Kratek izlet v zgodovino kriptografije

Štefko Miklavič

Univerza na Primorskem
UP FAMNIT in UP IAM

27. september 2013

Gaj Julij Cezar

Gaj Julij Cezar

Gaj Svetonij poroča, da se je Julij Cezar dopisoval s Cicerom tako, da je vsako črko v besedilu nadomestil s črko, ki je v abecedi tri mesta za njo.

Gaj Julij Cezar

Gaj Svetonij poroča, da se je Julij Cezar dopisoval s Cicerom tako, da je vsako črko v besedilu nadomestil s črko, ki je v abecedi tri mesta za njo.

A	B	C	Č	⋯	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓
Č	D	E	F	⋯	A	B	C

Gaj Julij Cezar

Primer

M	A	R	Č	E	V	E	I	D	E
P	Č	T	F	H	A	H	L	G	H

Cezarjeva šifra

Cezarjeva šifra

Vsako črko besedila zamenjamo s črko, ki je v abecedi n mest za zamenjano črko ($1 \leq n \leq 25$).

Varnost Cezarjeve šifra

Pri študiju varnost šifer upoštevamo Kerckhoffov princip:

Nasprotnik pozna algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.

Varnost Cezarjeve šifra

Pri študiju varnost šifer upoštevamo Kerckhoffov princip:

> Nasprotnik pozna algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.

Pri Cezarjevi šifri je samo 25 možnih ključev $\rightarrow$ šifra ni varna.

Substitucijska šifra

Vsako črko abecede zamenjamo z neko drugo črko, ne glede na to, koliko mest za njo je v abecedi.

Substitucijska šifra

Vsako črko abecede zamenjamo z neko drugo črko, ne glede na to, koliko mest za njo je v abecedi.

A	B	C	Č	⋯	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓
M	F	R	Z	⋯	O	Z	H

Varnost substitucijske šifre

Koliko je vseh možnosti, kako lahko to naredimo, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?

Varnost substitucijske šifre

Koliko je vseh možnosti, kako lahko to naredimo, oziroma, koliko je pri substitucijski šifri vseh možnih ključev?

Vseh možnih ključev je

$$25 \cdot 24 \cdot 23 \cdots 3 \cdot 2 \cdot 1 = 25! = 15511210043330985984000000.$$

Varnost substitucijske šifre

Če bi računalnik v eni sekundi lahko preveril milijardo (10^9) možnih ključev, bi rabil

$$\frac{1551121004333098598400000 0}{1000000000} = 1551121004333098 5, 984$$

sekund,

Varnost substitucijske šifre

Če bi računalnik v eni sekundi lahko preveril milijardo (10^9) možnih ključev, bi rabil

