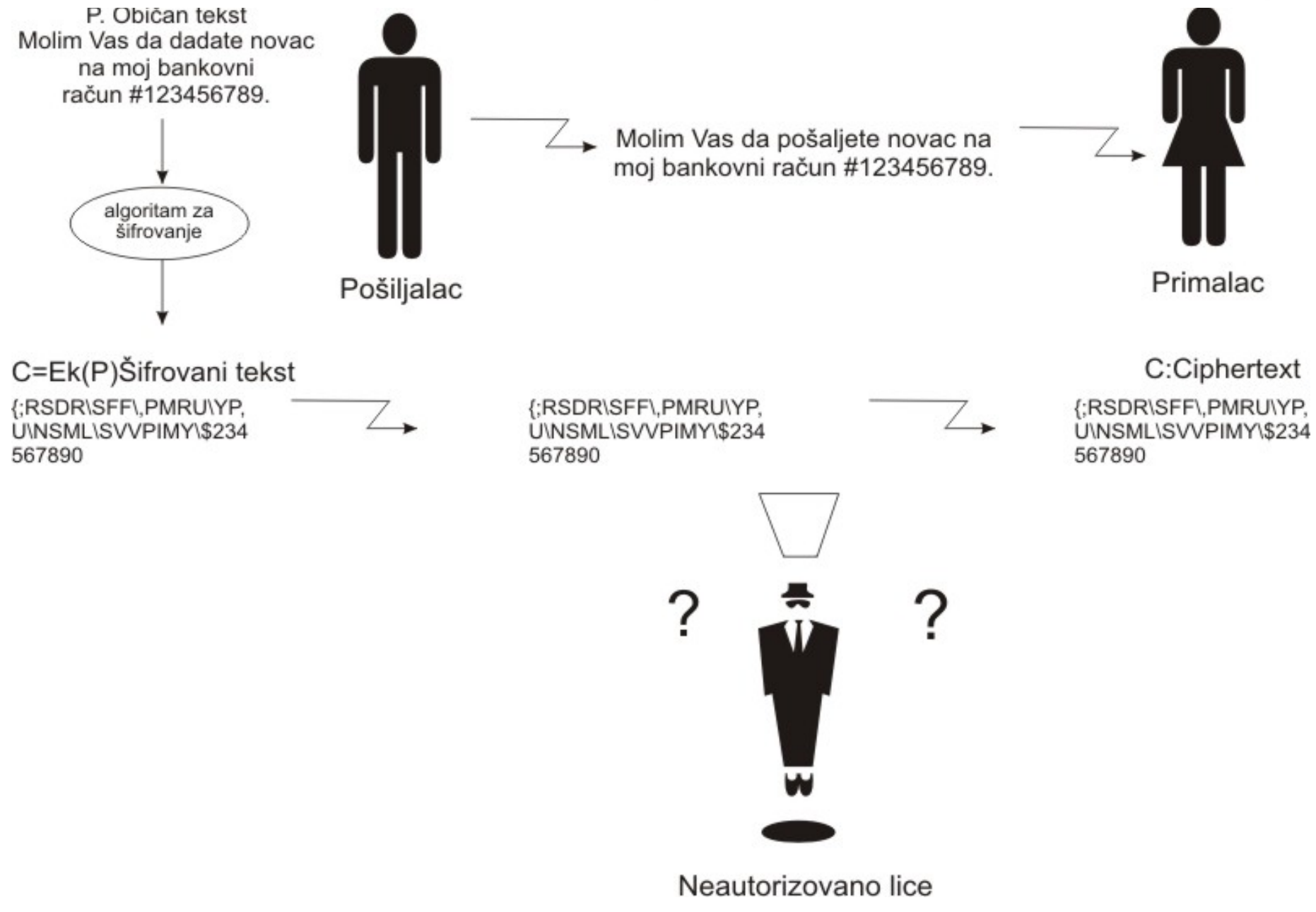
- Kao i mnoge druge sigurnosne metode i alati, steganografija se može koristiti u različitim aktivnostima, kako legalnim tako i nelegalnim.
- Legalna primena svodi se na upotrebu digitalnog vodenog pečata (***watermark***) u svrhu zaštite autorskih prava i vlasništva
- Digitalni vodeni pečat je umetanje dodatnih informacija u izvornu datoteku tako da nosilac ostaje sadržinski i po kvalitetu gotovo nepromenjen za oko ili sluh tako da pečat ostaje neprimećen.

1. Zaštitu autorskih prava - onemogućavanje krađe vlasništva nad datotekama (bitno je da se pečat ne može neautorizirano ukloniti i da je otporan na razne modifikacije signala nosioca)
2. Zaštitu od kopiranja - kontrolisanje uređaja za kopiranje zaštićenih multimedijalnih sadržaja.
3. Proveru autentičnosti - proveravanje autentičnosti multimedijalnih sadržaja (pečat se dodaje celom signalu nosioca tako da se kasnije može otkriti lokacija na kojoj isti nedostaje)
4. Skladištenje dodatnih informacija - dodavanje veće količine podataka koji mogu služiti kao prateće informacije o multimedijalnoj datoteci.

