<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

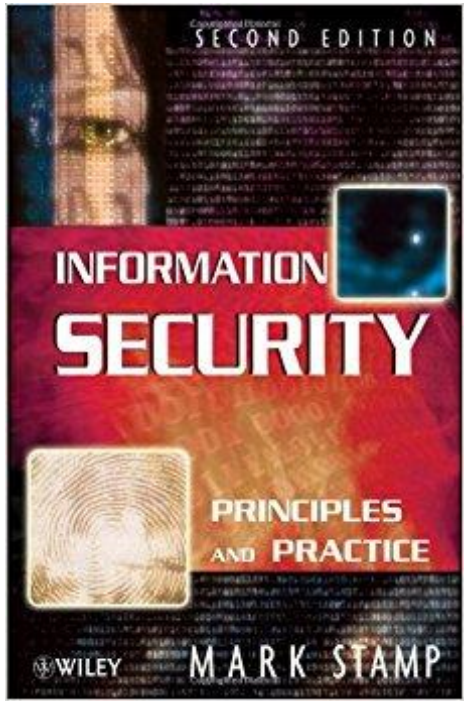
<CISSP> Kriptografija I</CISSP>

Summary

- Osnovni principi
- Metoda jednostavne zamjene
- Kriptoanaliza jednostavne zamjene
- One-Time pad
- Primjeri kroz noviju historiju

Credits

- Primjeri su preuzeti iz prvog poglavlja knjige: Information security (Principles and Practice) - Second edition



Lekcija 1. Osnovni principi

- Uvod
- Terminologija
- Kripto princip
- Osnovni model

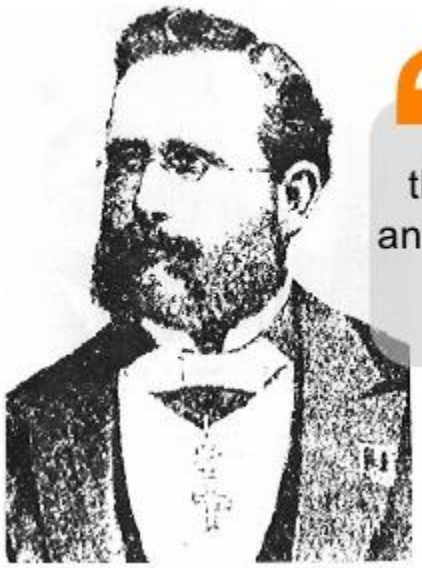
Uvod

- **Kriptologija** - Naučna disciplina kreiranja i razbijanja „tajnih kodova“
  - **Kriptografija** - kreiranje „tajnih kodova“
  - **Kriptoanaliza** - razbijanje „tajnih kodova“
- **Kripto** - sve navedeno (i još mnogo toga)

Terminologija

- Šifra *cipher* ili kriptosistem *cryptosystem* se koriste za enkriptovanje *encrypt* otvorenog teksta *plaintext*
  - Rezultat šifrovanja je šifrovani tekst *ciphertext*
  - Dekriptovanjem *decrypt* šifrovanog teksta se ponovo dobiva otvoreni tekst
- Ključ *key* se korisiti za konfigurisanje kriptosistema
- Kriptosistem simetričnog ključa *symmetric key* koristi isti ključ za enkriptovanje/dekriptovanje
- Kriptosistem javnog ključa *public key* koristi javni ključ za enkriptovanje, a privatni ključ *private key* za dekriptovanje