$$\frac{1551121004333098598400000}{1000000000} = 1551121004333098 5, 984$$

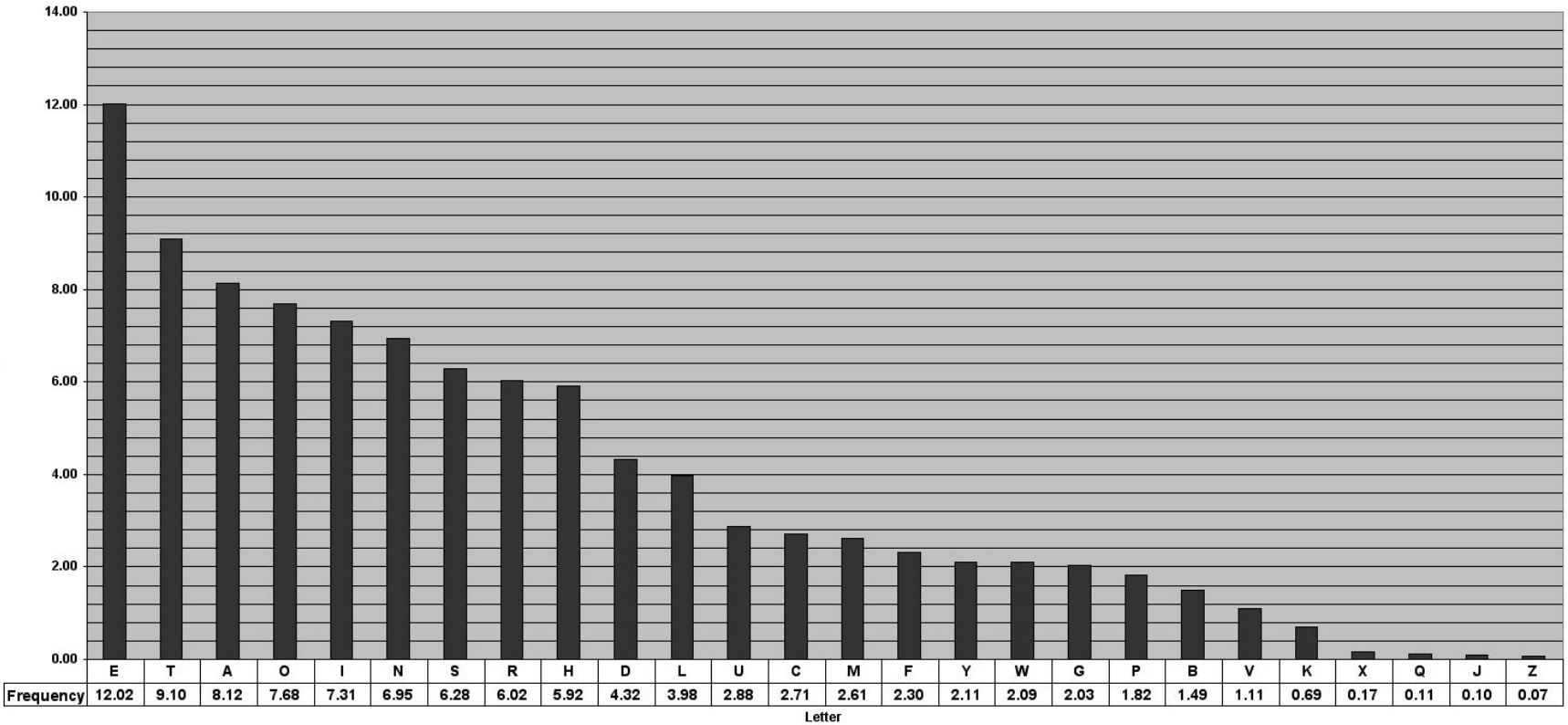
sekund, kar je približno 491857243 let.

Varnost substitucijske šifre

Vendar .....

Varnost substitucijske šifre

Vendar .....



	E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z
Frequency	12.02	9.10	8.12	7.68	7.31	6.95	6.28	6.02	5.92	4.32	3.98	2.88	2.71	2.61	2.30	2.11	2.09	2.03	1.82	1.49	1.11	0.69	0.17	0.11	0.10	0.07

Varnost substitucijske šifre

S pomočjo frekvenčne analize tajnopisa (če ga le imamo dovolj na voljo) lahko hitro razvozlamo substitucijsko šifro.

Vigenerjeva šifra

Blaise de Vigenere, 1523 - 1596

Vigenerjeva šifra

Primer

Tekst: ŽIVE NAJ VSI NARODI KI HREPENE DOČAKAT DAN
Ključ: FRANC

Vigenerjeva šifra

Primer

Tekst: ŽIVE NAJ VSI NARODI KI HREPENE DOČAKAT DAN
Ključ: FRANC

Ž I V E N A J V S I N A R O D I K I H R E P E N E D O Č A K A T D A N
F R A N C F R A N C F R A N C F R A N C F R A N C F R A N C F R A N C
7 18 11 5 3 7 18 11 5 3 7 18 11 5 3 7 18 11 5 3 7 18 11 5 3 7 18 11 5 3 7 18 11 5 3
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
F C Z T R G O R

Varnost Vigenerjeve šifre

Vigenerjeva je dosti časa veljala za nezlomljivo ....

Varnost Vigenerjeve šifre

Vigenerjeva je dosti časa veljala za nezlomljivo ....

