Klasična kriptografija

Sadržaj

- Osnovni pojmovi
- Šifre transpozicije
- Šifre zamene
- Kodne knjige

Podela

- Tajnost komunikacija:
  - Steganografija. Skrivanje poruke.
  - **Kriptologija**.
    - Kriptografija. Skrivanje značenja poruke.
    - Kriptoanaliza.

Osnovni pojmovi

- **Otvoreni tekst** (engl. *plaintext*) je poruka ili dokument koji treba da se zaštiti.
- **Šifrovanje** (engl. *encryption*) je skup operacija kojom se otvoreni tekst menja kako bi postao nerazumljiv.
  - Rezultat šifrovanja je **šifrat** (engl. *ciphertext*).
  - Skup pravila koji se koristi za šifrovanje otvorenog teksta se naziva **algoritam šifrovanja**.
  - Operacije algoritma šifrovanja zavise od vrednosti **ključa šifrovanja** (engl. *key*).
    - Ključ je ulazni parametar kao i otvoreni tekst.
- **Dešifrovanjem** (engl. *decryption*) se iz šifrata dobija otvoreni tekst.
  - Skup pravila koji se koristi za dešifrovanje šifrata se naziva **algoritam dešifrovanja**.
  - Ključ dešifrovanja određuje način rada algoritma dešifrovanja.

Osnovni pojmovi

- **Šifarski sistem sa simetričnim ključem** (engl. *symmetric key cryptosystem*) koristi isti ključ za šifrovanje i dešifrovanje.
  - Preciznije, dovoljno je da se iz jednog ključa može jednoznačno izračunati drugi ključ.
- **Šifarski sistem sa javnim ključem** (engl. *public key cryptosystem*) koristi:
  - **Javni ključ** (engl. *public key*) za šifrovanje.
  - **Privatni ključ** (engl. *private key*) za dešifrovanje.
  - Poznavanje javnog ključa nije dovoljno za izračunavanje ključa za dešifrovanje!
- **Kriptografija** je nauka o dizajniranju šifarskih sistema.

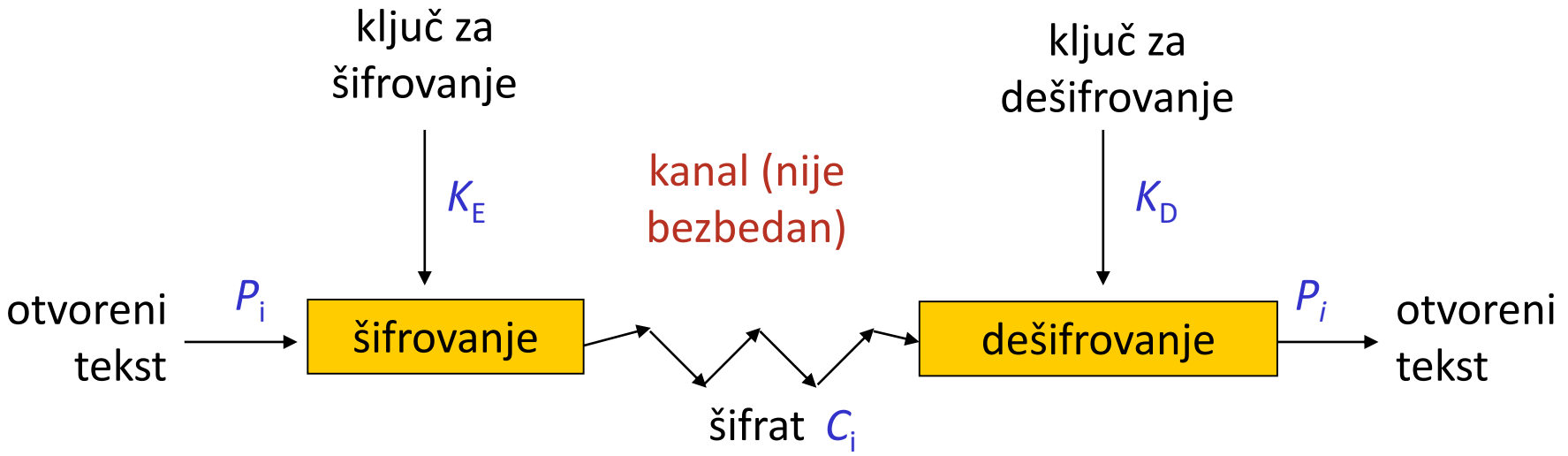
Polazne tačke

- **Cilj svakog kriptosistema**:
  - Da bi se od šifrata dobio otvoreni tekst NEOPHODNO je poznavanje ključa za dešifrovanje!
  - Ako napadač poznaje postupak šifrovanja – algoritam i šifrat (i još ...), on ne može doći do otvorenog teksta bez poznavanja ključa za dešifrovanje.
- Cilj : realnost?
- **Osnovne pretpostavke** u analizi sistema:
  - Sistem je potpuno poznat napadaču (*Trudy*).
  - Jedina tajna je ključ (za dešifrovanje).
- Ovo su **Kerhofovi (Kerckhoff) principi**.
  - Algoritam šifrovanja nije tajna!

Zašto se uvode ove pretpostavke?

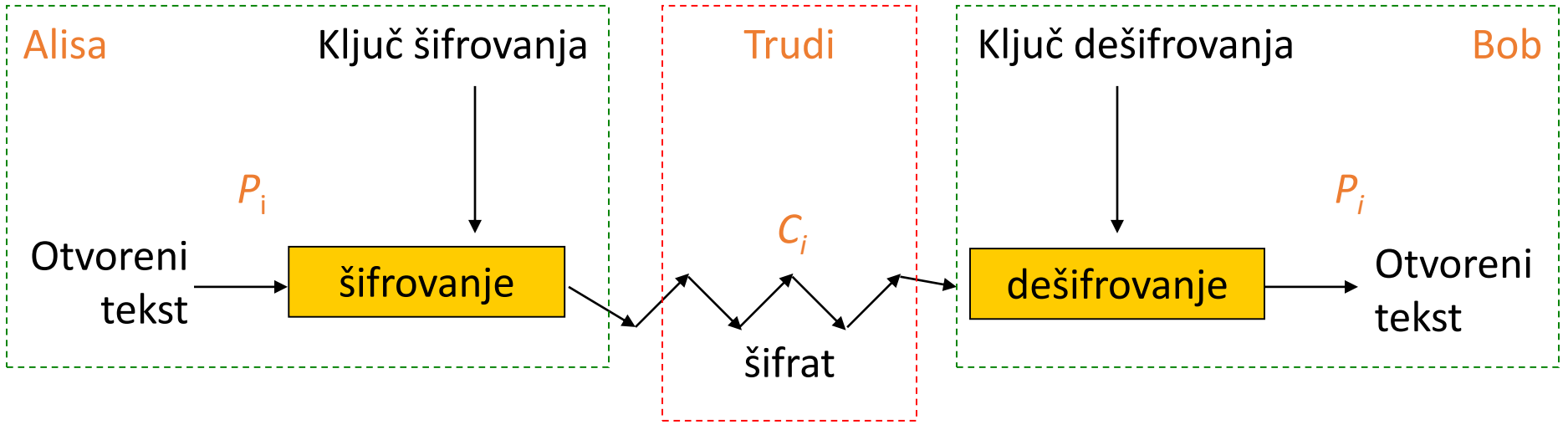
- Trudi će sigurno imati **teži posao ako ne zna algoritam**, ali ...
  - Tajni algoritmi retko dovoljno dugo ostaju tajni.
    - Reverzni inženjering sotvera i hardvera.
    - Neko može namerno da “pusti” algoritam u javnost.
    - …
  - Analiza tajnih algoritama (kada postanu dostupni) pokazuje da oni često imaju slabosti.
  - Javni algoritmi su **podložni analizi** mnogih kriptoanalitičara.
    - Bolje je znati slabosti unapred.