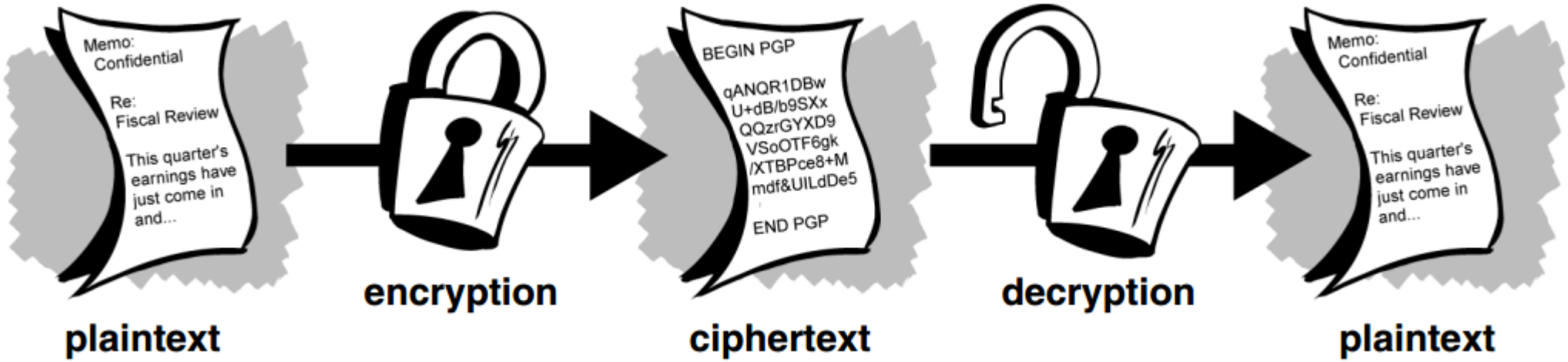
Kripto principi



> the system must not require secrecy and can be stolen by the enemy without causing trouble.
>
> - Auguste Kerckhoff, 1883

- Principi
  - Sistem je potpuno poznat napadaču
  - Samo je ključ tajan
  - Kripto algoritam nije tajan
  - Poznato još kao *Kerckhoff*-ov princip
- Zašto je ovako?
  - Iskustvo je pokazalo da su tajni algoritmi imaju mnogo slabih tačaka
    - Tajni algoritam nikada nije dugo ostao tajan
  - Otvorenost ?
    - Prije će se pronaći slabost i ispraviti

Osnovni model



Lekcija 2. Metoda jednostavne zamjene

- Cezarova šifra
- Broj kombinacija

Cezarova šifra

- Otvoreni tekst: Tajna poruka
- Ključ: **3**

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
Šifrovani tekst:	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

- Šifrovani tekst: WDMQDSRUND
- Međutim, nismo ograničeni samo na jedan ključ

Broj kombinacija

- Pomjeri sve za n koji je iz skupa $n \in \{0,1,2,\ldots,25\}$
- Ključ je n
- Primjer: ključ $n = 7$

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
Šifrovani tekst:	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

Lekcija 3. Kriptoanaliza jednostavne zamjene

- Kriptoanaliza cezarove zaštite
- Šta ako nije „jednostavna“ zamjena?
- Frekvencija ponavljanja znakova
- Primjer
- Zaključak

Kriptoanaliza cezarove zaštite

- Napadač zna da je korištena metoda zamjene
- Zna da je ključ broj „n“
  - Zavisi od broja znakova u specifičnom jeziku
- Šifrovani tekst je: CSYEVIXIVQMREXIH
- Kako da pronađemo ključ?
- Engleski alfabet
  - Imamo samo 26 opcija - moramo ih testirati SVE!
- Bosanski jezik
  - Imamo samo 30 opcija
- U našem primjeru n= 4

Šta ako nije „jednostavna“ zamjena?

- Generalno, ključ može biti bilo koja kombinacija (permutacija) slova.