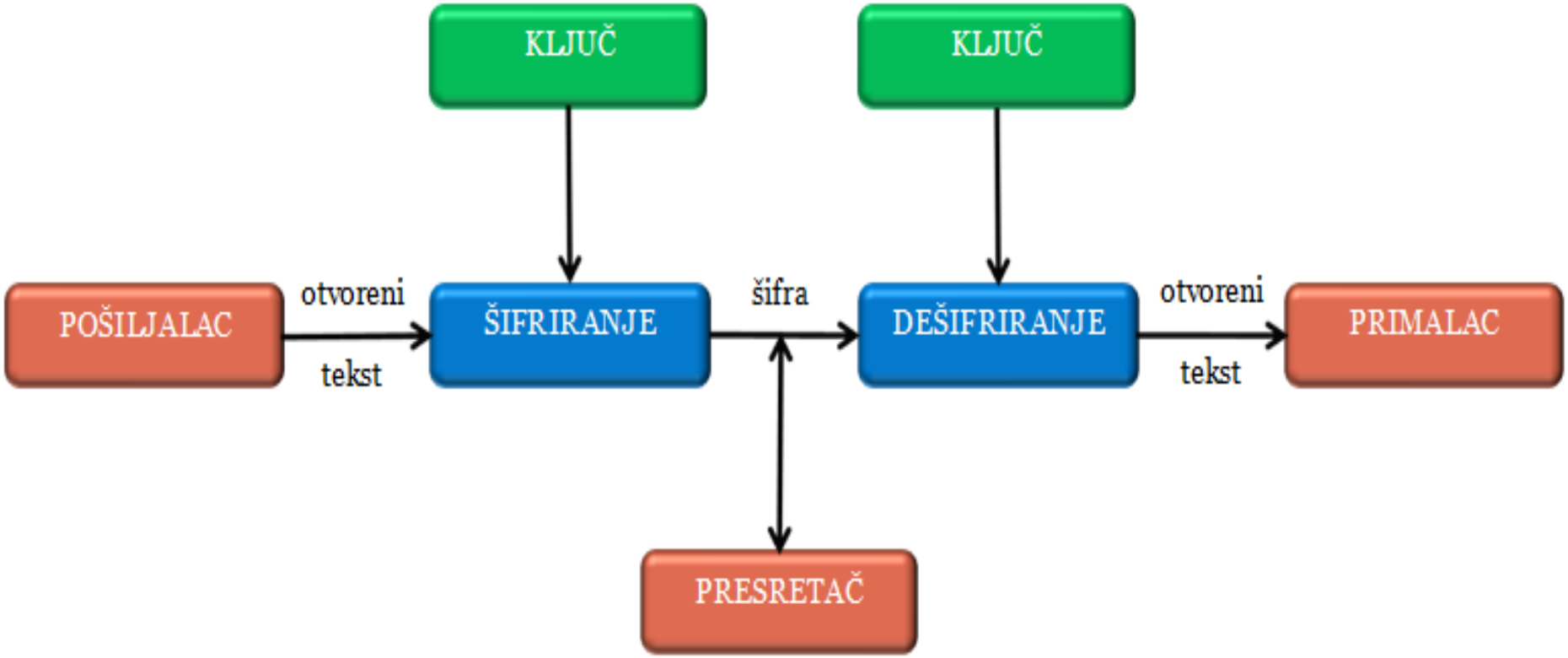
3.3 - Osnovni pojmovi kriptografije



3.3 - Osnovni pojmovi kriptografije

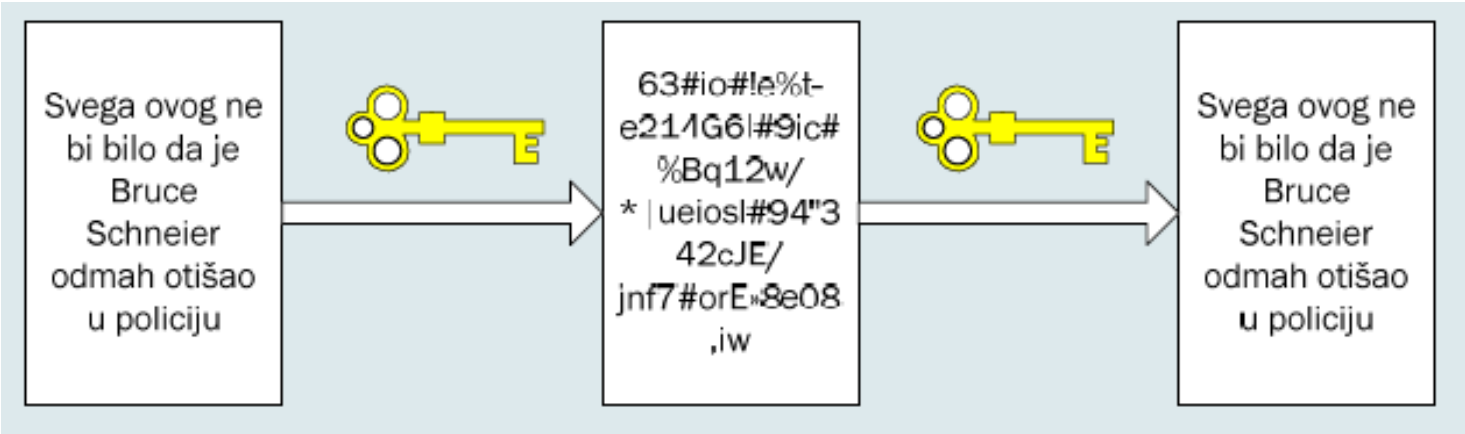


3.3 - Osnovni pojmovi kriptografije



3.3 – Osnovni pojmovi kriptografije

- **Šifrovanje** (*encryption*) obuhvata matematičke postupke modifikacije podataka tako da šifrovane podatke mogu pročitati samo korisnici sa odgovarajućim ključem.
- U procesu šifrovanja transformiše se otvoreni tekst (***plain text***), odnosno orginalna poruka ili datoteka pomoću ključa u zaštićen, šifrovan tekst, koji se zove šifrat (***ciphertext***).
- **Dešifrovanje** (*decryption*) je obrnuti proces, šifrovani podaci se pomoću ključa transformišu u orginalnu poruku ili datoteku.
- Šifrovani podaci su zaštićeni od neovlašćenog pristupa pa se mogu preneti preko nesigurnog kanala ili čuvati na disku koji nije zaštićen od neovlašćenog pristupa.