Blok šema



- P_i je i-ta "jedinica" otvorenog teksta
- "jedinica" može da bude bit, slovo, blok (niz) bita i sl.
- C_i je odgovarajući šifrat
- $C = E(P, K_E)$
- $P = D(C, K_D)$

Šta ko zna?



- Trudi zna šifrat.
- Trudi zna i kako radi algoritam šifrovanja/dešifrovanja.
- Trudi možda zna i još nešto.
- Trudu NE ZNA ključ dešifrovanja.

Kriptoanaliza

- **Kriptoanaliza** je proces pronalaženja informacija o otvorenom tekstu bez poznavanja ključa za dešifrovanje.
- Cilj kriptoanalize ne mora biti otvoreni tekst.
- Cilj može da bude:
  - Identifikovanje ključa.
  - Identifikovanje skupa loših ključeva.
- **Kriptologija** obuhvata kriptografiju i kriptoanalizu!

Lars Knudsen-ova klasifikacija rezultata kriptoanalitičkih napada

- Klasifikacija prema količini i kvalitetu otkrivenih tajnih informacija (od najboljeg rezultata ka najlošijem):
  - **Potpuno probijanje** (engl. *total break*).
    - Napadač je otkrio tajni ključ.
  - **Globalna dedukcija** (engl. *global deduction*).
    - Napadač je otkrio funkciju koja je ekvivalent algoritma za (de)šifrovanje, ali ne i ključ.
  - **Lokalna dedukcija** (engl. *instance or local deduction*).
    - Napadač je otkrio dodatne otvorene tekstove (ili šifrate) koji ranije nisu bili poznati.
  - **Informaciona dedukcija** (engl. *information deduction*).
    - Napadač dobija meru informacije sadržane u određenoj poruci o otvorenim tekstovima (ili šifratima) koji ranije nisu bili poznati.
  - **Algoritam koji omogućuje razlikovanje** (engl. *distinguishing algorithm*).
    - Napadač može razlikovati šifrat od slučajne permutacije.

Potpuna pretraga ključeva

- Na koji način Trudi može da napadne šifarski sistem?
- Ona može da isproba sve moguće ključeve i da nakon svakog dešifrovanja proveri da li je dobila željeni rezultat.
  - Ovaj postupak se naziva **potpuna pretraga ključeva**.
- Da bi se Trudi obeshrabrila, šifarski sistem treba da ima veoma veliki broj potencijalnih ključeva, odnosno veliki **prostor ključeva** (engl. *keyspace*).
  - Broj potencijalnih ključeva mora biti toliki da ih Trudi ne može isprobati u razumnom vremenu!

Ostali napadi

- Veliki prostor ključeva je **neophodan** za bezbednost šifarskog sistema.
- Ovo je potreban ali **nije dovoljan uslov**.
  - Postoje i drugi (skraćeni) tipovi napada.
  - Problem: teško (gotovo nemoguće) je za konkretan sistem dokazati da je imun na ove vrste napada.
  - To čini kriptografiju izazovnom ...
- NAPOMENA: Istorija šifara je vekovna borba između kriptografa i kriptoanalitičara.
  - Ova trka u intelektualnom naoružavanju bitno je uticala na tok istorije!

Ostali napadi

- **Samo šifrat** (engl. *ciphertext-only attack*).
  - Kriptoanalitičar ima samo šifrate nekoliko poruka šifrovanih pomoću istog algoritma.
  - Najmoćniji kriptoanalitički napad, budući da zahteva samo pasivnog napadača u cilju dobijanja šifrata.
  - Znanje o otvorenom tekstu je minimalno i sastoji se od opštih znanja o statistici jednog jezika ili podjezika.
  - Primer uspešnog dešifrovanja ovom metodom su sve šifre proste zamene.
- **Poznat otvoreni tekst** (engl. *known-plaintext attack*).
  - Kriptoanalitičar ima šifrat neke poruke i njemu odgovarajući otvoreni tekst.
  - Cilj je da se na osnovu ove informacije ili dodje do tajnog ključa ili izvršiti dešifrovanje ostatka ili dela šifrata.
  - Ovaj scenario je vrlo realan, budući da je teško sprečiti kriptoanalitičara da pretpostavi neke delove otvorenog teksta (metod verovatne reči, kontekst komuniciranja).

Ostali napadi

- **Odabran otvoreni tekst** (engl. *chosen-plaintext attack*).
  - Kriptoanalitičar je dobio privremeni pristup alatu za šifrovanje, tako da može dobiti šifrat odabranog otvorenog teksta.
  - U ovom scenariju se predpostavlja da kriptoanalitičar može da šifruje otvoreni tekst po sopstvenom izboru.
  - Realni scenariji:
    - Zarobljavanje šifarskog uredjeja sa napunjenim tajnim ključevima, do kojih se ne može doći fizički.
    - Slanje izabranog otvorenog teksta vlasniku šifarskog sistema, koji zatim šifruje istu poruku trećoj strani.
  - Oba scenarija zahtevaju aktivno učešće napadača i stoga je manje verovatan od prethodnih scenarija.

Ostali napadi

- **Odabrani šifrat** (engl. *chosen-ciphertext attack*).
  - Kriptoanalitičar je dobio pristup alatu za dešifrovanje, tako da može dobiti otvoreni tekst odabranog šifrata.
  - Ovo je tipičan napad na kriptosisteme sa javnim ključem.
  - Ovaj scenario je vrlo sličan prethodnom, sa izabranim otvorenim tekstom, s tom razlikom što u njemu kriptoanalitičar ima mogućnost izbora šifrata za zadati šifarski sistem.
  - Realni scenario:
    - Zarobljavanje šifarskog uredjeja sa napunjenim tajnim ključevima, do kojih se ne može doći fizički, a koji može da radi u režimu dešifrovanja.