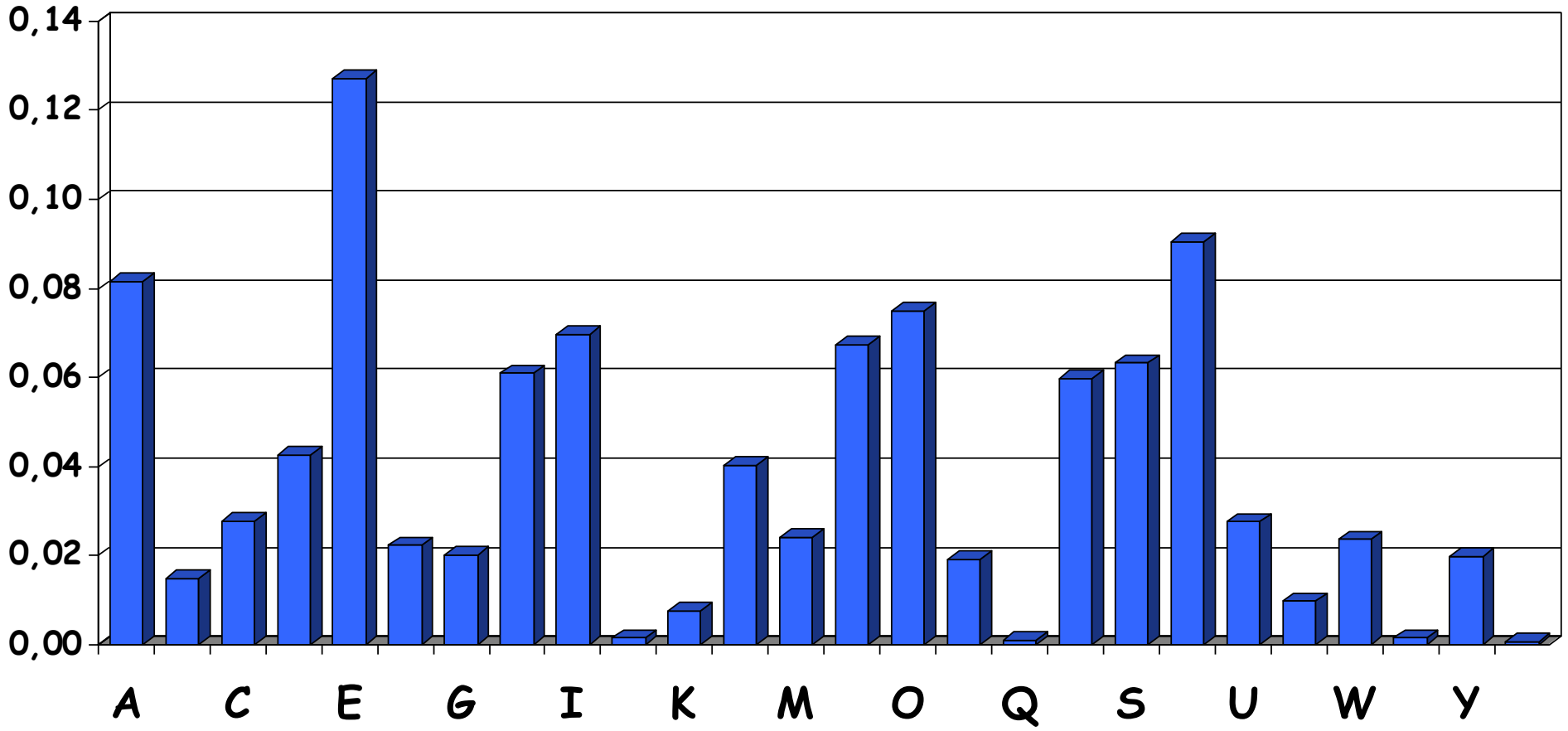
Otvoreni tekst:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrovani tekst:	J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

- Tada imamo 26! > 2^{88} mogućih ključeva

- 403291461126605635584000000

Frekvencija ponavljanja znakova

- Teško je probati svih 2^{88} ključeva
- Frekvencija korištenja slova… (eng. Verzija)



Primjer

- PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVC
  XQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTP
  QWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQ
  UFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHI
  XQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQ
  JHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILT
  TAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

- Pokušajte probiti gore navedeni 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
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	8

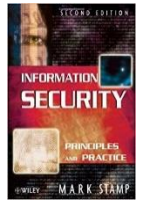
Zaključak

- Kriptosistem je **siguran** ako je najbolji mogući napad kombinacija svih mogućih opcija
  - Brut force
- Kriptosistem **nije siguran** ako postoji bilo koji napad zaobilaznim putem
  - Backdoor

