Kriptografija

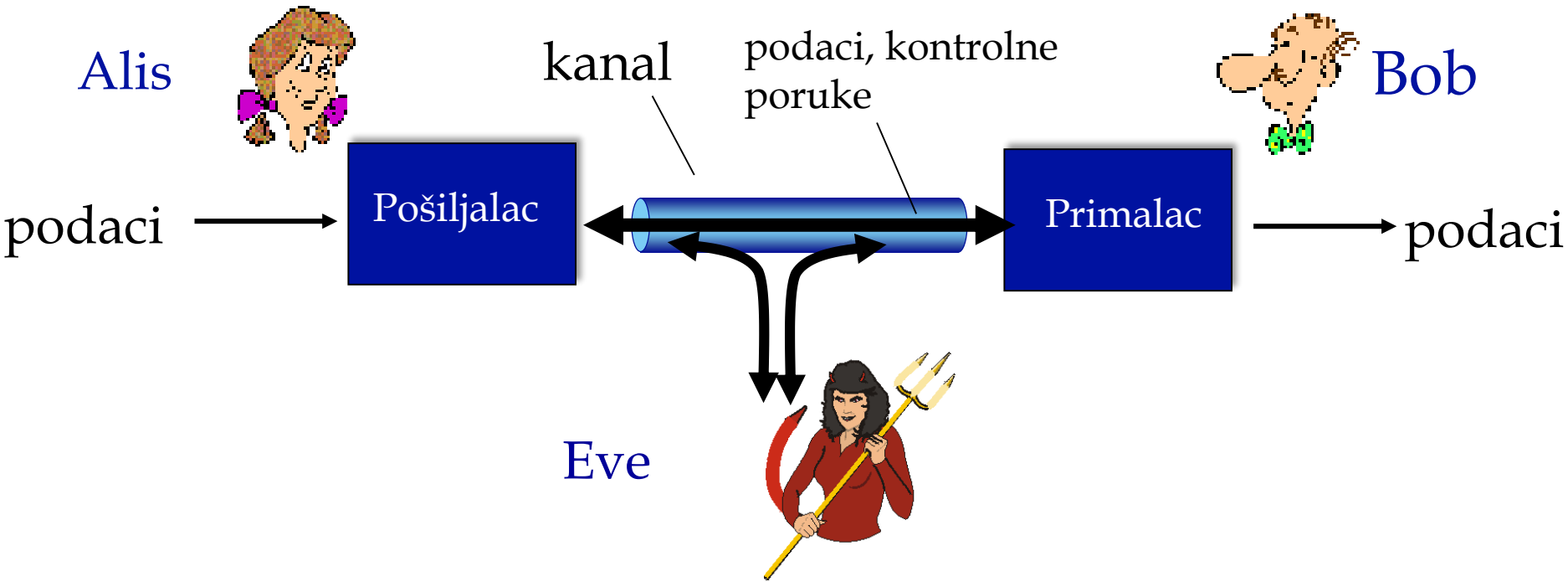
Simetrična enkripcija (Klasične tehnike enkripcije)

dr Slavica Tomović

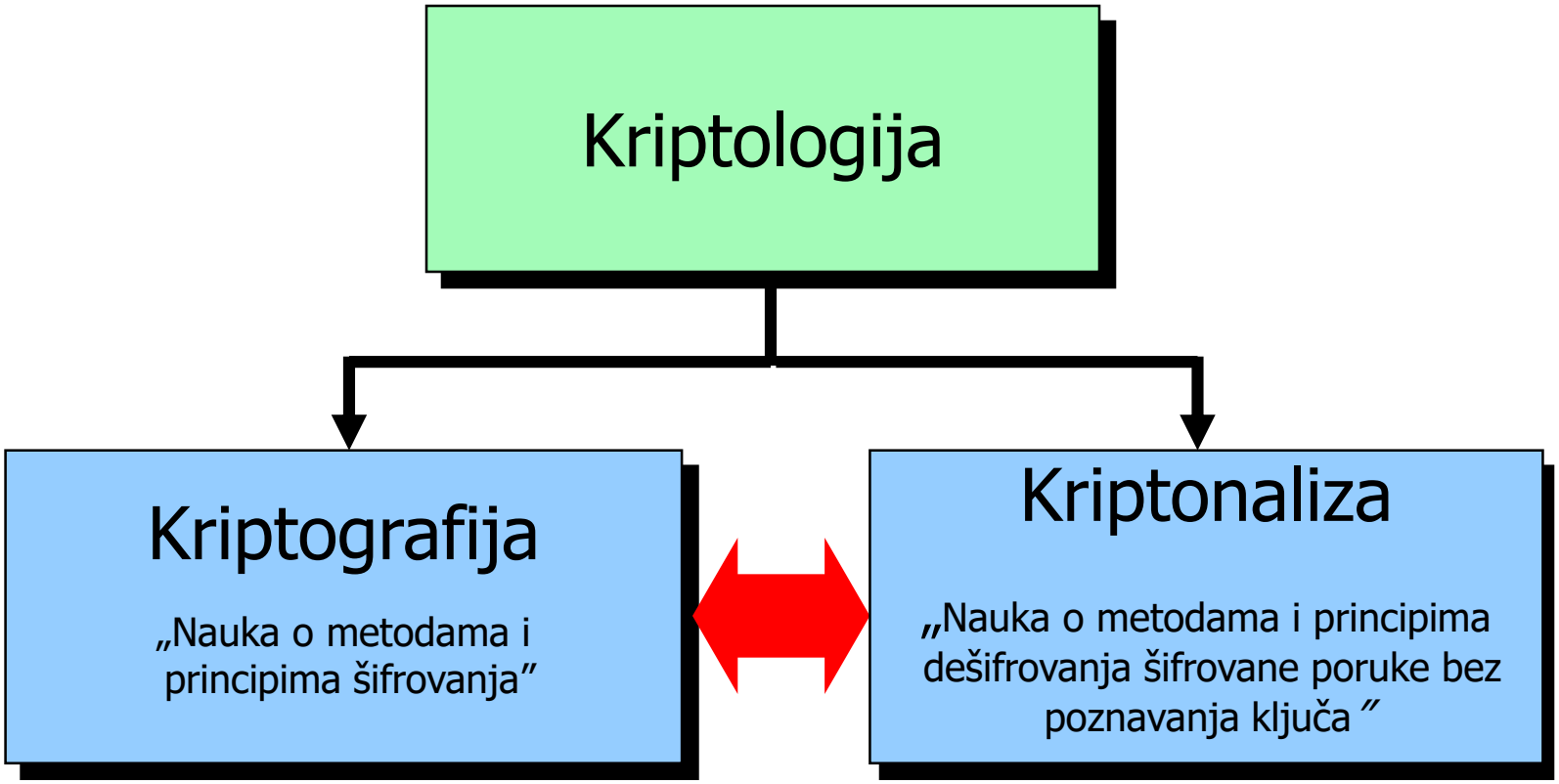
Univerzitet Crne Gore

Kriptologija

- Bob i Alis žele da komuniciraju “sigurno”
- Eve (protivnik) može presresti, izbrisati i dodati poruke
- Kriptologija je naučna disciplina koja bavi proučavanjem postupaka za šifrovanje i dešifrovanje informacija