Ostali napadi

- **Prilagodljivi odabrani otvoreni tekst** (engl. *adaptive chosen-plaintext*).
  - U ovom slučaju napadač može izabrati sledeći otvoreni tekst na osnovu informacija koje je prikupio u prethodno opisanom načinu dešifrovanja.
  - Ovaj napada zahteva još veću aktivnost kriptoanalitičara, koji aktivno bira naredni otvoreni tekst na osnovu dobijenog rezultata šifrovanja prethodno izabranog otvorenog teksta.
  - U teorijskom smislu je od velikog značaja, budući da se ovaj tip napada može povezati sa oblašću mašinskog učenja.
    - Ako je P otvoreni tekst a $C=f(P, K)$ šifrat, kriptoanalitičar treba da nauči nepoznati parametar K, korišćenjem minimalnog broja upita funkcije $f(P, K)$.
    - Obučavajući skup su parovi (P_i, C_i), $i=1, ...n$.
    - Dobar je onaj šifarski sistem koji se ne može efektivno „naučiti“.

- **NAPOMENA**: izraz kriptoanaliza ponekad se odnosi na pokušaj zaobilaženja sigurnosti kriptografskih algoritama ili protokola, a ne samo kriptografske zaštite!

Sigurnost šifarskog sistema

- Šifarski sistem je **siguran** ako je najbolji poznati napad **potpuna pretraga ključeva**.
- Šifarski sistem je **nesiguran** ako nije otporan na **bilo koji oblik skraćenog napada**.
- Pitanje:
  - Da li nesiguran sistem može biti otporniji na “razbijanje” od sigurnog sistema sa malim prostorom ključeva?
- Siguran sistem mora imati dovoljno veliki prostor ključeva!

Sigurnost šifarskog sistema

- Zašto se sigurnost definiše na ovakav način?
- Veličina prostora ključa je **polazna osnova za pretpostavku o stepenu sigurnosti**.
- Ukoliko napad zahteva manje posla od potpune pretrage ključeva onda je pretpostavka loša!
- Sigurnost šifarskog sistema nije egzaktna.
  - Zasniva se na pretpostavkama.
- Da li je sistem dovoljno siguran za određenu primenu?
  - Koliko dugo informacija treba da ostane poverljiva (uporediti sa vremenom potpune pretrage)?
  - Cena.
  - ...

Teorijska kriptoanaliza

- Pretpostavimo da šifarski sistem ima ključ dižine 100 bita.
  - Onda je prostor ključa (broj mogućih ključeva) 2^{100}.
- U proseku, za potpunu pretragu Trudi treba da testira $2^{100}/2 = 2^{99}$ ključeva.
- Ako Trudi može da testira 2^{30} ključeva u sekundi …
  - Onda će pronaći pravi ključ za oko $19 \cdot 10^{12}$ godina.

Teorijska kriptoanaliza

- Pretpostavimo da šifarski sistem ima ključ dižine 100 bita.
  - Prostor ključeva je 2^{100}.
- Pretpostavimo da postoji skraćeni napad koji posao pretrage svodi na pretragu 2^{80} ključeva.
- Ako Trudi testira 2^{30} ključeva po sekundi …
  - Pronaći će pravi ključ za 36 miliona godina.
- Bolje nego u prethodnom slučaju ali još uvek nepraktično!

Klasična kriptografija

- Ukratko će biti razmotrene klasične šifre:
  - Šifre transpozicije
  - Šifre zamene
  - *One-time pad*
  - Kodne knjige.
- Zašto baš one?
  - Zbog istorijskog mesta.
  - Da bi se prikazali osnovni principi koji postoje i kod modernih šifara.

Šifre transpozicije

- Međusobno se premeštaju (“skrembluju”) slova otvorenog teksta.
  - Skremblovani tekst je šifrat.
  - **Način premeštanja** je ključ.
- Odgovara Šenonovom principu difuzije (menjanje statistike otvorenog teksta kroz šifrat).
- Ideja ima primenu i kod modernih šifara.
- NAPOMENA:
  - Kod poruka koje su kratke primena transpozicije nema smisla.
    - Na primer, ABC može da se ispremešta samo na 3!=6 načina.
  - Kod samo malo dužih poruka broj premeštanja (permutacija) je ogroman.
    - Na primer, za poruku dužine 35 slova broj permutacija je 35!
    - To je ogromno vreme za napad potpunom pretragom.

Skitala (*Scytale*)

- Koristili Spartanci (500 god. PNE).
- Obaviti traku oko štapa.
- Potom horizontalno napisati poruku.
- Kada se traka odmota, slova su ispremeštana.
- Primer:
  - Poruka: kill king tomorrow midnight
  - Obmotano:

    ```
    k i l l k i n g
    t o m o r r o w
    m i d n i g h t
    ```
  - Šifat: ktmioi lmd lon kri irg noh gwt

Skitala (*Scytale*)

- Bob i Alisa koriste Skitalu za šifrovanje poruke.
- Pitanje: šta je ključ?
  - Ključ je **prečnik štapa**.
- Trudi: “Koliko je teško da se razbije ova šifra bez poznavanja ključa?”
- Neka Alisa i Bob imaju na raspolaganju mnogo štapova različitih prečnika.
  - Koji postupak Trudi treba da primeni za razbijanje šifrata?
  - Može li Trudi da automatizuje pretragu, bez ručne provere?
- Za pametnog kriptoanalitičara koji ima na raspolaganju dovoljan broj štapova različitog prečnika ovo nije težak posao!
- Siktala je predstavnik transpozicione šifre.
- Predstavlja **veoma lošu zaštitu**!

Transpozicija kolona

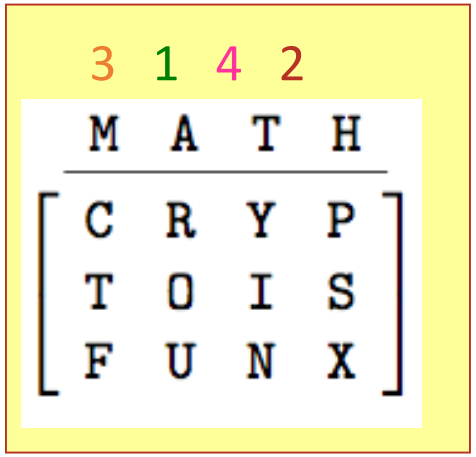
- Odabere se matrica sa željenim brojem kolona.
  - Broj redova zavisi od dužine otvorenog teksta.
  - Upiše se **otovreni tekst u redove matrice**.
- Šifrat se dobija **čitanjem kolona**.
- Primer:
  - Matrica dimenzija 3 x 4
  - Otvoreni tekst: SEETHELIGHT
  - Šifrat: SHGEEHELTTIX

$$\begin{bmatrix} S & E & E & T \\ H & E & L & I \\ G & H & T & X \end{bmatrix}$$

- Efekat je isti kao da se koristi Skitala.
- NAPOMENA: Ukoliko dužina otvorenog teksta nije dovoljna da se popuni matrica, dopunjava se odabranim znakom (X).
- Ključ je **broj kolona** (dimenzija matrice).
  - Broj redova se dobija kada se dužina šifrata podeli sa brojem kolona.
- Napad: probati sa matricama koje imaju S kolona, gde je S broj kojim je deljiva dužina šifrata.