Lekcija 4. One-Time pad

- One-Time pad enkripcija
- One-Time pad i različiti ključevi
- One-Time činjenice

One-Time pad enkripcija



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

Enkripcija: Otvoreni tekst ⊕ Ključ = Šifrovan tekst

Otvoreni tekst:	h	e	i	l	h	i	t	l	e	r
	001	000	010	100	001	010	111	100	000	101
Ključ:	111	101	110	101	111	100	000	101	110	000
	110	101	100	001	110	110	111	001	110	101
Šifrovani tekst:	s	r	l	h	s	s	t	h	s	r

One-Time pad i različiti ključevi

- Recimo da dvostruki agent otkrije „ključ“:

Otvoreni tekst:	s	r	l	h	s	s	t	h	s	r
	110	101	100	001	110	110	111	001	110	101
Ključ:	101	111	000	101	111	100	000	101	110	000
	011	010	100	100	001	010	111	100	000	101
Šifrovani tekst:	k	i	l	l	h	i	t	l	e	r

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

One-Time činjenice

- Dokazano sigurno…
  - Šifrovan tekst nema informacija o otvorenom tekstu
  - Svaki tekst može jednako odgovarati
- …ali samo jedan ima smisao.
  - Pad mora biti slučajan i korišten samo jednom
  - Pad je poznat samo pošiljaocu i primaocu
- Važno: pad (ključ) je iste veličine kao i poruka

Lekcija 5. Primjeri kroz noviju historiju

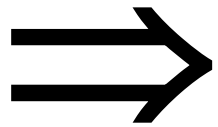
- Dvostruka transpozicija
- Projekat „Venona“
- Šifrovanje putem knjige kodova
- Zimmermanov telegram
- Kriptografija poslije WW II
- Claud Shannon

Dvostruka transpozicija

- Otvoreni tekst: attackxatxdawn

	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

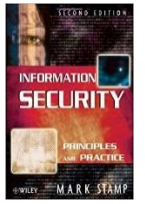
Šifrovano



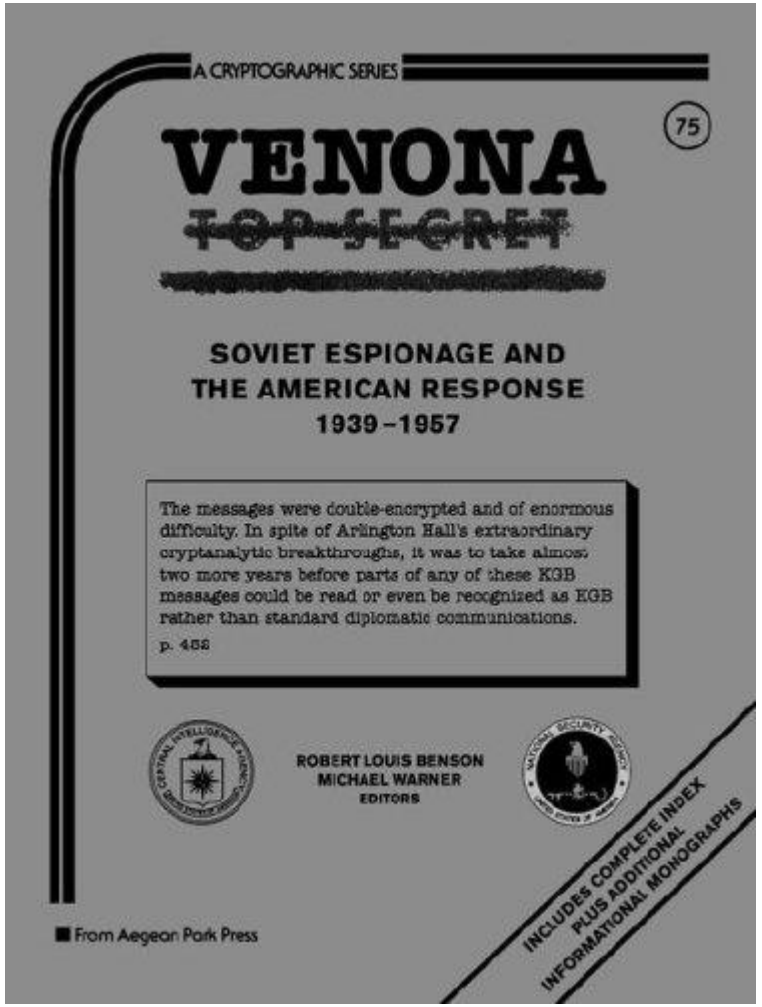
	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