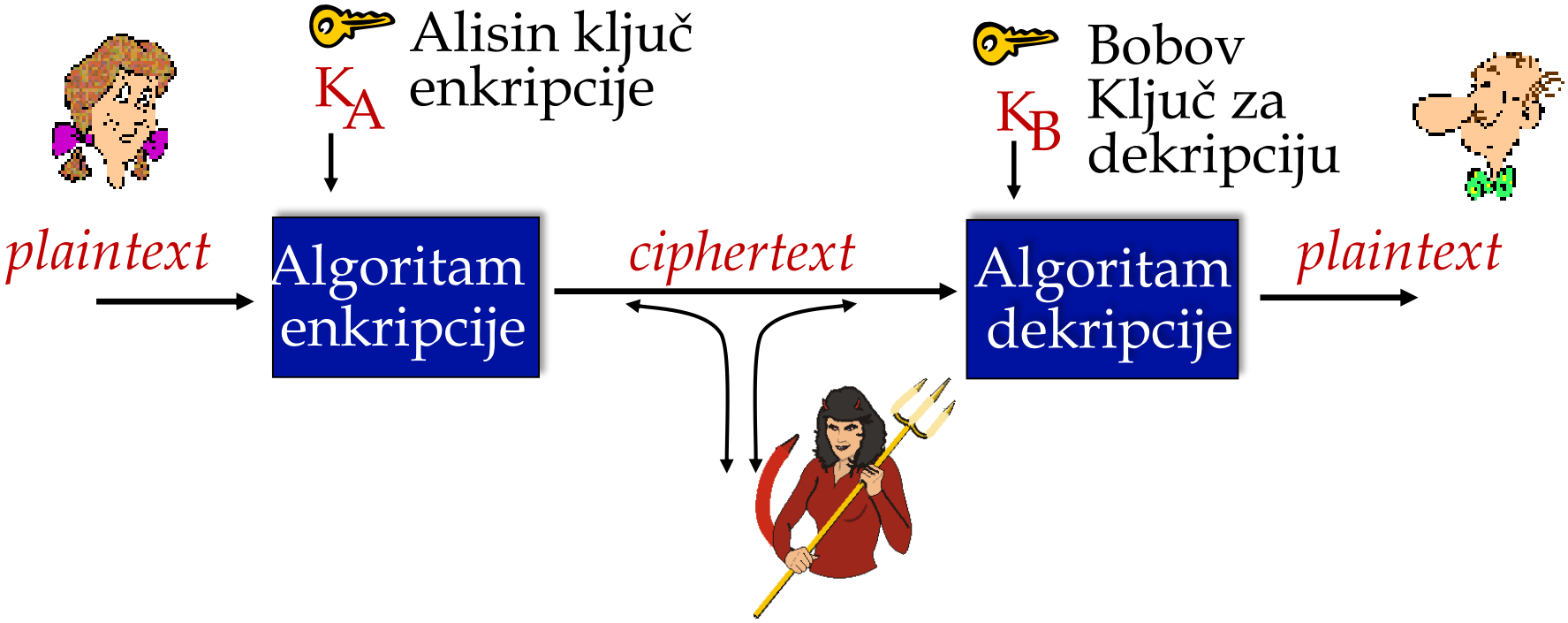
Kriptologija



Kriptografija

- Kriptografija obezbjeđuje sigurnost web sajtova i čini mogućim bezbjedan elektonski prenos informacija.
- Da bi web strana obezbjedila sigurnost prenosa podataka između računara, podaci se moraju šifrovati.
- Omogućava korisnicima *online banking* i *online* kupovinu putem njihovih kreditnih kartica, bez opasnosti da će bilo koji od njihovih računa biti ugrožen.
- Kriptografija je jako značajna za stalni razvoj Interneta, elektronske razmjene i kupovine.

Jezik kriptolgrafije



P: *plaintext*, otvoreni tekst ili originalna poruka

$C = E_{K_A}(P)$: *ciphertext*, poruka enkriptovana algoritmom E, sa ključem K_A

$P = D_{K_B}$ (C) poruke dekriptovana algoritimom D, sa ključem K_B

Osnovna terminologija

- *plaintext* - originalna poruka, “otvoreni tekst”
- *ciphertext*– šifrovana poruka (šifrat)
- *cipher* – algoritam transformacije originalne u kodiranu poruku
- *key* (ključ) – informacija korišćena u šifri, poznata samo pošiljaocu/primaocu
- *encipher* (*encrypt*) – kriptovanje (šifrovanje), tj. konverzija originalne poruke u kodiranu
- *decipher* (*decrypt*) - dešifrovanje (dekriptovanje), odnosno obnavljanje originalne poruke iz šifrovane

Osnovni princip funkcionisanja

- Pošiljalac transformiše originalnu poruku koristeći unaprijed dogovoreni ključ.
- Pošiljalac šalje šifrovanu poruku (šifrat) preko nekog komunikacionog kanala.
- Protivnik prisluškujući može da sazna sadržaj šifrata, ali ne može da odredi originalnu poruku.
- Za razliku od njega, primalac sa odgovarajućim ključem može da dešifruje šifrat i odredi *plaintext* (originalnu poruku)

Kriptosistem

- Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifrovanje i dešifrovanje.
  - Radi se o dvije funkcije, jednoj za šifrovanje, a drugoj za dešifrovanje
  - Njegovi argumenti su ključ i otvoreni tekst, odnosno ključ i šifrat.
- Skup svih mogućih vrijednosti ključeva zovemo prostor ključeva.
- Kriptosistem se sastoji od kriptografskog algoritma, svih mogućih poruka, šifrata i ključeva.

Šta određuje jedan kriptosistem?

Tip korišćene operacije šifrovanja:

- Supstitucione šifre - svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) preslikava se u neki drugi element;
- Transpozicione šifre - elementi otvorenog teksta se permutuju;
- Produkt šifre – kombinuje dvije ili više transformacija (supstitucija ili transpozicija).

Primjer: Ako riječ TAJNA šifrujemo u XIWOI, uradili smo supstituciju, a ako je šifrujemo u JANAT, uradili smo transpoziciju.

Šta određuje jedan kriptosistem?