Transpozicija kolona pomoću ključne reči

- Unapređenje transpozicije kolona.
- **Ključna reč određuje redosled transpozicije**.
- Primer:
  - Otvoreni tekst: CRYPTOISFUN
  - Matrica 3 x 4
  - Ključna reč MATH se tumači po abecednom redosledu kao 3 1 4 2
  - Šifrat: ROUPSXCTFYIN
- Šta je ključ?
  - Ključ je **ključna reč**, ali i **dimenzije matrice**.
  - Potrebna je ključna reč sa brojem slova koliko ima kolona.
  - Ukoliko se pojave ista slova unutar ključne reči, ona se izbacuju.
- Koliki je prostor ključeva?



Transpozicija kolona pomoću ključne reči

- Neka Trudi ima na raspolaganju šifrat:
  VOESA IVENE MRTNL EANGE WTNIM HTMLL ADLTR NISHO DWOEH
- Šta Trudi može da uradi?
- Matrica je dimenzija $n \cdot m$ za neko n i m.
- Šifrat ima 45 slova, $n \cdot m = 45$
- Koliko je mogućih rešenja?
  - Matrice dimenzija: $9 \cdot 5$, $5 \cdot 9$, $3 \cdot 15$ ili $15 \cdot 3$.
- Kako će Trudi znati da je na pravom putu?

Transpozicija kolona pomoću ključne reči

- Ako se odabere matrica 9 x 5, onda …

0	1	2	3	4
V	E	G	M	I
O	M	E	E	S
E	R	W	E	H
S	T	T	A	O
A	N	N	D	D
I	L	I	L	W
V	E	M	T	O
E	A	H	R	E
N	N	T	N	H

2	4	0	1	3
G	I	V	E	M
E	S	O	M	E
W	H	E	R	E
T	O	S	T	A
N	D	A	N	D
I	W	I	L	L
M	O	V	E	T
H	E	E	A	R
T	H	N	N	N

- Da li se iz prvog reda može dobiti **smislena reč**?
  - Traže se permutacije samo prvog reda!
  - Ako se može dobiti smislena reč pokuša se sa premeštanjem kolona po tom redosledu.
  - Ako se ovde ne dođe do rezultata bira se nova dimnzija matrice.

Dvostruka transpozicija

- Dalja poboljšanja...
- Otvoreni tekst: ATTACK AT DAWN
- Ključ:
  - Dimenzije matrice: 5 x 3
  - Permutacije (2,4,0,3,1) i (0,2,1).

Kolone	0	1	2
Red 0	A	T	T
Red 1	A	C	K
Red 2	X	A	T
Red 3	X	D	A
Red 4	W	N	X

Permutacije redova i kolona

Kolone	0	2	1
Red 0	X	T	A
Red 1	W	X	N
Red 2	A	T	T
Red 3	X	A	D
Red 4	A	K	C

- Šifrat: XTAWXNATTXADAKC

Dvostruka transpozicija

- Neka Trudi ima šifrat od 45 slova.
- Koliko ima **potencijalnih ključeva**?
- Matrice dimenzija: $3 \cdot 15$, $15 \cdot 3$, $5 \cdot 9$ ili $9 \cdot 5$.
- **Mnogo mogućih permutacija**:
  - $5! \cdot 9! > 2^{25}$
  - $3! \cdot 15! > 2^{42}$
- Prostor ključa je veći od 2^{42} (približno 10^{12})
- Postoji li skraćeni napad?

Dvostruka transpozicija

- Skraćeni napad na dvostruku transpoziciju?
- Neka je šifrat:
  ILILWEAHREOMEESANNDDVEGMIERWEHVEMTOSTTAONNTNH
- Neka je Trudi pogodila dimenzije matrice: $9 \cdot 5$.
- Šta dalje?
  - Da proba sve permutacije?
  - $5! \cdot 9! > 2^{25}$
- Postoji li lakši put?

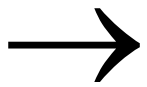
Kolone	0	1	2	3	4
Red 0	I	L	I	L	W
Red 1	E	A	H	R	E
Red 2	O	M	E	E	S
Red 3	A	N	N	D	D
Red 4	V	E	G	M	I
Red 5	E	R	W	E	H
Red 6	V	E	M	T	O
Red 7	S	T	T	A	O
Red 8	N	N	T	N	H

Dvostruka transpozicija

- Trudi pokušava da prvo pogodi permutacije kolona (traži **smislenu reč u redu 0**).

Kolone	0	1	2	3	4
Red 0	I	L	I	L	W
Red 1	E	A	H	R	E
Red 2	O	M	E	E	S
Red 3	A	N	N	D	D
Red 4	V	E	G	M	I
Red 5	E	R	W	E	H
Red 6	V	E	M	T	O
Red 7	S	T	T	A	O
Red 8	N	N	T	N	H

Permutuje kolone



Kolone	2	4	0	1	3
Red 0	I	W	I	L	L
Red 1	H	E	E	A	R
Red 2	E	S	O	M	E
Red 3	N	D	A	N	D
Red 4	G	I	V	E	M
Red 5	W	H	E	R	E
Red 6	M	O	V	E	T
Red 7	T	O	S	T	A
Red 8	T	H	N	N	N

- Šta dalje?
  - Preostaje da se **slože redovi**. Posao nije lak ali je rešiv.

Šifre zamene (supstitucije)

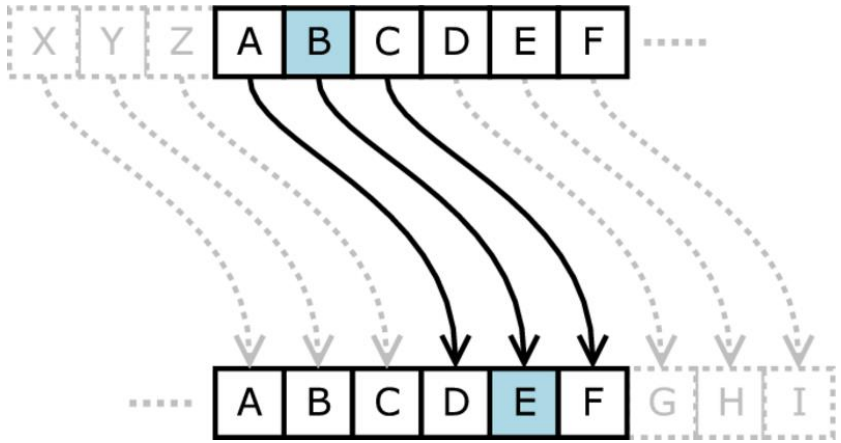
- Kod šifara zamene jedno slovo (simbol) otvorenog teksta se zamenjuje sa nekim drugim slovom (simbolom).
  - Na taj način se dobija šifrat.
  - Ključ: **pravilo zamene**.
- Ovaj pristup odgovara Šenonovom principu **konfuzije** (složena relacija između otvorenog teksta i šifrata).
- Ova ideja se koristi i kod savremenih šifarskih sistema.
- NAPOMENA: Kama sutra (4 vek).
  - Od ukupno 64 veština, 45. veština koja se preporučuje ženama je veština tajnog pisanja (primena supstitucije) za sakrivanje ljubavnih veza.
  - Ostale veštine su kuvanje, bajanje, bacanje čini, …

Šifre zamene (supstitucije)

- Šifre proste zamene (monoalfabetske)
- Homofone
- Poligramske
- Polialfabetske.