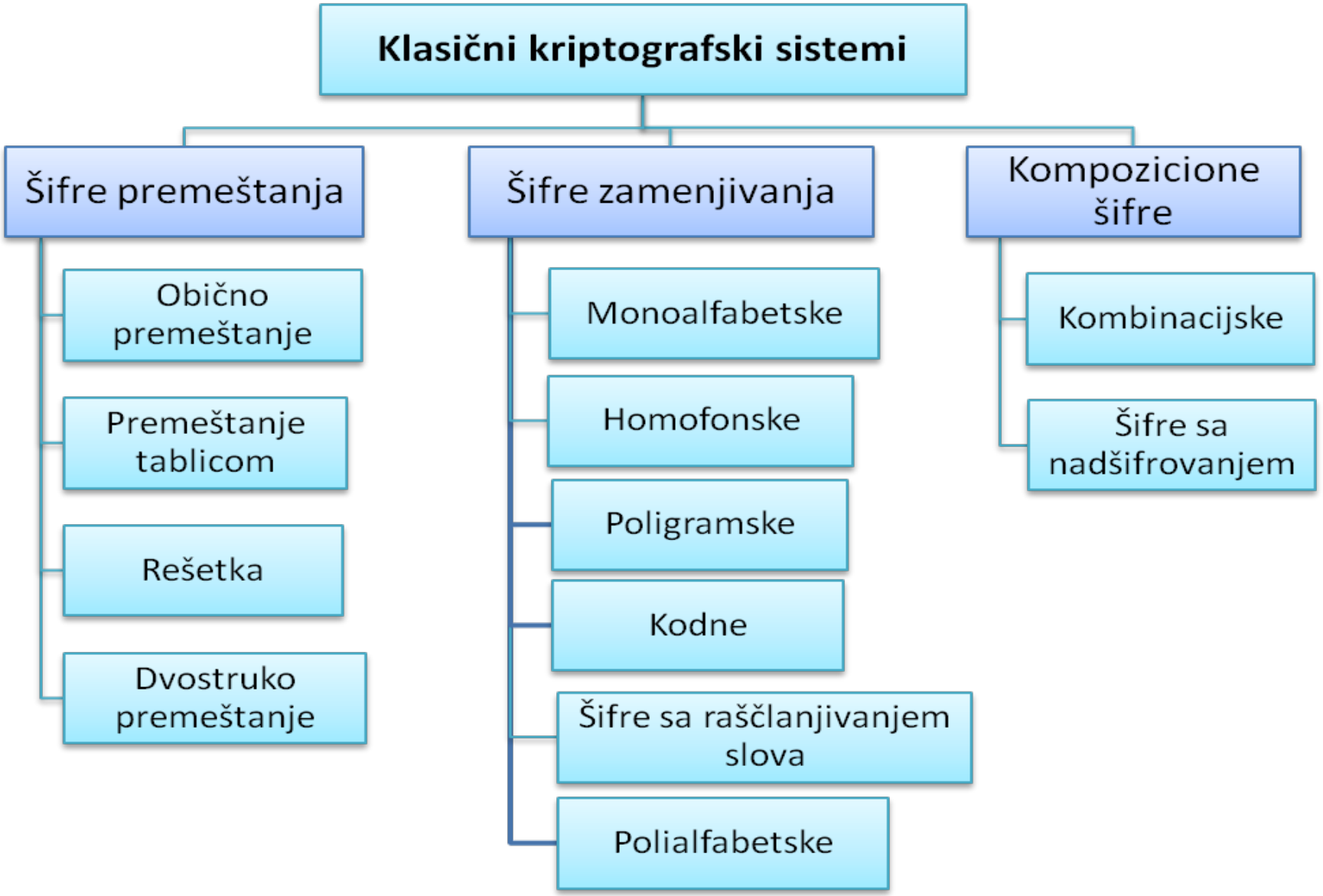


3.3 – Osnovni pojmovi kriptografije

- Kriptografski sistem je skup srodnih šifrarskih algoritama.
- Osnovna podela na **klasične** i **savremene** je zasnovana na vremenskoj distanci kako su nastajali i na kompleksnosti primenjenih tehnika.

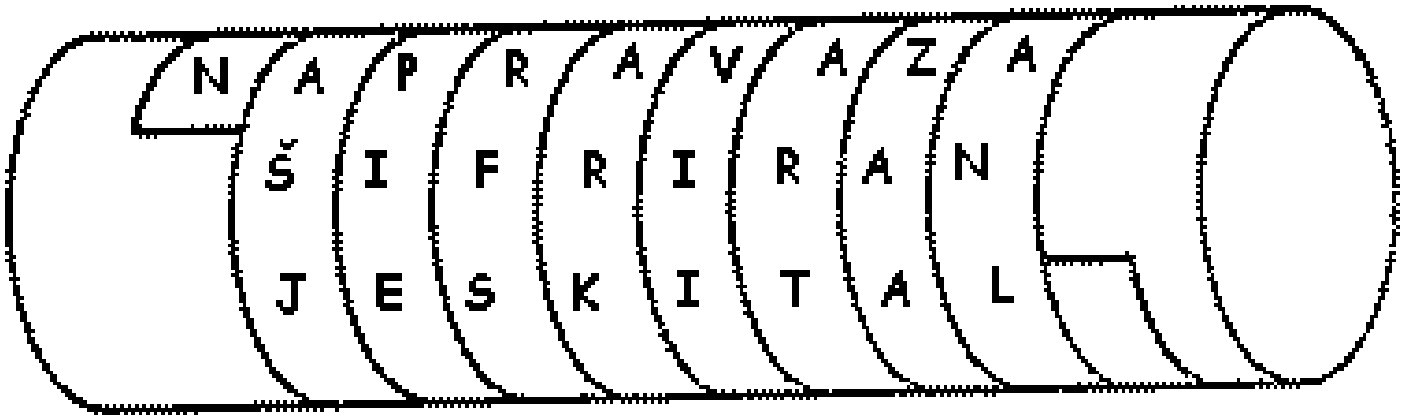
1. ***Klasični kriptografski sistemi*** koriste transformacije koje vrše:
   - ✓ **šifre premeštanja** - permutuju slova otvorenog teksta
   - ✓ **šifre zamenjivanja** - menjaju delove otvorenog teksta određenim šifarskim zamenama
   - ✓ **kompozicione šifre** - vrše dvostruku transformaciju kombinujući šifre ova dva sistema.
2. ***Savremeni kriptografski sistemi*** - realizuju se pomoću računara.
   - ✓ Koriste različite transformacije klasičnih šifara, specijalne matematičke i fiksne slučajne funkcije ili višestruka šifrovanja različitim ključevima
   - ✓ Razlika između **simetričnih** i **asimetričnih** algoritama (pored samog oblika i mogućnosti algoritama) je u tome što simetrični algoritmi koriste isti ključ za šifrovanje i dešifrovanje a asimetrični različite, javni i tajni, koji svoju snagu baziraju na tome da se bez dodatne informacije ne mogu dobiti jedan iz drugog.