- Šifrovani tekst: xtawxnattxadakc
- Ključ je matrica: (3,5,1,4,2) i (1,3,2)

Projekat „Venona...



- Projekat VENONA
- Enkriptovane poruke špijuna iz USA u SSSR unutar 30tih, 40tih i 50tih
- Nuklearne tajne i sl.
- Špijuni su donijeli one-time pad u USA.
- Ista je korištena za slanje poruka
- Ponavljanjam unutar “one-time” pad-a je omogućena kriptoanaliza



...projekat Venona

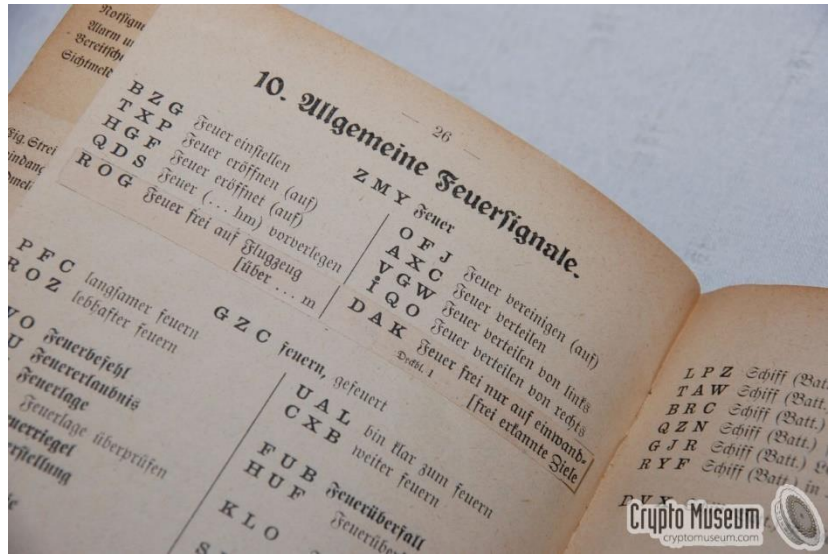
[C% Ruth] learned that her husband [v] was called up by the army but he was not sent to the front. He is a mechanical engineer and is now working at the ENORMOUS [ENORMOZ] [vi] plant in SANTA FE, New Mexico. [45 groups unrecoverable]

detain VOLOK [vii] who is working in a plant on ENORMOUS. He is a FELLOWCOUNTRYMAN [ZEMLYaK] [viii]. Yesterday he learned that they had dismissed him from his work. His active work in progressive organizations in the past was cause of his dismissal. In the FELLOWCOUNTRYMAN line LIBERAL is in touch with CHESTER [ix]. They meet once a month for the payment of dues. CHESTER is interested in whether we are satisfied with the collaboration and whether there are not any misunderstandings. He does not inquire about specific items of work [KONKRETNAYa RABOTA]. In as much as CHESTER knows about the role of LIBERAL's group we beg consent to ask C. through LIBERAL about leads from among people who are working on ENOURMOUS and in other technical fields.