Šifre zamene (supstitucije)

- Cezarova šifra je primer šifre zamene.
- Koristio Julije Cezar oko 50-30. godine PNE.
- Šifrat se dobija tako što se svako slovo (otvorenog teksta) od A do W zameni sa slovom koje je za 3 mesta dalje po abecednom redu, a slova X, Y i Z se zameljuju slovima A, B i C.



Cezarova šifra

- Primer:
- Otvoreni tekst: FOURSCOREANDSEVENYEARSAGO
- Ključ za Cezarovu šifru je ciklički pomeraj za 3 mesta.

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
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

- Šifrat: IRXUVFRUHDAGVHYHABHDUVDIR

Cezarova šifra

- Primer.
- Šifrat: VSRQJHEREVTXDUHSDQWU
- Ključ za Cezarovu šifru je ciklički pomeraj za 3 mesta.

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
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

- Otvoreni tekst: SPONGEBOBSQUAREPANTS

Cezarova šifra (formalno)

- Svakom od 26 slova se može dodeliti broj od 0 do 25
- A je 0, B je 1, C je 2, ..., X je 25.
- **Algoritam šifrovanja**:
  - $c_i = p_i + K_E \pmod{26}$, gde je:
    - p_i je i-to slovo otvorenog teksta
    - c_i je i-to slovo šifrata
    - K_E je ključ (pomeraj), u ovom slučaju 3.
- Ako se šifruje slovo X, onda je $p_i = 25$:
  - $c_i = 25 + 3 \pmod{26} = 28 \pmod{26} = 2$.
  - Dakle, slovo X se šifruje kao slovo C.
- **Algoritam dešifrovanja**:
  - $p_i = c_i + (26 - K_E) \pmod{26}$.
- Ako se šifruje slovo C, onda je $c_i = 2$:
  - $p_i = 2 + (26 - 3) \pmod{26} = 25 \pmod{26} = 25$.

Analiza Cezarove šifre

- Ključevi šifrovanja i dešifrovanja su isti ali su algoritmi “različiti”.
  - Šifrovanje: pomeraj u levo za 3.
  - Dešifrovanje: pomeraj u desno za 3.
- Cezarova šifra je **veoma slaba**.
- Šta treba izmeniti?
  - Potrebna je šifra zamene koja ima veliki prostor ključeva.
  - Generalizacija Cezarove šifre …

Opšti oblik šifre proste zamene

- Ključ ne mora biti pomeraj već može da bude bilo koja **permutacija slova**.
- Prostor ključa (engleski jezik) = broj permutacija od 26 slova.
- $26! > 2^{88} \approx 4 \cdot 10^{26}$ različitih ključeva.
- Primer:

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

- Kako Bobu dostaviti **informaciju o ključu**?
  - Ključ je složen, ne može se lako upamtiti.
  - Bob treba da usaglasi ključ sa Alisom a ključ se ne može poslati nesigurnim kanalom!
  - Odabira se ključna reč ili rečenica, ona se postavlja na početak druge kolone (ista slova se izbacuju) a ostatak druge kolone se popunjava preostalim slovima koja nisu iskorišćena i to redom.

Kriptoanaliza proste zamene

- Trudi zna da je primenjena prosta zamena
- Može li pronaći ključ za dati šifrat:

  PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWL
  EQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLX
  GDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPB
  QWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQ
  OTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHI
  LTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

Kriptoanaliza proste zamene

- Nije moguće probati svih 2^{88} ključeva.
- Postoji li skraćeni napad?
- Statistika!
  - Statističaka struktura engleskog jezika.
  - Meri se frekvencija pojavljivanja pojedinih slova u šifratu:

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
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6

  - Poređenjem dobijenih frekvencija sa statističkim (očekivanim) određuje se koje slovo je sa kojim zamenjeno.
- Nije uvek jednostavno:
  - Potrebno je znati jezik, tip teksta (matematika, diplomatija,....)
  - Kriptolozi su uvodili razne zamke.
    - Primer: oni koji su unosili otvoreni tekst namerno su pogrešno pisali i slično.

Homofono šifrovanje

- Unapređenje šifre proste zamene.
- Šifrat sadrži više od 26 znakova (otvoreni tekst je iz skupa 26 slova).
  - Većina slova iz otvorenog teksta se u šifratu zamenjuju **jednoznačno** (kao i u prethodnim primerima)
  - Neka slova otvorenog teksta mogu da u šifratu budu predstavljena na **dva ili više načina**.
- Dodatni znakovi služe za **uvođenje elemenata slučajnosti**.

Homofono šifrovanje

- Primer.
  - Svako slovo otvorenog teksta šifrovati brojevima počev od 00, 01, ... do 31 (5 više)
  - Svaki broj u šifratu jednoznačno određuje slovo otvorenog teksta.
  - Slova otvorenog teksta A, E, N, O, R i T mogu da budu šifrovana na dva načina (dva broja).

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
01	07	14	21	04	13	17	20	29	31	06	28	12	30	17	00

N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
18	26	19	09	10	25	23	02	08	24	22	05	16	15	11	03

Homofono šifrovanje

- Primer.

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
01	07	14	21	04	13	17	20	29	31	06	28	12	30	17	00

N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
18	26	19	09	10	25	23	02	08	24	22	05	16	15	11	03

  - Otvoreni tekst: **TEETN** (ponovljena slova E i T)
  - Šifrat: **24 27 13 08 3**
- Pravilo izbora ”nekih” slova?
- Pravilo kada dodeliti koju od dve vrednosti za isto slovo otvorenog teksta?
- Ovakvi sistemi su otporniji na statističke napade.
- Ipak, ostaju ranjivi na napade poznatog (dela) otvorenog teksta.

Neke napomene o statističkoj analizi

- Statističkom analizom se može doći do informacija o ključu.
- Šifrat bi trebalo da prikrije statističke osobine otvorenog teksta.
- To znači da šifrat treba da ima **osobine slučajnog niza**.
  - Postizanje slučajnosti je često **veoma složen posao**.
  - Teško je **precizno definisati slučajnost** (entropiju).
- Kriptografi ulažu velike napore da se uspešno nose sa napadima zasnovanim na statistici.

Poligramske šifre

- Otvoreni tekst se podeli na blokove (skupove) simbola i **svaki blok se šifruje kao jedna celina**.
- Primer: ”ABA” se šifruje sa ”RTQ”, ”ABB” se šifruje sa ”SLL” ...
- Predstavnici:
  - Playfair šifra
    - Pronađena 1854.
    - Britanci su je koristili u I svetskom ratu
    - Šifruje parove slova (bigrame) zajedno.
  - Hilova šifra.