3.3 – Osnovni pojmovi kriptografije



3.3 – Osnovni pojmovi kriptografije

- Neki elementi kriptografije bili su prisutni već kod starih Grka.
- Spartanci su u 5. veku pre Hrista upotrebljavali napravu za šifriranje zvanu ***skital***.
- To je bio drveni štap oko koga se namotavala traka od pergamenta, pa se na nju horizontalno pisala poruka.
- Nakon upisivanja poruke, traka bi se odmotala, a na njoj bi ostali izmešani znakovi koje je mogao pročitati samo onaj ko je imao štap iste debljine.



3.3 – Osnovni pojmovi kriptografije

- Da bi šifra mogla da se koristi za zaštitu informacija određenog nivoa tajnosti, neophodno je da zadovoljava odgovarajuće zahteve kvaliteta:

1. ***praktičnost*** - brzina i lakoća rada, element koji zavisi od složenosti postupka šifrovanja/dešifrovanja i obučenosti šifrera
2. ***ekonomičnost*** - odnos dužine otvorenog teksta i šifrata. Šifra se smatra ekonomičnom ako dužina šifrata nije veća od dužine otvorenog teksta. Neekonomična šifra smanjuje brzinu rada, opterećuje prenosne puteve i zahteva veće materijalne izdatke.
3. ***osetljivost na greške*** - element koji procenjuje da li je zbog eventualne greške u šifrovanju nemoguće dešifrovati poruku (greška sa posledicom) ili ne (greška bez posledice). Greška može nastati usled nedovoljne obučenosti šifrera ili složenosti postupka šifrovanja/dešifrovanja.
4. ***kriptološka vrednost*** - "sigurnost" šifre, njena otpornost na dekriptovanje. Ovom ocenom se bave određene državne institucije (kod nas Institut za primenjenu matematiku i elektroniku).

3.3 – Osnovni pojmovi kriptografije

- Kvalitet šifre zavisi od svih prethodno navedenih elemenata iako je **kripto vrednost** najvažnija od njih.
- Kako pojedinačni zahtevi ovih elemenata mogu biti u međusobnoj suprotnosti, pri izboru šifre mora se voditi računa da oni budu usaglašeni sa stepenom tajnosti poruke, vremenskim ograničenjem, zahtevima i dr.
- Kod savremenih šifarskih sistema koji se realizuju složenim program. rešenjima na moćnim računarima **praktičnost**, **ekonomičnost** i **osetljivost** na greške postaju manje bitni elementi ocene
- Kvalitet šifre se svodi na **jačinu njene kriptološke vrednosti**.
- Određivanje kriptoloških zahteva je najvažniji zadatak kriptologa i oni zavise od vrste i jačine algoritma i predstavljaju državnu tajnu.
- Postoje **dve vrste** "sigurnih" šifarskih sistema:

1. **Apsolutno**(teorijski) siguran šifarski sistem-otporan na svaki pokušaj napada čak i pod pretpostavkom neograničenih mogućnosti napadača
2. **praktično** siguran šifarski sistem - sistem koji se teorijski može dekriptovati ali ne i u okviru raspoloživih mogućnosti napadača (ograničenje vremena, sredstava, raspoloživim resursima i ljudstva).

3.4 – Principi kriptovanja

- **Kvalitet šifre** u opštem slučaju zavisi od kvaliteta algoritma i ključa a nekada i isključivo od ključa.
- Ključ je sastavni deo šifre i on jednoznačno određuje ("bira") jednu transformaciju iz određenog skupa srodnih transformacija
- Danas, većina konvencionalnih kriptosistema svoju sigurnost zasniva upravo na ključu - njegovom **kvalitetu**, **tajnosti** i **načinu upotrebe**
- Zahteva se masovno i brzo generisanje kvalitetnih ključeva, njihova brza i bezbedna dostava velikom broju udaljenih korisnika.
- Teorija dokazuje da postoje apsolutno sigurni šifarski sistemi a njihova realizacija se zasniva na upotrebi slučajnih nizova kao ključeva.
- Praksa pokazuje da ima puno problema u realizaciji apsolutne tajnosti
- Zbog toga se apsolutno tajni šifarski sistemi koriste za šifrovanje samo najpoverljivijih informacija i retko se zbog svoje složenosti korste
- U praksi se koriste tajni šifarski sistemi koji svoju sigurnost zasnivaju na kvalitetnim **pseudoslučajnim ključevima** koji su ograničeni **vremenom** i **mogućnostima napadača**.

3.4 – Principi kriptovanja

- Da bi jedan niz bio deklarisan kao ključ potrebno je da ispunjava neke tehničke zahteve.
- Generisanje takvih nizova nije jednostavno pa se u praksi koriste generatori koji rade na principu transformisanja fizičkih procesa u binarne znakove (šum elektron.cevi, isijavanje radioaktivnih čestica)
- Ovako dobijeni nizovi podležu nizu statističkih testova koji se vrše na različitim strukturama niza (pojedinačnim znakovima, bigramima, poligramima i serijama) na čitavoj dužini i tek nakon toga, ukoliko svi testovi budu negativni, jedan niz se proglašava **ključem**.
- Da li će to biti **apsolutno slučajan** ili **pseudoslučajan** niz zavisi od jednog parametra – jednake verovatnoće da se bilo koji član niza nađe na bilo kom mestu na celoj posmatranoj dužini.
- ***Pseudoslučajni nizovi*** su danas veoma zastupljeni jer pružaju dovoljno dobro rešenje za većinu primena.
- Generišu se po nekom unapred utvrđenom algoritmu na osnovu zadatog početnog vektora stanja a po svojoj strukturi su približni slučajnim nizovima.