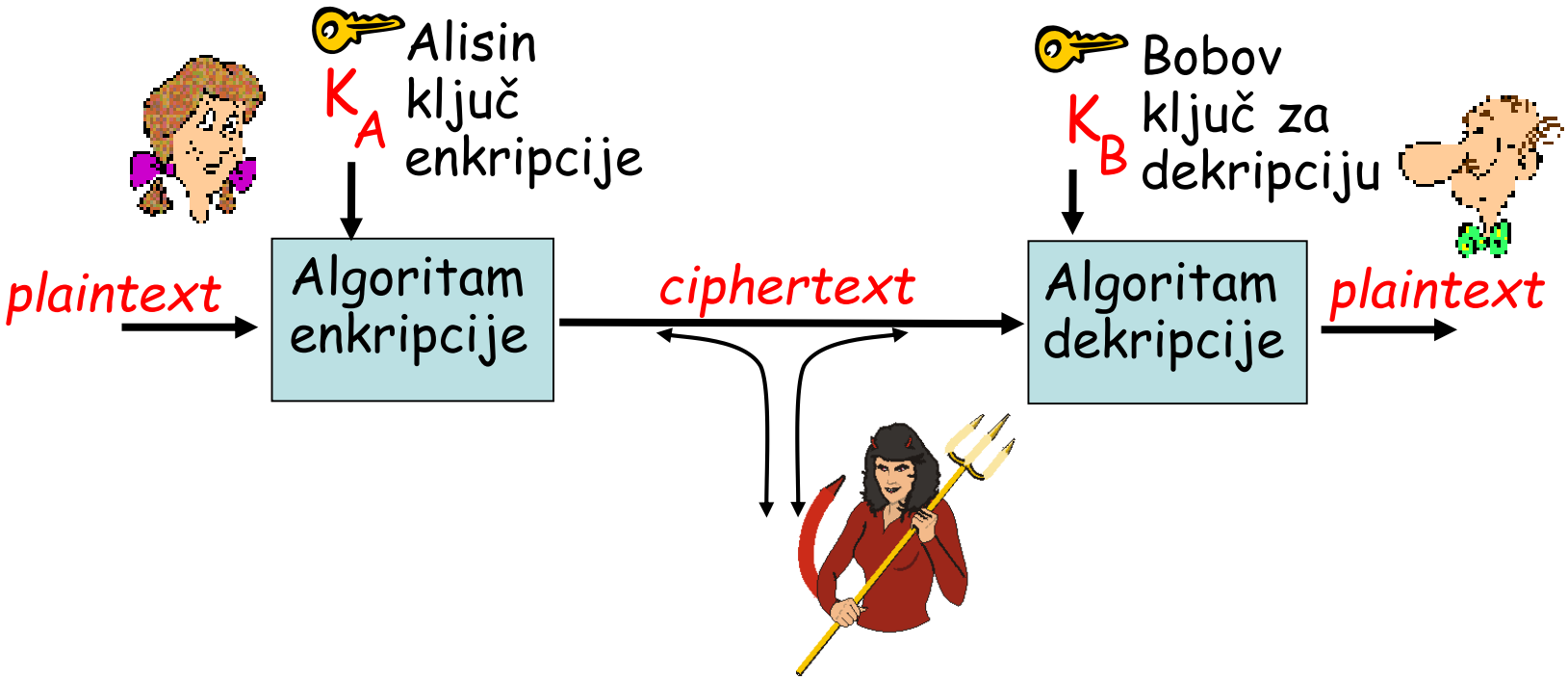
Način na koji se obrađuje originalni tekst:

- Blokovski (engl. *block chiper*) - kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta korišćenjem jednog istog ključa;
- Sekvencijalno (engl. *stream cipher*) - kod kojih se elementi otvorenog teksta obrađuju jedan po jedan korišćenjem niza ključeva koji se paralelno generišu.

Broj ključeva koji se koriste

- Simetrični kriptosistemi - Pošiljalac i primalac dijele zajednički ključ. Sigurnost ovih kriptosistema leži u tajnosti ključa (kriptosistemi s tajnim ključem)
- Asimetrični kriptosistemi (kriptosistem s javnim ključem) - ključ za šifrovanje je javni ključ. Bilo ko može šifrovati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifrovanje (privatni ili tajni ključ) može dešifrovati tu poruku

Simetrični vs asimetrični kriptosistemi

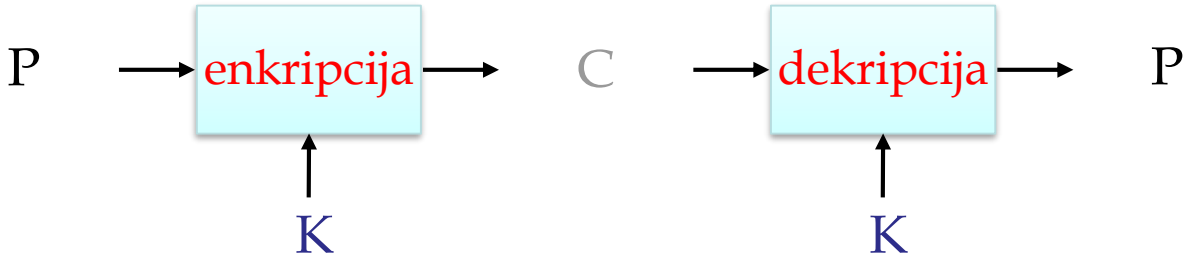


Simetrični kriptosistem: ključevi pošiljaoca i primaoca su *identični*

Aismetrični kriptosistem: ključ koji se koristi za enkripciju je javni, ključ za dekripciju je tajni (privatni)

Simetrični kriptosistemi

- Scenario
  - Alis želi da pošalje poruku (*P*) Bobu.
  - Komunikacioni kanal je nesiguran i može biti prisluškivan
  - Ukoliko su se Alis i Bob prethodno dogovorili oko šeme enkripcije i ključa *K*, poruka se šalje enkriptovana (*ciphertext* C)
- Otvorena pitanja
  - Kako izgleda dobra šema simetrične enkripcije?
  - Kolika je kompleksnost enkripcije/dekripcije?
  - Kolika je veličina šifrata u odnosu na originalnu poruku (*plaintext*)?