Klasična kriptografija

- **Playfairova** šifra je polialfabetska i poligramska, što znači da operaciju šifrovanja obavlja nad parovima slova i to tako da rezultat zavisi i od jednog i od drugog slova.
- Ključ Playfairove šifre je matrica koja se formira na osnovu ključne reči.
  - Ukoliko se koristi engleski alfabet, matrica je veličine 5x5 elemenata.
  - Konstrukcija matrice: u polja počev od prvog reda prve kolone upisuje se ključna reč (pri čemu se slova koja su već upisana ne ponavljaju) a zatim ostatak alfabeta.
  - Engleski alfabet ima 26 slova, matrica 25 elemenata: po dogovoru se „I“ i „J“ poistovećuju.
  - Primer: ključna reč „KRIPTOGRAFIJA“.

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

Klasična kriptografija

- Poruka koja se šifruje deli se na parove slova.
- Poruka se šifruje zamenom parova slova otvorenog teksta na osnovu ključa.
  - Slova koja se nalaze u istom redu menjaju se slovima koja se nalaze jedno mesto u desno (ciklički): GF → AB, EL → HC;
  - Slova koja se nalaze u istoj koloni menjaju se slovima koja se nalaze jedno mesto ispod (ciklički): AQ → EX, DW → NR;
  - U suprotnom, slova formiraju pravougaonik u matrici i zamenjuju se slovima koja se nalaze u preostala dva ugla tog pravougaonika: GY → FW, PN → RS.

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

Klasična kriptografija

- Primer: „MOJA PORUKA“
  - Deli se na parove „MO JA PO RU KA“.
  - Nakon šifrovanja dobijaju se sledeći parovi slova: „VC AE KF TN IO“.
- Napomene:
  - U slučaju da se u otvorenom tekstu nalazi par za šifrovanje koji čine ista slova, između njih se po dogovoru ubacuje slovo X.
  - U sličaju da je broj slova neparan, poslednji par se formira dodavanjem slova A. Na primer, reč „MITTWOCH“ se pre šifrovanja deli na parove „MI TX TW OC HA“.

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

Hilova šifra

- Pronašao je Lester Hill 1929. godine.
- Preteča je savremenih blok šifri.
- Osnovna idjea: šifra zamene sa velikim ”alfabetom”.
- Koristi jednostavne linearne jednačine.
- Trebalo bi da bude unapređenje šifre proste zamene.

Hilova šifra

- Obeležimo otvoreni tekst sa: p_0, p_1, p_2, …
  - p_i predstavlja blok (niz) od n uzastopnih slova
  - Svako p_i se zapisuje u jednoj koloni matrice
- Neka je ključ je A matrica dimenzija n x n
- Imamo 26^n mogućih ključeva.
- Matrica A mora biti **invertibilna**.
  - Šifovanje: $c_i = A\ p_i \pmod{26}$
  - Dešifrovanje: $p_i = A^{-1} c_i \pmod{26}$

Hilova šifra

- Primer.
- Otvoreni tekst: MEETMEHERE = (12, 4, 4, 19, 12, 4, 7, 4, 17, 4).

$$A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$$

- Pošto je matrica veličine 2 x 2:

$$p_0 = \begin{bmatrix} 12 \\ 4 \end{bmatrix},\ p_1 = \begin{bmatrix} 4 \\ 19 \end{bmatrix},\ p_2 = \begin{bmatrix} 12 \\ 4 \end{bmatrix}, p_3 = \begin{bmatrix} 7 \\ 4 \end{bmatrix},\ p_4 = \begin{bmatrix} 17 \\ 4 \end{bmatrix}$$

$$c_0 = \begin{bmatrix} 4 \\ 22 \end{bmatrix},\ c_1 = \begin{bmatrix} 23 \\ 9 \end{bmatrix},\ c_2 = \begin{bmatrix} 4 \\ 22 \end{bmatrix},\ c_3 = \begin{bmatrix} 24 \\ 19 \end{bmatrix},\ c_4 = \begin{bmatrix} 10 \\ 25 \end{bmatrix}$$

- Šifrat: (4,22,23,9,4,22,24,19,10,25) = EWXJEWYTKZ

Polialfabetske šifre

- Slične šiframa proste zamene, ali postoji više alfabeta koji se koriste za šifrovanje.
- Može se primeniti novi alfabet za svako slovo.
- Velika primena kod klasičnih šifarskih sistema.
- Primer je Vižnerova šifra.
- Korišćena u II svetskom ratu.

Vigenèreova šifra

- **Vigenèreova šifra** je polialfabetska, što znači da se svako slovo otvorenog teksta može preslikati u jedno od *m* mogućih slova, gde je *m* dužina ključa.
  - Neka je: *n* broj slova u alfabetu, $k = (k_1, k_2, \ldots, k_m)$ ključ dužine *m*, $x = (x_1, x_2, \ldots, x_m)$ deo otvorenog teksta dužine *m*, $y = (y_1, y_2, \ldots, y_m)$ deo šifrata dužine *m*.
  - Operacije šifrovanja i dešifrovanja date su sa:
    - $E(x, k) = x_1 + k_1 \pmod n, x_2 + k_2 \pmod n, \ldots x_m + k_m \pmod n$
    - $D(y, k) = y_1 - k_1 \pmod n, y_2 - k_2 \pmod n, \ldots y_m - k_m \pmod n$.
- Primer:

Otv. tekst	D	U	S	K	**O**	D	U	G	**O**	U	S	K	**O**
Ključ	K	O	J	O	**T**	K	O	J	**O**	T	K	O	**J**
Šifrat	N	I	B	Y	**H**	N	I	P	**C**	N	C	Y	**X**

- Prostor ključeva: $n^1 + n^2 + \ldots + n^m$, gde je *n* broj slova u alfabetu, a *m* najveća dužina ključa.
  - Primer za za n=26, k=5 treba ispitati 12.356.630 ključeva

Savršena sigurnost

- Šifarski sistem je **računski siguran** (engl. *computationally secure*) ako:
  - Cena ”razbijanja” šifrata prevazilazi vrednost šifrovane informacije.
  - Vreme potrebno za ”razbijanje šifrata” je duže od vremena u kom informacija treba da bude tajna.
- Šifarski sistem je **bezuslovno siguran** ako ne može da bude ”razbijen” ni uz primenu neograničenih računarskih resursa.
- Šifre koje su prethodno pominjane imaju slabosti – ”razbijene” su.
  - Neke od njih su bile ”sigurne” u jednom delu vremena kada su korišćene.
  - Čekalo se na razvoj nauke, tehnologije, itd.
- **Bezuslovno sigurna šifra**:
  - Ne može se doći do otvorenog teksta iz šifrata bez poznavanja ključa, čak ni potpunom pretragom ključeva.
  - Potpuna pretraga ne pomaže jer su svi mogući otvoreni tekstovi jednako verovatni.