3.4 – Principi kriptovanja

- Svoju popularnost pored pristupačnosti u generisanju mogu zahvaliti i tome što je za generisanje identičnog niza potrebno poznavanje algoritma i početnog uslova
- Slaba tačka ovih nizova je algoritam generisanja i inicijalni vektor.
- Algoritam mora biti takav da otklanja i ublažava nedostatke, a to su:
  - ✓ periodičnost za bilo koju dužinu inicijalnog vektora
  - ✓ broj različitih nizova koje je moguće generisati je u korelaciji sa inicijalnim vektorom
  - ✓ ni jedan ovako generisan niz po default-u ne može da zadovoljava tražene uslove već se mora dodatno ispitati
  - ✓ maksimizirati periodu generisanih nizova
  - ✓ onemogućiti rekonstrukciju na osnovu poznavanja dela niza, itd.
- Najjednostavniji generatori pseudoslučajnih nizova su **pomerački registri** od kojih jedan generiše niz a drugi npr. služi za taktovanje s tim da se između njih može ubaciti i jedan multiplekser koji doprinosi **nelinearnosti rezultata**.

3.5 – Podela klasične kriptografije

- Klasična kriptografija odnosi se na algoritme koji šifruju tekst poruke
- Različiti kripografski sistemi su ili zamenjivali slova teksta jedno drugima ili su ih premeštali tako da se mogu podeliti na:
  1. **Sistem premeštanja** (*supstitution cipher*)
  2. **Sistem zamenjivanja** (*transposition cipher*)
  3. **Kombinacijske šifre** (premeštanje + zamenjivanje)
- Pojavom računara, algoritmi više ne rade sa slovima, već sa bitovima
- Činjenica da su neki klasični algoritmi vekovima bivali neporaženi unatoč brojnim napadima pomaže nam isto koliko i činjenica da su na kraju podlegli napadima i da je otkriven način da se razbiju
- Prva činjenica daje nam neke algoritme čije pune mogućnosti dolaze do izražaja tek kad se implementiraju na računarima, dok nas druga činjenica upozorava na već učinjene propuste koje nikako ne treba ponovo učiniti.
- Mnogi algoritmi još uvek kombinuju elemente zamene i premeštanja.
- Svi šifarski sistemi mogu da koriste neki ALFABET: sređeni ili nesređeni koji će koristiti kod šifriranja (ABCD.. , DOJA..)

3.5 – Klasični algoritmi šifrovanja

- **Šifarski sistemi premeštanja - transpozicije** obuhvataju:
  1. obično premeštanje
  2. premeštanje ključem
  3. premeštanje rešetkama
  4. dvostruko premeštanje

- **Šifarski sistemi zamenjivanja** se deli na:

  I. Šifre proste zamene (MONOALFABETSKE) se dele na:
  a) alfabetske šifre
  b) bigramske, Trigramske i poligamske šifre
  c) kodne tablice
  d) Kodovi
  e) šifre raščlanjivanjem slova

  II. Šifre složene zamene (POLIALFABETSKE)
  a) šifre sa sređenim alfabetom
  b) šifre sa nesređenim alfabetom

3.5.1 – Šifre premeštanjem

- Šifre premeštanja su šifre kod kojih šifrat nastaje permutovanjem slova otvorenog teksta - slova menjaju mesto a zadržavaju značenje.
- Permutovanje se vrši na osnovu određenog dogovora koji se u opštem slučaju može svesti na određenu permutaciju.
- Svaka šifra premeštanja može se predstaviti kao preslikavanje pozicija slova otvorenog teksta u pozicije koje ta slova dobijaju u šifratu.
- Time je određena odgovarajuća permutacija ***p*** prvih ***n*** prirodnih brojeva (n je dužina poruke) koja predstavlja ključ premeštanja.

1.1 Obično premeštanje - transpozicija

- Ovde se slova premeštaju u vidnu nekog **anagrama**.
- Kada se koristi mali broj slova, ova je metoda je nesigurna za slanje

Primer: *Šifriraj otvoreni tekst*: **OVA**

  - ✓ Broj mogućih transpozicija je 6 (3 faktorijela)
  - ✓ Moguće transpozicije: **OVA, VAO, AVO, OAV, AOV, VOA**.

- Kod poruke sa velikim brojem znakova **N** ova metoda je sigurna za šifriranje, jer je teška za dešifriranje (**N!** → 25!=**1524** kombinacija)

3.5.1 – Šifre premeštanjem

1.2 Naizmenična transpozicija

- Kod ove metode slova poruke se naizmenično pišu u gornji i donji red

  Primer: *Šifriraj otvoreni tekst*: **DISKRETNA MATEMATIKA**

  Transpozicija: D S R T A A E A I A

  I K E N M T M T K

- Skrivena poruka ili šifrat je : **DSRTNAAEAIA IKENMTMTK**
- Šifriranjem otvorenog teksta u više redova gde broj redova predstavlja ključ K može se postići još bolja zaštita teksta

1.3 Transpozicija s obilaskom

- Kod ove metode slova poruke se pišu u polje zadatih dimenzija, a šifrat dobivamo korišćenjem ključa koji opisuje obilazak polja.

  Primer: *Šifrirati otvoreni tekst*: **DISKRETNA MATEMATIKA**

  ✓ Transpozicija:

D K T M E T A	→→
I R N A M I	↑ → ↓
S E A T A K	←←

  ✓ Ključ: u smeru kazaljke na satu sa početkom od levog desnog ugla, spiralno prema unutra Šifrat: **DKTMETA KATAES IRNAMI**

3.3.1 – Šira premeštanja

1.4 Stepenasta transpozicija

- Slova otvorenog teksta zapisujemo u redove manjih dužina. Dužinu reda određuje ključna reč a zadati ključ redosled čitanja kolona.
  Primer: *Šifrirati otvoreni tekst*: **THE ALCHEMIST BY PCOELHO**
  Ključna reč: **DREAM** Ključ : 2 5 3 1 4 (redosled slova po abecedi)
  - ✓ Transpozicija: T H E A L
    A L C H E
    M I S T B
    Y P C O E
    L H O

    Šifrat: AHTO TAMYL ECSCO LEBE HLIPH

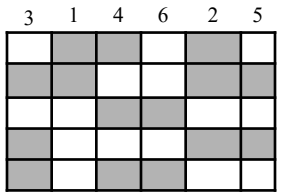
2. Kompletna i nekompletna tablica su šifre premeštanja kod kojih se otvoreni tekst upisuje u tablicu određenih dimenzija redom po vrstama a šifrat čita po kolonama redom koji određuje ključ premeštanja.