- „Ruth“ == Ruth Greenglass
- „Liberal“ == Julius Rosenberg
- „Enormous“ == the atomic bomb

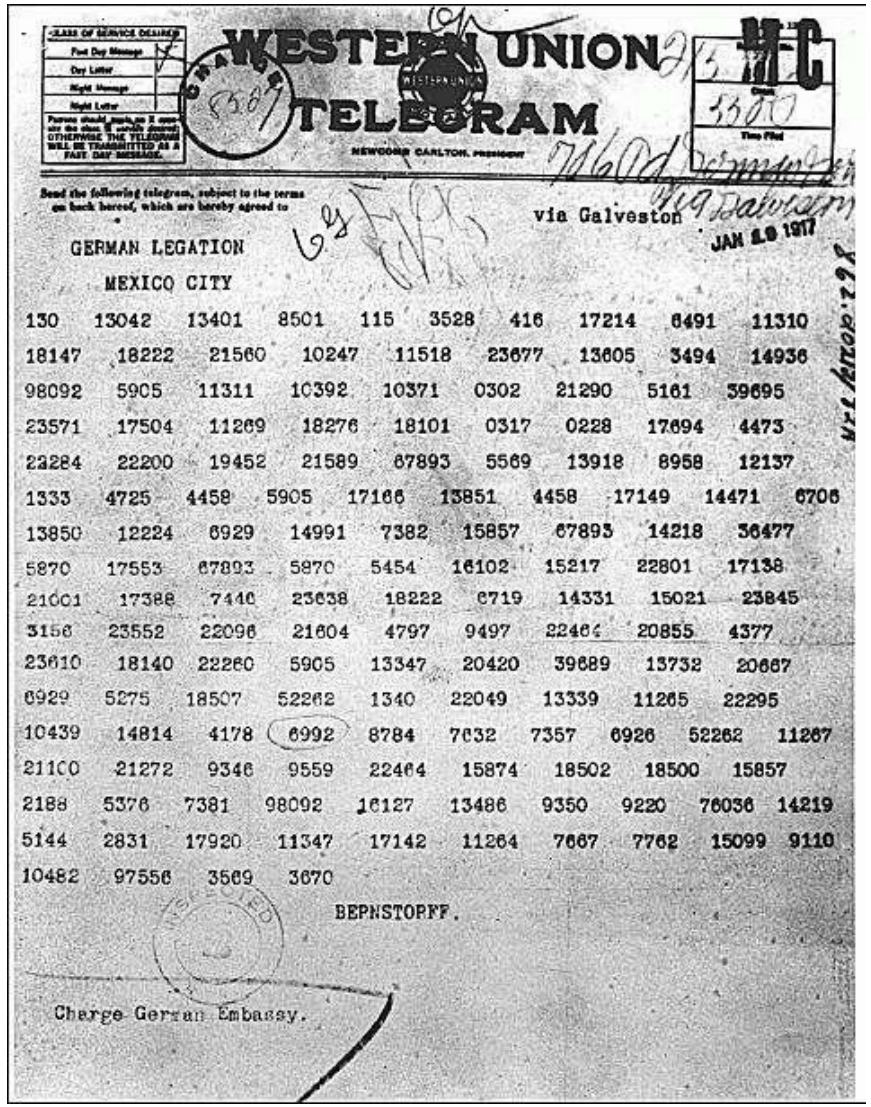
Šifrovanje putem knjige kodova

- Doslovno knjiga kodiranih riječi “codewords”
- Zimmermanov Telegram – poznati primjer
  - fest 13732
  - finanzielle 13850
  - folgender 13918
  - Frieden 17142
  - Friedenschluss 17149