One-time Pad (OTP)

- Operacija ekskluzivno ILI (*eXclusive OR*, *XOR*) definisana je jednačinama:
  - $0 \oplus 0 = 1 \oplus 1 = 0$.
  - $0 \oplus 1 = 1 \oplus 0 = 1$.
- Šifrovanje zasnovano na ovoj logičkoj operaciji oslanja se na njenu osobinu:
  - $(A \oplus B) \oplus B = A$.
- Šifrovanje: $c_i = p_i \oplus k_i$
- Dešifrovanje: $p_i = c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i$

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

$$a \oplus a = 0$$
$$a \oplus 0 = a$$
$$a \oplus 1 = \bar{a}$$
$$a \oplus b \oplus b = a$$

One-time Pad (OTP)

- Gilbert Vernam i Joseph Mauborgne 1917.
- Šifra sa jednokratnim ključem.
- Postoji **matematički dokaz o savršenoj sigurnosti šifre**!
  - Ni jedna druga šifra koja će biti razmatrana nema ovu osobinu.
- Zašto se onda ne koristi samo ona?
  - Veoma je **nepraktična** za opštu primenu.
- Ima veliku primenu za najviše nivoe sigurnosti.

One-time Pad (OTP)

- Pretpostavimo da imamo alfabet od 8 slova: (e, h, i, k, l, r, s, t)
- Svakom slovu se može dodeliti odgovarajući binarni kod:
  - e = 000, h = 001, i = 010, k = 011, …, t = 111
  - Kod nije tajna (može biti ASCII, ...)
- Neka je Alisa špijun i treba da šifruje poruku: heilhitler
  - Prvo poruku predstavlja binarnim nizom.
  - Potreban je ključ (neki drugi binarni niz) iste dužine kao i poruka.

One-time Pad (OTP)

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Šifrovanje: otv. tekst ⊕ ključ = šifrat

	h	e	i	l	h	i	t	l	e	r
Otv. tekst:	001	000	010	100	001	010	111	100	000	101
Ključ:	111	101	110	101	111	100	000	101	110	000
Šifrat:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

One-time Pad (OTP)

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Dešifrovanje: šifrat ⊕ ključ = otv. tekst

	s	r	l	h	s	s	t	h	s	r
Šifrat:	110	101	100	001	110	110	111	001	110	101
Ključ:	111	101	110	101	111	100	000	101	110	000
Otv. tekst:	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

One-time Pad (OTP)

- Dvostruki agent tvrdi da je korišćen “ključ”

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Dešifrovanje: šifrat ⊕ ključ = otv. tekst

	s	r	l	h	s	s	t	h	s	r
Šifrat:	110	101	100	001	110	110	111	001	110	101
“Ključ”:	101	111	000	101	111	100	000	101	110	000
Otv. tekst:	011	010	100	100	001	010	111	100	000	101
	k	**i**	**l**	**l**	h	i	t	l	e	r

One-time Pad (OTP)

- Pošiljalac je uhapšen i on tvrdi da je korišćen “ključ”

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Dešifrovanje: šifrat ⊕ ključ = otv. tekst

	s	r	l	h	s	s	t	h	s	r
Šifrat:	110	101	100	001	110	110	111	001	110	101
“Ključ”:	111	101	000	011	101	110	001	011	101	101
Otv. tekst:	001	000	100	010	011	000	110	010	011	000
	h	e	i	l	**k**	**e**	**s**	**i**	**k**	**e**

One-time Pad (OTP)

- Kako možemo tvrditi da OTP ne može da se “razbije”?
- Sigurnost se zasniva na slučajnosti ključa!
- Sa kriptografskog stanovišta, zahtevaju se dva osnovna svojstva binarnog slučajnog ključa:
  - **Nepredvidivost**.
    - Nezavisno od broja bita (ključa) koji su poznati, verovatnoća pogađanja sledećeg bita nije veća od ½.
    - Verovatnoća da određeni bit bude 1 ili 0 tačno je jednaka ½.
  - **Balansiranost**.
    - Broj 1 i 0 mora biti jednak.
- **Matematički dokaz**.
  - Verovatnoća da bit ključa bude 1 ili 0 je ½.
  - Otvoreni tekst nije balansiran. Neka je verovatnoća pojave nule x, a pojave jedinice 1-x.
  - Verovatnoća da bit šifrata bude 1 ili 0 je (½)x + (½)(1-x) = ½.
  - Šifrat je slučajan niz.