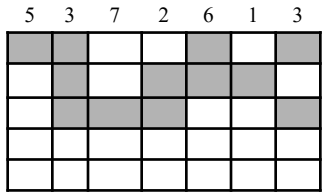
- Ključ premeštanja je permutacija brojeva kolona u tablici
- Razlika između kompletne i nekompletne tablice je u tome što su kod kompletne ispunjena sva polja a kod nekompletne nekoliko poslednjih u poslednjem redu ostaje nepopunjeno - poništava se šrafiranjem.

- Dešifrovanje se vrši obrnuto:šifrat se upisuje u kolone tablice po ključu

3.3.1 – Šifre premeštanja

3. Figura (**rešetka**) je tablica slična kompletnoj ili nekompletnoj tablici s tim što je u njoj, slično ukrštenim rečima, poništen izvestan broj polja: po čitavoj dubini (*unutrašnja figura*) ili u prvih nekoliko redova (*spoljašnja figura*)





- Dobro konstruisana figura treba da ima 40-60% na slučajan način poništenih polja (pomoću slučajnog binarnog ili dekadnog niza), pri čemu se odbacuju delovi koji poništavaju uzastopno više od 5 polja (po vrstama ili kolonama).

4. Dvostruko premeštanje je kombinacija dve, kompletne ili nekompletne tablice, gde se otvoreni tekst prvo šifruje jednom od tablica i tako nastaje polušifrat koji se zatim šifruje drugom tablicom i daje šifrat

- Svaka šifra premeštanja je teorijski rešiva jer za konačan broj slova postoji konačan broj permutacija.
- Kompletna i nekompletna tablica su praktično rešive ali se to ne može reći i za dobro konstruisanu figuru primenjenu na duži otvoreni tekst, ili za dvostruko premeštanje, jer je za rešavanje potrebno mnogo vremena.

3.5.2 – Šifre zamene

- To su šifre kod kojih se nezavisni delovi otvorenog teksta zamenjuju šifarskim zamenama sastavljenim od jednog ili više znakova.
- Šifre zamenjivanja se dele na šifre proste i šifre složene zamene.
- **Šifre proste zamene** svakom elementu dodeljuju jednu ili više šifarskih zamena pri čemu jedna šifarska zamena može biti zamena samo za jedan element otvorenog teksta.

1. **Monoalfabetska zamena** (*Cezarova* i *afina* šifra). Svaki znak poruke preslikava se u tačno jedan znak šifrata.
2. **Polialfabetska zamena** (*Vigenere-ova* i *Playfair-ova*). Preslikavanje 1→n, svaki znak poruke preslikava se jedan od n dozvoljenih znakova
3. **Poligramska zamena** (*Playfairova* i *Hillova*).Bijektivno preslikavanje pri čemu se kao osnovna jedinica koja se supstituiše uzima poligram
4. **Homofonske** svako slovo teksta, u zavisnosti od verovatnoće u jeziku, dobija jednu ili više šifarskih zamena i njima se zamenjuje u šifratu.
5. **Kodne šifre**
6. **Šifre sa raščlanjavanjem slova**.

3.5.2 – Cezarova šifra

- Predstavlja šifru u kojoj su slova otvorenog teksta zamenjena slovima koja su se nalazila **tri mesta** dalje od njih u alfabetu (A ➡ **D**, B ➡ **E**, itd.)
- Ako bi upotrebili današnji engleski alfabet od 26 slova, onda bi poznata Cezarova izreka VENI VIDI VICI **YHQL YLGL YLFL**.
- Cezarovu šifru možemo pregledno zapisati ➡ na sledeći način:

otvoreni tekst: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

šifrat: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Supstituciona šifra ne mora izgledati kao gornji primer, odnosno, ne mora se raditi o čistom pomeranju slova alfabeta za tri-četiri mesta
- Ukoliko pošiljalac koristi neki opštiji algoritam supstitucije, gde šifrovan alfabet može da bude bilo koja kombinacija slova početne azbuke, onda se stvaraju milioni mogućih ključeva, a samo primalac zna tačnu kombinaciju, odnosno pravi ključ.
- Međutim supstituciona šifra se i pored toga može vrlo lako dešifrovati koristeći metodu koja se naziva **Analiza učestanosti**.
- Brojimo slova šifrovanog teksta, i pravimo tabelu najčešće korišćenih
- Za $0 \leq K \leq 25$ definišemo $\boldsymbol{e_K(x) = x + K \bmod 26}$, $\boldsymbol{d_K(y) = y - K \bmod 26}$.

3.5.2 – Afina šifra

- Pošto su sve dotadašnje supstitucijske šifre bile 26! (permutacija) od 26 elemenata, potrebno je bilo razviti složeniju funkciju zaštite.
- Afina šifra je poseban slučaj supstitucijske šifre sa dva parametra ***a*** i ***b***.
  - ✓ neka su $x,y,a,b \in \mathbb{Z}26$
  - ✓ Enkripcija $\boldsymbol{e_k}$ $\boldsymbol{(x) = y \equiv a \cdot x + b \bmod 26}$
  - ✓ Dekripcija $\boldsymbol{d_k}$ $\boldsymbol{(y) = y \equiv a \cdot x + b \bmod 26}$

$$a \cdot x + b \equiv y \bmod 26$$
$$a \cdot x \equiv (y - b) \bmod 26$$
$$x \equiv (y - b) \bmod 26/a$$
$$x \equiv a^{-1} \cdot (y - b) \bmod 26$$

- Najlakše je da odredimo broj ***b*** elemenata iz funkcije enkripcije, a to su: 0,1,2,3...25 $\#b = 26$
- Pogledom na Afinu funkciju enkripcije zaključujemo da nema uslova i ograničenja za elemente ***a*** tako da ih možemo brojati kao **b** elemente
- Razlika je što ***a*** nema istu funkciju u dekripciji odnosno koristimo inverzni ***a*** parametar što rezultuje ograničenjem broja elemenata **a**.
- Uslov koji važi za ***a*** elemente je korišćenje **NZD (*a*,26) = 1**.