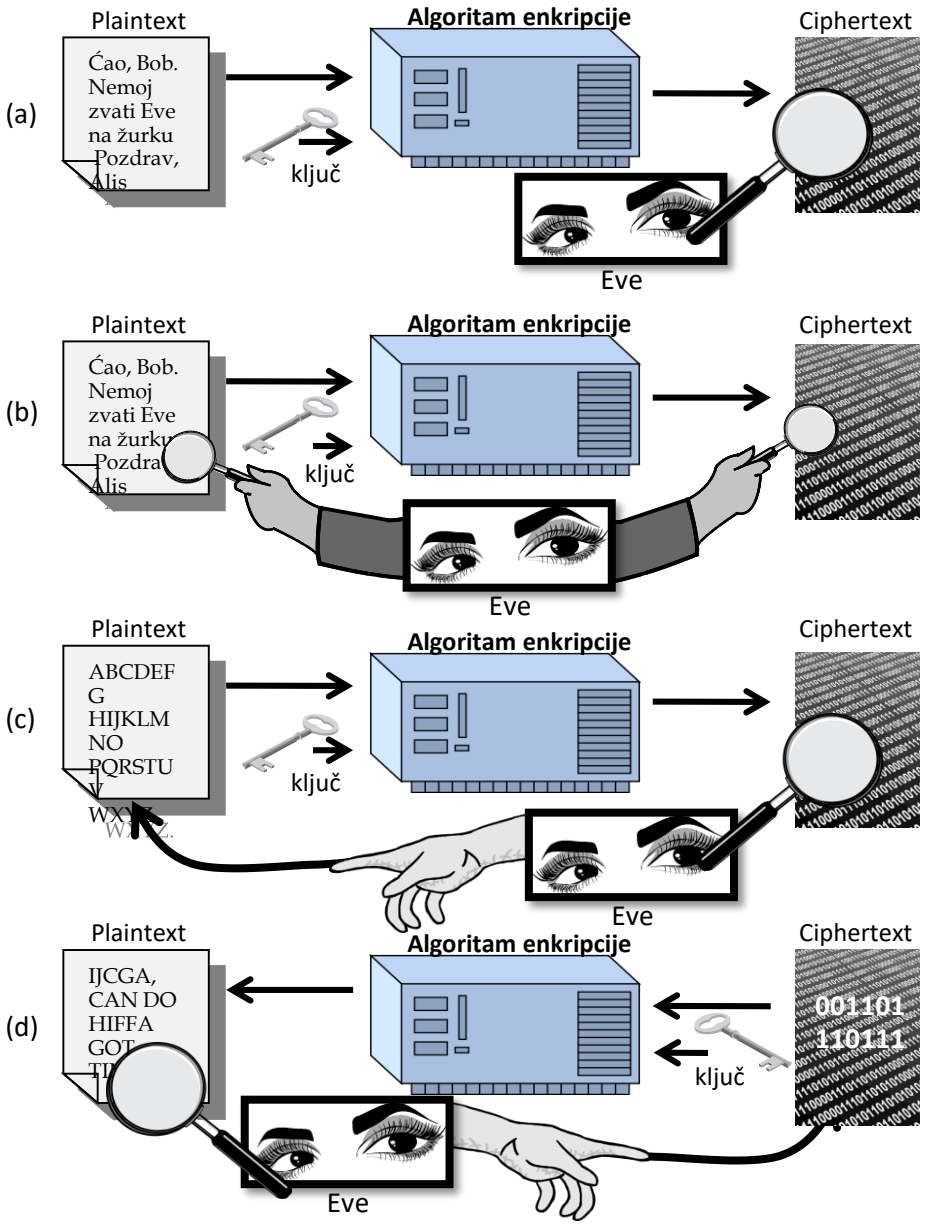


Osnove

- Notacija
  - Tajni ključ K
  - Funkcija enkipcije $E_K(P)$
  - Funkcija dekripcije $D_K(C)$
- Zahtjevi
  - Jak algoritam šifrovanja (čak i kada je poznat veći broj enkriptovanih poruka, kao i njihove neenkriptovane verzije P, nije moguće dešifrovati novu enkriptovanu poruku)
  - Tajni ključ poznat samo pošiljaocu i primaocu: $D_K(E_K(P)) = P$
- Ostale karakteristike
  - Veličina enkriptovane poruke tipično je približno jednaka veličini originalne poruke P
  - Pretpostavlja se da je algoritam šifrovanja poznat
  - Podrazumjeva se siguran kanal za distribuciju ključa

Napadi

- Vrste napada:
  a) Poznata samo kodirana poruka (*cyphertext-only*) - Na osnovu poznatog algoritma enkripcije i statistika može da se odredi orginalna poruka.
  b) Poznati su ili pretpostavljeni originalan tekst i kodirani tekst (*known plaintext*)
  c) Izabran *plaintext* (*chosen-plaintext*) – Izabere se originalan tekst da se dobije kodirani
  d) Izabran kodirani tekst (chosen-ciphertext) – Ubacuje se kodirani tekst da se dobije originalni



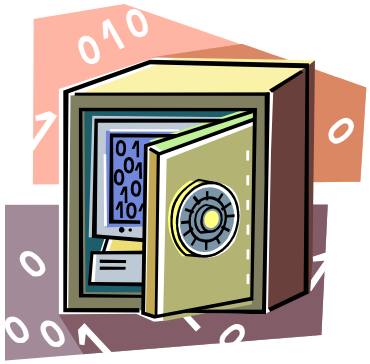
Napad grubom silom

- Pokušaj sve moguće ključeve K i odredi da li je $D_K(C)$ osnovna poruka
  - U prosjeku je potrebno probati barem polovinu mogućih šifara
  - Korisno je određeno poznavanje strukture originalne poruke (npr. da li je PDF fajl ili email poruka, jezik)
- Ključ treba biti dovoljno dug niz slučajnih vrijednosti kako bi napadi ovog tipa bili teško izvodljivi

Image by Michael Cote from http://commons.wikimedia.org/wiki/File:Bingo_cards.jpg

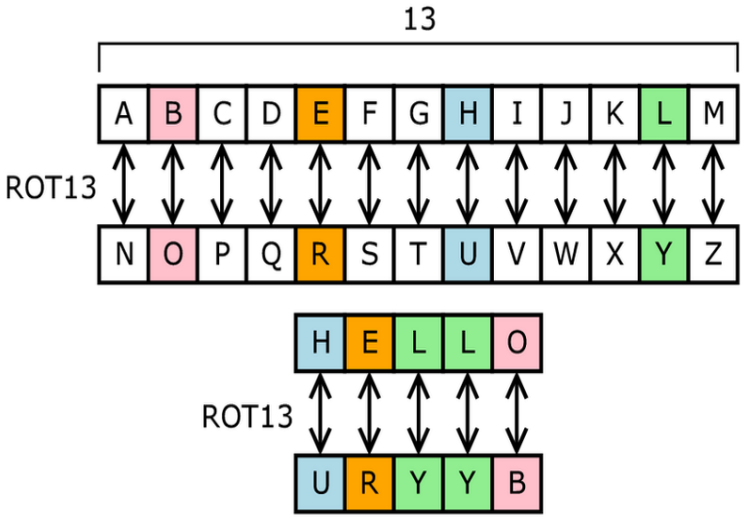
Dodatne definicije

- Bezuslovna sigurnost
  - Bez obzira na raspoložive računare, šifra se ne može razbiti, jer kodirana poruka nema dovoljno informacija da jedinstveno odredi odgovarajući otvoreni tekst
- Računarska sigurnost
  - Pri datim računarskim resursima, šifra se ne može razbiti u smislenom vremenu
  - Cijena razbijanja šifre prevazilazi vrijednost informacije



Klasične supstitucione šifre

- Slova osnovne poruke se zamjenjuju drugim slovima, brojevima ili simbolima
- Jedan od popularnih supstitucionih šifratora za Interenet postove je ROT13



Cezarova šifra

- Najranija poznata enkripcija
- Koristio je Julije Cezar
  - Upotreba u vojnim operacijama
- Zamijeniti svako slovo sa slovom koje je za *n* mjesta dalje u alfabetu

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

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

Primjer: enkriptovati “Napadam”

Kriptoanaliza Cezarove šifre

- Ukoliko se razmatra engleski alfabet, samo 26 različitih kodiranih tekstova
  - A se preslikava u A,B,..Z
  - Može se probati svih 26 (25) preslikavanja metodom grube sile
- Dat kodiran tekst, probate sve varijante ključa
  - Potrebno je prepoznati smislen tekst
  - Npr. razbiti poruku “X NROLNR VDWL MH QDSDG”

Kriptoanaliza Cezarove šifre

Ključ	
1	W MQNKMQ UCVK LG PCRCF
2	V LPMJLP TBUJ KF OBQBE
3	U KOLIKO SATI JE NAPAD
4	T JNKHJN RZSH ID MZOZC
5	S IMJGIM QYRG HC LYNYB
6	R HLIFHL PXQF GB KXMXA
7	Q GKHEGK OWPE FA JWLWZ
8	P FJGDFJ NVOD EZ IVKVY
9	O EIFCEI MUNC DY HUJUX
10	N DHEBDH LTMB CX GTITW
11	M CGDACG KSLA BW FSHSV
12	L BFCZBF JRKZ AV ERGRU
13	K AEBYAE IQJY ZU DQFQT