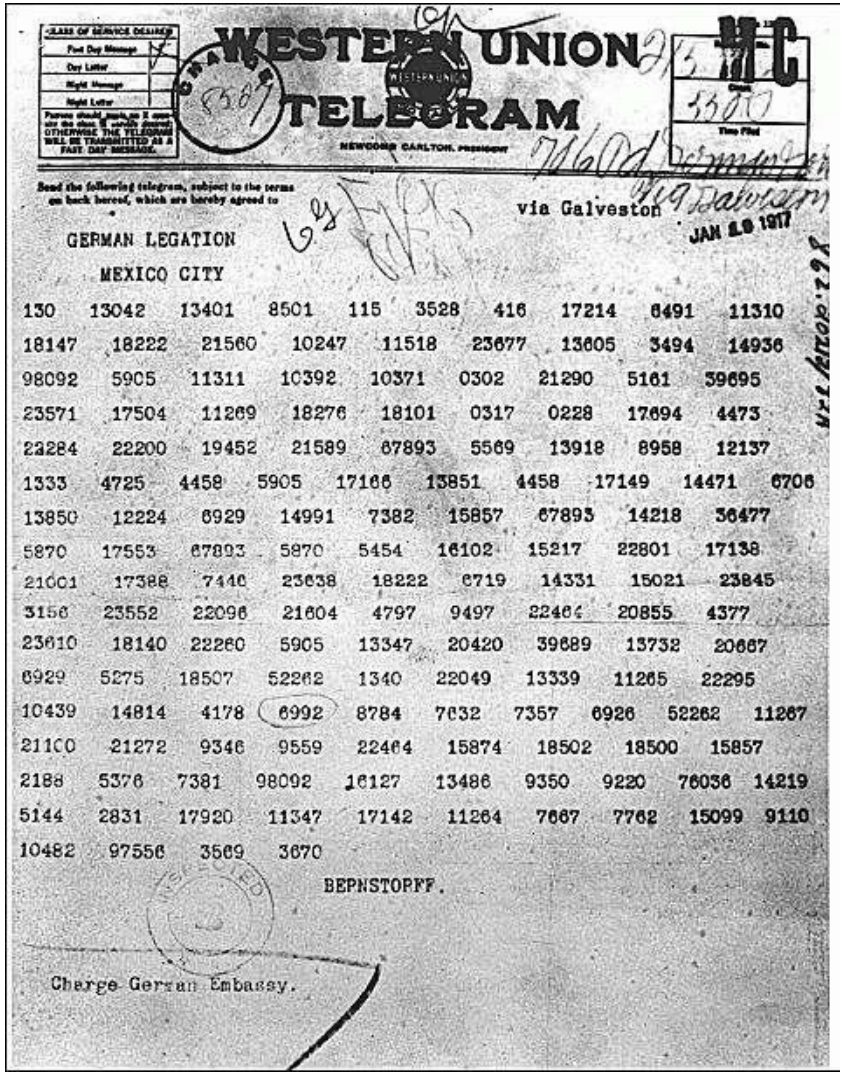
Kodne knjige

- Pojednostavljeno: rečnik koji uparuje reči (fraze) i kodne oznake.
  - Na primer, reč: Februar, kodna oznaka: 13065.
  - Preciznije: 2 kodne knjige, 1 za šifrovanje i 1 za dešifrovanje
- **Ključ je kodna knjiga**!
- Sigurnost šifarskog sistema se zasniva na fizičkoj sigurnosti kodne knjige.
  - Ako jedna kodna knjiga padne u ruke neprijatelju onda se mogu dešifrovati sve prethodne komunikacije koje su šifrovanje zasnivali na toj kodnoj knjizi.
  - U ratnoj situaciji više jedinica koristi kopije kodne knjige.
  - Neophodno je definisati stroge procedure koje u slučaju opasnosti predupređuju da kodna knjiga padne u ruke neprijatelju.
- Neke savremene šifre su zasnovane na ovom principu.

Kodne knjige

- **Cimermanov telegram** je jedna od najpoznatijih kodnih knjiga u istoriji sveta.
- Šifrovan je kodnom knjigom čiji je deo:
  - Februar : 13605
  - Fest : 13732
  - Finanzielle : 13850
  - Folgender : 13918
  - Frieden : 17142
  - Friedenschluss : 17149
  - …
- 1917. nemački ministar spoljnih poslova je pozvao Meksikance da napadnu SAD (I svetski rat).
- SAD su bile neutralne do tog momenta.
- Dešifrovanje telegrama je povod za ulazak SAD u I svetski rat!

Cimermanov telegram



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

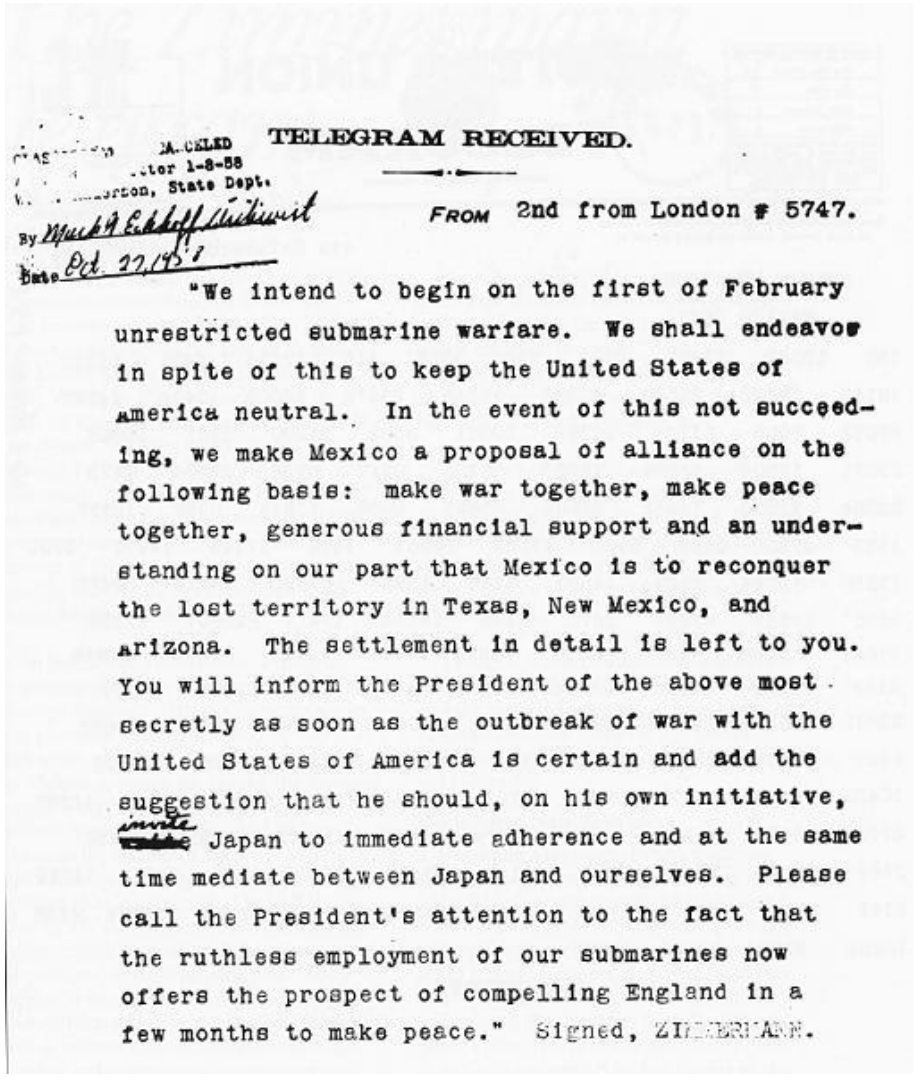
GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3509 3670

BERNSTORFF.

Charge German Embassy.



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Kodne knjige

- Kodne knjige su podložne statističkoj analizi.
  - Slično kao i kod šifara zamene, ali je za napad potrebno mnogo više šifrata.
- U toku II svetskog rata kodne knjige su bile veoma popularne.
  - Međutim, treba uzeti u obzir da je zamena skupa i teško izvodljiva.
- Da bi ostale u upotrebi uvedene su **aditivne kodne knjige**.
  - Aditivna kodna knjiga je dodatna knjiga koja sadrži mnogo "slučajnih" brojeva.
  - Sekvence "slučajnih" brojeva se sabiraju sa kodnim rečima i formiraju konačni šifrat.
  - Početna pozicija iz aditivne knjige treba da se dogovori između pošiljaoca i primaoca.
  - Početno mesto u kodnoj knjizi, određuje pošiljalac i šalje se nezaštićeno uz šifrat.
    - **Indikator poruke** (engl. *message indicator*, MI).
    - To su informacije (osim ključa) potrebne za dešifrovanje.
    - Savremeni izraz: inicijalizacioni vektor (engl. *initialization vector*, IV).
  - Kako ovaj postupak povećava sigirnost kodne knjige?
    - Ako se MI koristi samo jednom, šifra postaje One-time Pad.

Literatura

1. M. Stamp: *Information Security*. John Wiley and Sons.
2. M. Veinović, S. Adamović: Kriptologija 1. Univerzitet Singidunum, Beograd. *
3. M. Milosavljević, S. Adamović: Kriptologija 2. Univerzitet Singidunum, Beograd. *

* Može se besplatno preuzeti sa portala: www.singipedia.com

Hvala na pažnji

Pitanja su dobrodošla.