3.5.2 – Afina šifra

- NZD označava najveći zajednički delilac argumenata u zagradi.
- Kako je 2·13 = 26, a NZD (a,26) = 1, za elemente parametra $a \in \mathbb{Z}$ važe sledeći brojevi: **1,3,5,7,9,11,15,17,19,21,23,25**.
- Uzmemo li za parametar **b** 26 brojeva iz skupa $\mathbb{Z}26$ a za parametar mogućih 12 brojeva, množenjem tih dva elemenata dobijemo Afinu šifru sa **312 različitih ključeva → 26 ·12 = 312, #*k* = 312**
- Možemo da izvedemo zaključak da 312 različitih ključeva mogu otežati nekome ko pokuša da vrši dekripciju brute-force napadom.
- Afina šifra se smatra poboljšanom verzijom Cezarove, ali u principu ima jednake slabosti jer je lako dešifrirati metodom učestalosti slova.

  Primer: *Šifrirajte opvoreni tekst* **RADAR** *ako je dat ključ* K=(7,3)

  Rešenje:

  Kako je redosled pojavljivanja slova u abecedi: R→17, A→0 i D→3

  imamo da je: 17 * 7 + 3 = 18 (mod26) → S

  0 * 7 + 3 = 3 (mod26) → D

  3 * 7 + 3 = 24 (mod26) → Y

  Pa je šifrat: **SDYDS**

3.5.2 – Vigener-ova šifra

- **Vigener** šifra predstavlja revolucionarno otkriće u svetu kriptografije.
- Snaga Vižnerove šifre ogleda se u tome što ona umesto jednog koristi onoliko šifrovanih alfabeta (abeceda, azbuka) koliko slova ima jezik na kojem se šifruje:26 šifrovanih alfabeta u engleskom a u srpskom 30.
- Prvi korak u šifrovanju je crtanje tzv. Vižnerovog kvadrata koji se sastoji od početnog alfabeta i 26 šifrovanih alfabeta, od kojih je svaki pomeren za jedno slovo u odnosu na prethodni.
- Korišćenje Vižnerove šifre podrazumeva da se za šifrovanje različitih slova iz poruke koriste različiti redovi Vižnerovog kvadrata.
- Drugim rečima, pošiljalac bi mogao da šifruje prvo slovo prema redu 5, drugo prema redu 12, treće prema redu 23 itd.
- Jačina ove šifre leži u tome što je nemoguće primeniti analizu učestanosti jer su sva slova relativno podjednako zastupljena.
- Vižnerova šifra ima ogroman broj ključeva jer se pošiljalac i promalac mogu dogovoriti da to bude bilo koja reč ili kombinacija slova
- Ovu šifru možemo svrstati u klasu polialfabetskih šifara
- Zbog svoje snage i složenosti često se naziva **Neprobojnom šifrom**!

3.5.2 – Vigener-ov kvadrat

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3.5.2 – Vigener-ova šifra

- Prva primena ovog načina šifriranja bio je **Albertijev sistem**
- Albertijev sistem se zasnovao na tome da poruku možemo kriptovati naizmenično iz više datih abeceda.
- Prvo slovo kriptujemo iz prve šifrirane abecede, sledeće iz druge i td.

Primer: *Šifrirajte otvoreni tekst* MATEMATIKA *prema datoj tablici*

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
S T Q U V W X Z Y A B C D E F G H I J K L M N O P R

Rešenje:

Šifrat poruke MATEMATIKA glasi **WSDVWSDYUS**.

Primer: *Šifrirajte* MATEMATIKA *ako je data ključna reć* **MIRKO** *a na raspolaganju vam je Vigener-ov kvadrat*

Rešenje:

Otvoreni tekst:	M A T E M A T I K A
Ključna riječ:	M I R K O M I R K O
Šifrirana poruka:	**Y I K O A M B Z U O**

3.5.2 – Playfair-ova šifra

- Predstavlja polialfabetsku šifru koja se zasniva na upotrebi blokova slova kao osnovnih elemenata otvorenog teksta.
- Ovde se šifruju parovi slova i to tako da rezultat zavisi i o jednom i o drugom slovu.
- Algoritam za šifrovanje se bazira na 5x5 matrici slova, koja se konstruiše koristeći ključnu reč.
- Ako je ključna reč PLAYFAIR, onda matrica izgleda ovako:

P L A Y F
IJ R B C D
E G H K M
N O Q S T
U V W X Z

- Budući da imamo 25 slova, dogovor je da se slova I i J poistovete.
- U slučaju srpskog jezika mi ćemo poistovećivati V i W.
- Šifrovanje se sada vrši na sledeći način:

1. Najprije podelimo otvoreni tekst na blokove od po dva slova.
2. Blokovi ne smeju da imaju ista slova i dužina teksta mora da je parna.
3. I jedno i drugo rešavamo umetanjem slova X ukoliko je to potrebno.

3.5.2 – Playfair-ova šifra

- Kod šifrovanja bloka od dva slova, mogu nastupiti tri slučaja:
  1. Ako se slova nalaze u istom redu menjamo sa slovima koja se nalaze za jedno mesto udesno (ciklično) EH→GK, ST→TN, FP→PL.
  2. Slova se nalaze u istoj koloni. Tada ih menjamo sa slovima koja se nalaze za jedno mesto ispod (ciklično): OV→VL, KY→SC, PI→IE.
  3. U protivnom, pogledamo pravougao koji određuju ta dva slova, te ih zamenimo sa preostala dva vrha tog pravougla. Redosled je određen tako da najprije dođe ono slovo koje se nalazi u istom redu kao prvo slovo u polaznom bloku: OC→SR, RK→CG, PD FI.

Primer: *Šifrujmo otvoreni tekst* CRYPTOGRAPHY *pomoću* Playfairove *šifre s ključem* PLAYFAIR.