Ključ	
14	J ZDAXZD HPIX YT CPEPS
15	I YCZWYC GOHW XS BODOR
16	H XBYVXB FNGV WR ANCNQ
17	G WAXUWA EMFU VQ ZMBMP
18	F VZWTVZ DLET UP YLALO
19	E UYVSUY CKDS TO XKZKN
20	D TXURTX BJCR SN WJYJM
21	C SWTQSW AIBQ RM VIXIL
22	B RVSPRV ZHAP QL UHWHK
23	A QUROQU YGZO PK TGVGJ
24	Z PTQNPT XFYN OJ SFUFI
25	Y OSPMOS WEXM NI RETEH

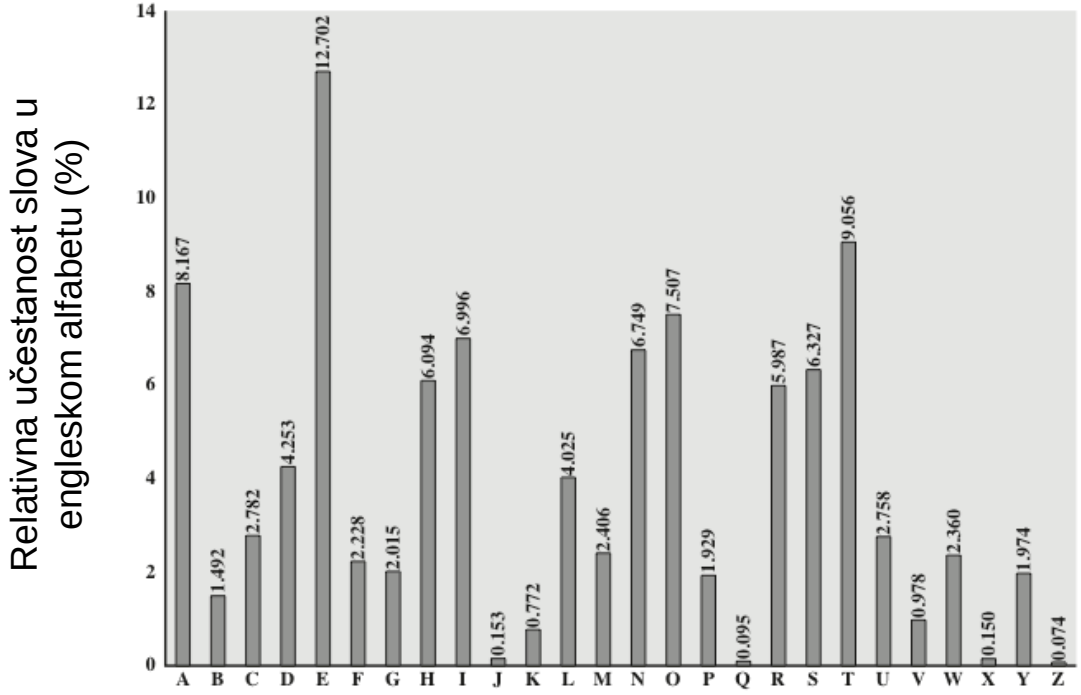
Monoalfabetska enkripcija

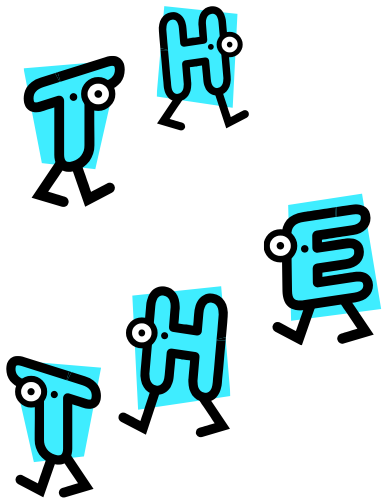
- Permutacija
  - Promiješati alfabet (permutacija svih slova alfabeta) i primijeniti na otvoreni tekst
  - Svako slovo osnovne poruke se preslikava u različito slovo u enkritptovanom tekstu
  - Za alfabet od 26 karaktera postoji 26!, odnosno preko 4 x 1026 mogućih ključeva

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: QAZWSXEDCRFVTGBYHNUJMIKOLP
Plaintext: napad je u podne
Ciphertext: GQYQW RS M YBWGS
```

Monoalfabetska enkripcija

- Laka za "provaljivanje"jer se ne mijenja relativna učestanost slova
  - Izračunati učestanost slova u enkriptovanom tekstu
  - Uporediti učestanost slova sa poznatom statistikom jezika
  - Tabele sa čestim parovima i trojkama slova pomažu





Monoalfabetska enkripcija

Primjer kriptoanalize:

- Dat kodirani tekst:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- Izračunati relativnu učestanost slova u tekstu
- Pretpostaviti da su ***P*** i ***Z***, ***e*** i ***t***
- Pretpostaviti **ZW** je "**th**", pa je **ZWP** "**the**"
- Produžavanjem sa pretpostavkama i ispravkama grešaka:

```
it was disclosed yesterday that several informal
but direct contacts have been made with political
representatives of the viet cong in moscow
```

Playfair šifra

- Šifrovanje većeg broja slova odjednom
- Veliki broj ključeva u monoalfabetskoj šifri nije obezbijedio sigurnost
- Tretira digrame u originalnom tekstu kao jedinice za šifrovanje
- 5 x 5 matrica slova zasnovana na ključu
  - Matrica se popunjava po vrstama sa slovima ključa, uz izostavljanje duplikata
  - Ostatak matrice se popunjavam ostalim slovima alfabeta, po redosledu

Primjer za ključ: **MONARCHY**

I i **J** se tretiraju kao isto slovo!

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

Playfair šifra

Tekst se šifruje po dva slova odjednom, po sledećim pravilima:

1. Ako je par ponovljeno slovo, ubaciti slovo za dopunu (npr. ‘X’)

npr . riječ "balloon" šifruje po parovima "ba lx lo on"

1. Ako oba slova pripadaju istom redu, zamijeni sa slovima udesno u istom redu (uz rotaciju)

npr. “ar" se šifruje kao "RM"

2. Ako su oba slova u istoj koloni, zamijeni sa slovom ispod (opet sa rotacijom)

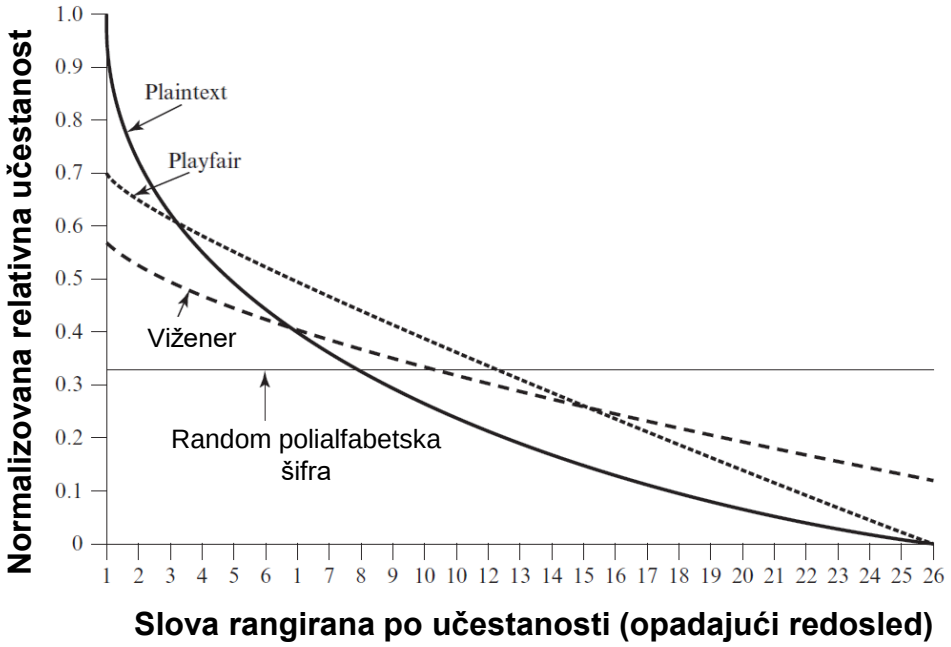
npr “mu" se šifruje kao "CM"

1. U svim ostalim slučajevima se slovo zamjenjuje slovom iz istog reda koje odgovara tjemenu pravougaonika zone koju formira ulazni par

npr. “hs" se šifruje kao "BP", a “ea" kao "IM" ili "JM" (po želji)

Sigurnost Playfair šifre

- Sigurnost značajno popravljena u odnosu na monoalfabetsku šifru
- Postoji 26 x 26 = 676 digrama (parova slova)
- Ipak lake za razbijanje: još uvek sadrže mnoge elemente strukture originalnog teksta



Hill-ova šifra

- U potpunosti "krije" učestanost pojedinačnih slova
- *m* sukcesivnih slova originalnog teksta se zamjenjuje sa *m* slova kriptovanog teksta:
  - Svaki karakter originalnog teksta *P* se numeriše (a = 0, b = 1, c=2, … z = 25 u engleskom alfabetu)
  - Ključ *K* je dat u vidu matrice dimnezije ***m*x*m***
  - Za m=3 šifrovani tekst **C** se dobija rešavanjem tri jednačine:

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \text{mod} 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{32}p_3) \text{mod} 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \text{mod} 26$$

ili u matričnom obliku: $\mathrm{C} = \mathrm{PK} \bmod 26$

$$(c_1\, c_2\, c_3) = (p_1\, p_2\, p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

Hill-ova šifra

- Primjer:
  - Enkripcija poruke “YOU”: P=(24, 14, 20)
  - Pretpostavimo da je ključ:

$$K = \begin{pmatrix} 3 & 25 & 4 \\ 23 & 6 & 15 \\ 13 & 17 & 21 \end{pmatrix}$$

  - Enkriptovanu poruku dobijamo:

$$c_1 = (3 \cdot 24 + 14 \cdot 23 + 13 \cdot 20) \bmod 26 = 654 \bmod 26 = 4\,(E)$$
$$c_2 = (15 \cdot 24 + 14 \cdot 6 + 17 \cdot 20) \bmod 26 = 1024 \bmod 26 = 10\,(K)$$
$$c_3 = (4 \cdot 24 + 14 \cdot 15 + 21 \cdot 20) \bmod 26 = 726 \bmod 26 = 24\,(Y)$$

  - Enkriptovana poruka je C=(4, 10, 24), odnosno “EKY”

Hill-ova šifra

- Dekripcija:
  - $\mathrm{P} = \mathrm{D}(\mathrm{K}, \mathrm{C}) = \mathrm{C}\mathrm{K}^{-1} \bmod 26 = \mathrm{P}\mathrm{K}\mathrm{K}^{-1} = \mathrm{P}$
- Određivanje K^{-1}:
  - $\det(K)\, mod\ 26 = -6335\, mod\ 26 = 9\, mod\ 26$
  - $\det(K)^{-1} = 9^{-1}\ \ mod\ 26 = 3$
  - Odrediti adjungovanu matricu
  - $K^{-1} = \det(K)^{-1}\,\mathrm{adj}(\mathrm{K})\ mod\ 26 = 3\ \mathrm{adj}(\mathrm{K})\ mod\ 26$

$$K^{-1} = \begin{pmatrix} 3 & 7 & 13 \\ 20 & 7 & 11 \\ 3 & 16 & 19 \end{pmatrix}$$

Za domaći: Dekriptovati poruku **EKYIMBHKXVNAZYUELMVPBJVS**

Polialfabetske šifre

- Polialfabetski supstitucioni čiper
  - Upotreba višestrukih alfabeta šifara
  - Otežava kriptoanalizu jer treba pogoditi više alfabeta, a zaravnjuje distribuciju učestanosti

Zajednička svojstva polialfabetskih tehnika enkripcije:

- Koristi se set povezanih monoalfabetskih supstitucionih pravila
- Na osnovu ključa bira se pravilo koje će se koristiti za svako slovo u originalnom tekstu

Vigenere šifra

- Ideja: Koristiti Cezarov šifrator sa različitim pomjerajima kako bi se sakrila distribucija slova.
- Ključ definiše pomjeraj koji će se koristiti za svako slovo u originalnom tekstu.