- Moderni sistemi šifrovanja koriste „codebook" princip

Zimmermanov telegram



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

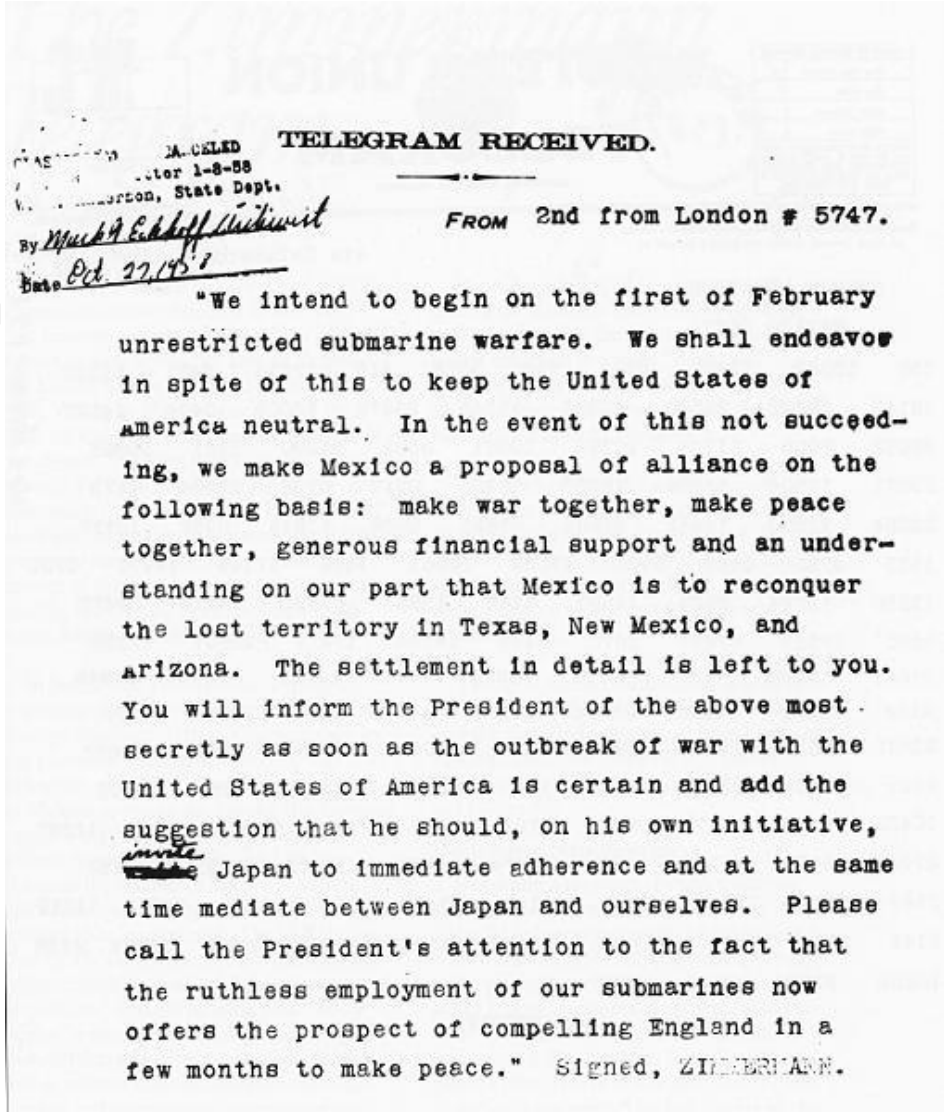
MEXICO CITY

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 3569 3670

BEPNSTORFF.

Charge German Embassy.

- Poznati primjer u historiji
- Glavni faktor ulaska USA u WW I
- Britanci pronašli djelomičnu knjigu kodova
- Logikom su popunjene „praznine



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.

Kriptografija poslije WW II

- Claude Shannon — otac nauke o informacijskoj teoriji
- Digitalizacija— mnogo podataka za zaštiti
- Data Encryption Standard (DES), 70’te
- Public Key kriptografija, 70’te
- CRYPTO konferencije, 80’te
- Advanced Encryption Standard (AES), 90’te

Claude Shannon

- Izumitelj teorije informacija
- 1949
- Fundametalni koncepti
  - **Confusion** - zasjeniti vezu između otvorenog i šifrovanog teksta
  - **Diffusion** - rasuti statistiku iz otvorenog teksta kroz šifrovani tekst
- One-time pad je samo konfuzija, dok je dvostruka transpozicija samo difuzija

Pitanja