Rešenje: CR YP TO GR AP HY → **DB FL NQ OG YL KA**

- Playfairova šifra ima brojne prednosti pred supstitucionom šifrom:
  - ✓ gube se u šifratu jednoslovne reči koje dosta utiču na učestanosti.
  - ✓ bigramsko šifrovanje smanjuje na polovinu broj elemenata dostupnih analizi učestanosti.
  - ✓ broj bigrama je puno veći od broja individualnih slova (676 bigrama)

3.5.2 – Hilova šifra

- Lester Hill je 1929. godine izumeo kriptosistem kod koga se **m slova** otvorenog teksta zamenjuje sa **m slova u šifratu**.
- Predstavlja poligrafsku supstitucijsku šifru, što znači da se zamenjuje više znakova odjednom.
- Čisti tekst se deli na n-torke nad kojima se zatim primenjuje Hillov algoritam i dobija se kriptovana n-torka.
- U slučaju da broj slova otvorenog teksta nije deljiv sa **m**, poruku treba nadopuniti kako bi mogla biti podeljenja u blokove od **m** slova.
- Ključ u ovoj šifri je definisan matricom K dimenzija $\boldsymbol{m \times m}$.
- Element u matrici definišemo po njegovom položaju, odnosno ako je u i-tom redu i j-toj koloni zapisujemo element kao $\boldsymbol{k(i,j)}$.
- Šifra se bazira na množenju matrica i to je prva šifra koja u kriptografiju unela ozbiljniji matematički aparat.
- Ideja Hillovog algoritma za šifriranje je istorijski jako bitna jer je izvršila velik uticaj na formiranje **Feistelovih rundi**, mehanizma koji koriste moderni simetrični blokovski kriptosistemi.

3.5.2 – Hilova šifra

- Šifra funkcioniše na temeljima linearne algebre gde se slova čistog teksta pretvaraju u brojeve i formiraju vektore dimenzije **n**.
- Kao ključ se uzima kvadratna matrica dimenzije **n** invertibilna nad prstenom Z_{26} te se ulazni vektor pomnoži po modulu 26 sa matricom.
- Tako se dobija izlazni vektor dimenzije **n** sastavljen od elemenata prstena Z_{26} čije se numeričke vrednosti pretvaraju nazad u slova.

Primer 1: *Kriptujte tekst* **KREVET** *a kao ključ koristite matricu*:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times_{26} \begin{bmatrix} 10 \\ 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \\ 3 \end{bmatrix} \qquad \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times_{26} \begin{bmatrix} 21 \\ 17 \\ 19 \end{bmatrix} = \begin{bmatrix} 7 \\ 7 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- Kao izlaz dobijamo niz **EADHHG**.
- Izlazni vektor ima brojeve 0-25 jer se operacije izvršavaju po mod26.

Primer 2: *Kriptujete tekst* **KROBET** *korišćenjem istog ključa*:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times_{26} \begin{bmatrix} 10 \\ 17 \\ 14 \end{bmatrix} = \begin{bmatrix} 14 \\ 22 \\ 23 \end{bmatrix} \qquad \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times_{26} \begin{bmatrix} 1 \\ 17 \\ 19 \end{bmatrix} = \begin{bmatrix} 17 \\ 7 \\ 22 \end{bmatrix}$$

- Kao izlaz dobijamo niz **OWXRHW**
- Promenila su se sva slova osim jednog,što znači da Hillova šifra sadrži osnovni princip modernih kriptosistema: **da promena samo jednog elementa ulaza dovodi do promene više elemenata izlaza**

3.5.2 – Hilova šifra

- Dešifriranje se radi na isti način samo što se kao ključ dešifriranja koristi inverzna matrica po mod26 onoj koja je korišćena za šifriranje.
- Korišćenje involutornih matrica (onih koje su inverzne same sebi) olakšava posao jer se ista matrica koristi za šifriranje i dešifriranje
- Ako izvršimo inverziju matrice po modulu 26 iz prethodnog primera dobićemo:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \Rightarrow \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Primer: *Dešifrirajmo niz* **FADHHG** *korišćenjem dobijene inverzne matrice:*

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \times_{26} \begin{bmatrix} 4 \\ 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 10 \\ 17 \\ 4 \end{bmatrix} \qquad \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \times_{26} \begin{bmatrix} 7 \\ 7 \\ 6 \end{bmatrix} = \begin{bmatrix} 21 \\ 17 \\ 19 \end{bmatrix}$$

- Dobili smo polazni niz koji smo šifrirali: **KREVET**.

3.6 – Kriptoanaliza

- Suština kriptografije je očuvanje otvorenog teksta ili ključa od upada prisluškivača kanala/njuškala
- Osnovni zadatak kriptoanalize je da bez ključa odredi otvoreni tekst samo na osnovu šifrata
- Upotrebom kriptoanalize moguće je pronaći slabosti u kriptosistemu
- Pokušaj kriptoanalize naziva se **napad** (***attack***).
- Osnovna postavka kriptoanalize je da tajnost mora biti potpuno zasnovana na ključu jer se kriptografski algoritam poznaje.

- Postoje **četiri opšta tipa** kriptoanalitičkog napada:

  1. Napad "samo šifrat" (***ciphertext-only attack***)

  ✓ Kriptoanalitičar ima šifrate nekoliko poruka šifrovanih istim algoritmom za šifrovanje.

  ✓ Zadatak kriptoanalitičara je da rekonstruiše otvoreni tekst što većeg broja poruka, ili – još bolje – da otkrije ključ (ili ključeve) korišćene za šifrovanje poruka kako bi dešifrovao druge poruke šifrovane istim ključem.

3.6 – Kriptoanaliza

2. Napad "poznat otvoreni tekst" (***known-plaintext attack***)

- ✓ Kriptoanalitičar ima pristup šifratima za nekoliko poruka, kao i otvorenim tekstovima tih poruka.
- ✓ On treba da izračuna ključ korišćen za šifrovanje poruka, ili algoritam

3. Napad "odabran otvoreni tekst" (***chosen-plaintext attack***)

- ✓ Kriptoanalitičar ima pristup šifratu i pripadajućem otvorenom tekstu nekoliko poruka i može da bira otvoreni tekst koji će biti šifrovan.
- ✓ On sada može da odabere specifične blokove otvorenog teksta za šifrovanje i tako dođe do više informacija o ključu.

4. Napad "prilagodljiv odabrani otvoreni tekst" (***adaptive-chosen-plaintext attack***)

- ✓ Ne samo da kriptoanalitičar može da odabere šifrovan otvoreni tekst, već može i da modifikuje ono što je odabrao na osnovu rezultata prethodnih šifrovanja.
- ✓ Ovde on može da odabere manji blok otvorenog teksta, a zatim još jedan na osnovu rezultata prvog, i tako dalje.

Hvala na pažnji !!!

Pitanja

? ? ?