- Ukoliko je poruka duža od ključa, ključ se koristi iznova.

Plaintext: I a t t a c k
Key: 2 3 4 2 3 4 2 (Ključ je "234")
Ciphertext: K d x v d g m

Sigurnost Vigenere šifre

- Više slova u kodiranom tekstu za svako slovo originalnog teksta
- Učestanost slova narušena, ali nije potpuno izgubljena
- Ideja za kriptoanalizu – Kasiski metod:
  - Početi sa analizom učestanosti slova
  - Ponavljanja u kodiranom tekstu daju sugestiju o dužini ključa
    - Pronađi nekoliko ponovljenih sekvenci u šifrovanoj poruci
    - Izračunaj rastojanja između ovakvih sekvenci i traži zajednički faktor
  - Da li je šifra monoalfabetska? Ukoliko nije posmatraj šifru kao sekvencu monoalfabetskih šifara i napadaj sistem kao da je monoalfabetski

Vigenere Autokey sistem

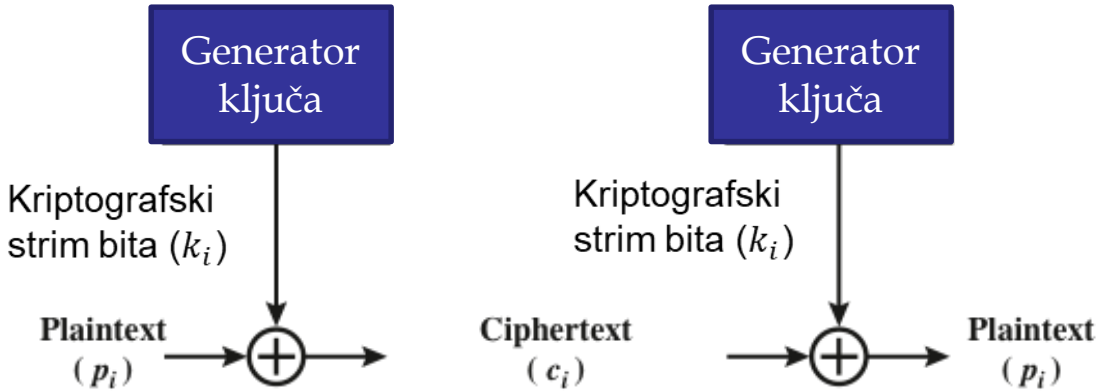
- Želimo ključ dužine poruke
- Ključ se dobija spajanjem ključne riječi sa odsječenim originalnim tekstom
- Poznavanjem ključne riječi se otkriva prvih nekoliko slova originalne poruke, pa se onda ta slova koriste za dešifrovanje daljih slova poruke
- Još uvijek postoje karakteristike učestanosti

Primjer

- Ključna riječ: deceptive
- Ključ: deceptivewearediscoveredsav
- Plaintext: wearediscoveredsaveyourself
- Ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

Vernam-ova šifra

- 1918.godina.
- Radi nad binarnim podacima:
  - $c_i = p_i$ XOR k_i
  - $p_i = c_i$ XOR k_i
- Vernam je predložio dugačku traku sa ključem koja se ponavlja
- I dalje ostaje mogućnost statističke analize teksta sa dovoljnom količinom kriptografskog materijala

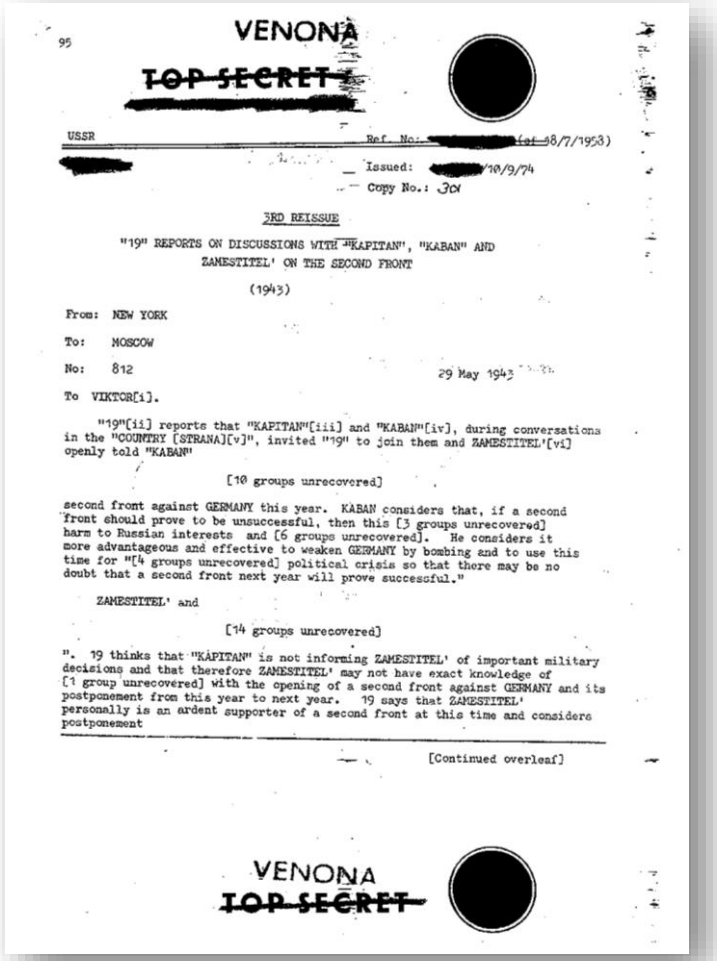


One-Time Pad

- Poboljšanje Vernamovog čipera
- Koristi se random ključ koji je dug kao i poruka, tako da nema potrebe za ponavljanjem ključa
- Ključ se koristi za enkripciju i dekripciju samo jedne poruke, a zatim se diskredituje
- Svaka nova poruka zahtijeva novi ključ iste dužine kao nova poruka
- Šema enkripcije se **ne može razbiti**
  - Kreira slučajni (random) izlaz koji nema statističku vezu sa originalnim tekstom

One-Time Pad

- Problem je distribucija ključa
- Ključevi se ne smiju ponavljati
  - Ponovljeno korišćenje *one-time pad* ključa omogućilo je USA da razbije komunikaciju sovjetskih špijuna tokom Hladnog rata.



95

VENONA

~~TOP SECRET~~ [redacted]

USSR

Ref. No.: [redacted] (of 18/7/1958)

[redacted]

Issued: [redacted] 10/9/74

Copy No.: 301

3RD REISSUE

"19" REPORTS ON DISCUSSIONS WITH "KAPITAN", "KABAN" AND ZAMESTITEL' ON THE SECOND FRONT

(1943)

From: NEW YORK

To: MOSCOW

No: 812

29 May 1943

To VIKTOR[i].

"19"[ii] reports that "KAPITAN"[iii] and "KABAN"[iv], during conversations in the "COUNTRY [STRANA][v]", invited "19" to join them and ZAMESTITEL'[vi] openly told "KABAN"

[10 groups unrecovered]

second front against GERMANY this year. KABAN considers that, if a second front should prove to be unsuccessful, then this [3 groups unrecovered] harm to Russian interests and [6 groups unrecovered]. He considers it more advantageous and effective to weaken GERMANY by bombing and to use this time for "[4 groups unrecovered] political crisis so that there may be no doubt that a second front next year will prove successful."

ZAMESTITEL' and

[14 groups unrecovered]

". 19 thinks that "KAPITAN" is not informing ZAMESTITEL' of important military decisions and that therefore ZAMESTITEL' may not have exact knowledge of [1 group unrecovered] with the opening of a second front against GERMANY and its postponement from this year to next year. 19 says that ZAMESTITEL' personally is an ardent supporter of a second front at this time and considers postponement

[Continued overleaf]

VENONA

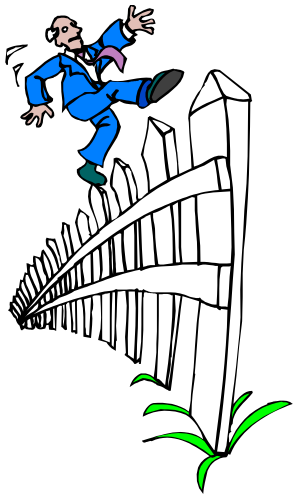
~~TOP SECRET~~ [redacted]

Rail Fence šifrator

- Najjednostavniji transpozicioni čiper
- Plaintext se ispisuje dijagonalno u nekoliko redova
- Krajnja šifra se čita red po red
- Trivijalno za kriptoanalizu
- Primjer:
  - Plaintext: VOZ IDE PO PRUZI
  - Poruka se ispisuje u tri reda (redovi imaju ulogu ključa)

```
V...d...p...i
.o.i.e.o.r.z.
..z...p...u..
```

  - Chipertext: VDPIOIEORZZPU



Row Transposition šifrator

- Kompleksnija transpozicija
- Poruka se ispisuje u formi matrice, red po red
- Šifrovana poruka se čita kolonu po kolonu, ali se permutuje redosled kolona
  - Redosled kolona predstavlja ključ algoritma

Ključ: 4 3 1 2 5 6 7

Plaintext: ZANIMLJIVA INFORMACIJA

```
z a n i m l j
i v a i n f o
r m a c i j a
```

Ciphertext: NAAIICAVMZIRMNILFJJOA

- **Višestrukom transpozicijom se može poboljšati sigurnost**

Produkt algoritmi

- Supstitucioni i transpozicioni algoritmi nisu dovoljno sigurni zbog jezičkih karakteristika
- Zato se koristi više algoritama uzastopno da bi se šifre učinile sigurnijim:
  - dva algoritma supstitucije čine kompleksniju supstituciju
  - dva algoritma transpozicije čime kompleksniju transpoziciju
  - algoritam zamjene, praćen algoritmom transpozicije čini novu, mnogo komplikovaniju šifru
  - Produkcioni algoritmi predstavljaju most između klasičnih i modernih šifri

Rotor mašine

- Prije modernih šifara, rotor mašine su bile najpopularnije produkt šifre
- Korišćene su u Drugom svjetskom ratu
  - Nemačka Enigma, Japanska Purple
- Korišćen je niz nezavisno rotirajućih cilindara
- Svaki cilindar ima 26 ulaznih i 26 izlaznih tačaka, koje su interno međusobno povezane tako da je svaki ulaz povezan sa jedinstvenim izlazom
- Ako se svakoj ulaznoj i izlaznoj tački dodijeli po jedno slovo engleskog alfabeta, tada jedan cilindar definiše jedan monoalfabetski algoritam zamjene

Rotor mašine

- Ako posmatramo mašinu sa samo jednim cilindrom i ako se cilindar rotira nakon šifrovanja jednog slova, imali bismo polialfabetski supstitucioni algoritam sa periodom 26 (eng. alfabet)
- Mašina sa jednim cilindrom ne proizvodi složene šifre, ali kada se upotrebi veći broj cilindara situacija se mijenja
- Zamislimo mašinu sa 3 cilindra, koji su redno vezani, tako da su izlazi prvog povezani na ulaze drugog, a izlazi drugog povezani na ulaze trećeg cilindra
  - Prvi cilindar se rotira za 1 nakon svakog šifrovanog slova, drugi cilindar se rotira za 1 svaki put kada prvi cilindar završi kompletan ciklus (26 rotacija), treći cilindar se rotira za 1 svaki put kada drugi cilindar završi kompletan ciklus (26 rotacija)
  - Sada postoji 17576 različitih algoritama zamjene koji se koriste prije nego što dođe do ponavljanja

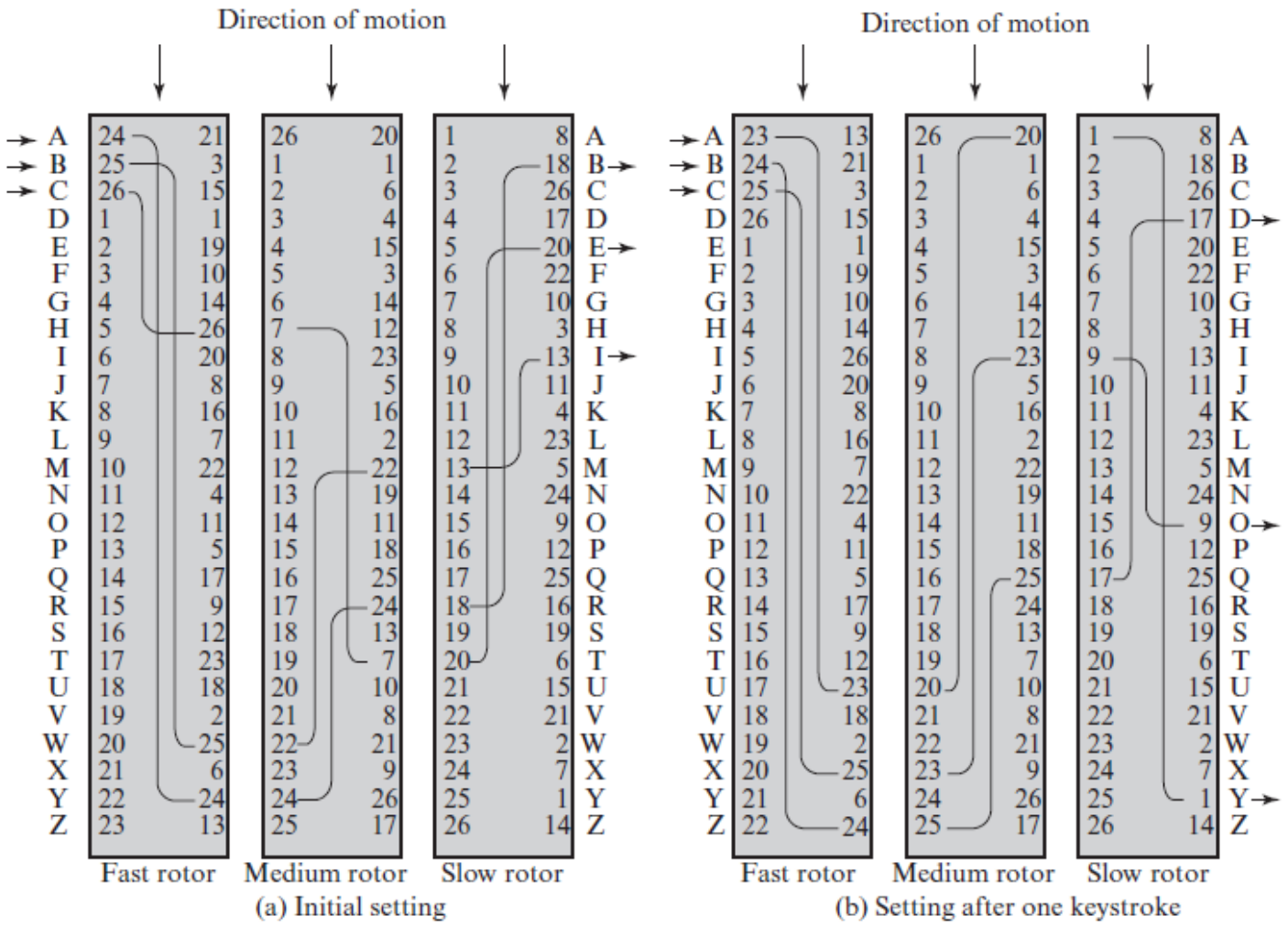
Enigma

- 65 x 45 x 35cm, 50kg
- Ključ – knjiga kodova
- Postupak:
  - Podešavanje prema ključu
  - Kucanje slova po tastaturi
  - Paljenje lampice koja odgovara šifrovanom slovu
  - Slanje poruke radio vezom

Bomba

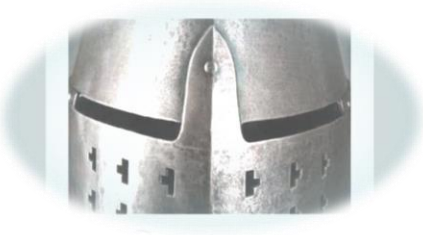
- 2.1m x 1.98m x 0.61m
- Poznata originalna poruka
- Na osnovu prevoda pronaći sva moguća podešavanja Enigme

Rotor mašine



Rezime

- Simetrična enkripcija
  - Kriptografija
  - Kriptoanaliza i napad grube sile
- Transpozicione tehnike enkripcije
- Rotor mašine



- Supstitucione tehnike enkripcije
  - Cezar šifra
  - Monoalfabetske šifre
  - Playfair šifra
  - Hill-ova šifra
  - Polialfabetske šifre
  - One-time pad