.... do leta 1863, ko je nemški oficir Friedrich Kasiski opisal, kako jo lahko zlomimo ...

Varnost Vigenerjeve šifre

$\cdots$	N	A	R	O	D	I	$\cdots$	H	O	D	I
$\cdots$	F	R	A	N	C	F	$\cdots$	A	N	C	F
$\cdots$	7	18	1	15	3	7	$\cdots$	1	15	3	7
$\cdots$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\cdots$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$\cdots$	U	S	S	E	G	P	$\cdots$	I	E	G	P

Varnost Vigenerjeve šifre

Razdalja med “narODI” in “hODI” je 35 mest. Če pravilno domnevamo, da sta bila oba “ODI” zašifrirana z istim ključem, potem je dolžina ključa 1, 5, 7 ali 35.

Varnost Vigenerjeve šifre

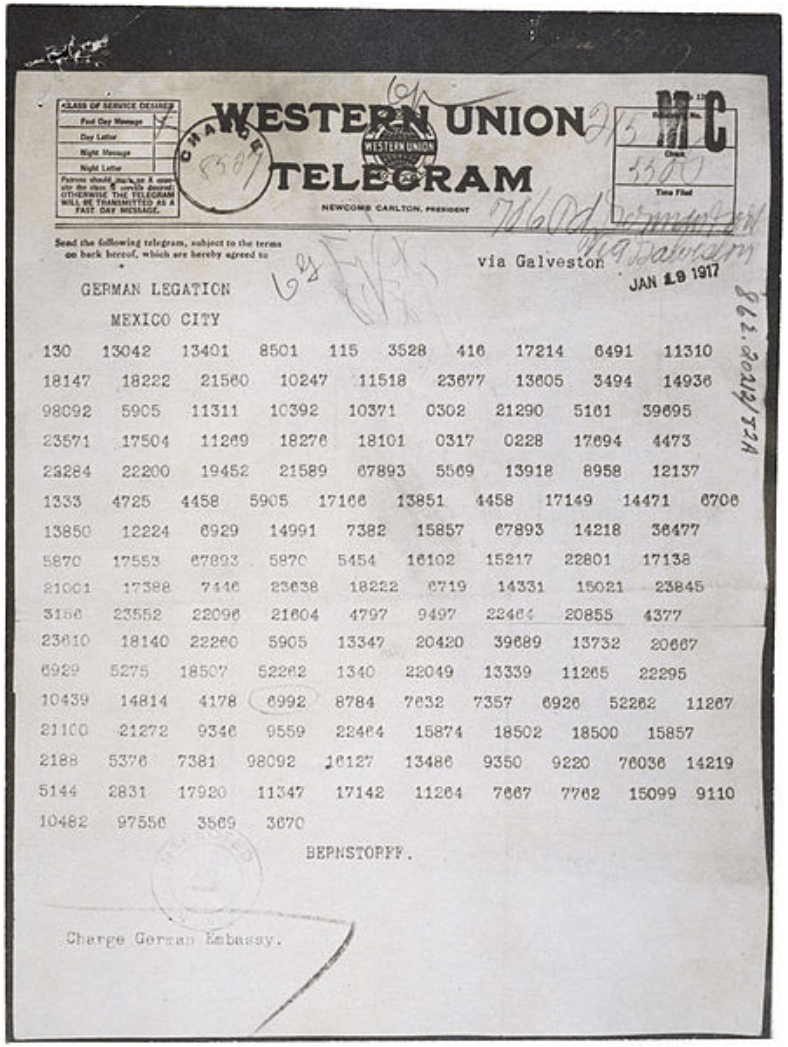
Razdalja med “narODI” in “hODI” je 35 mest. Če pravilno domnevamo, da sta bila oba “ODI” zašifrirana z istim ključem, potem je dolžina ključa 1, 5, 7 ali 35.

Brž ko pa poznamo dolžino ključa, lahko razvozlamo tajnopis s pomočjo frekvenčne analize.

Zimmermannov telegram

Arthur Zimmermann, 1864 - 1940

Zimmermannov 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

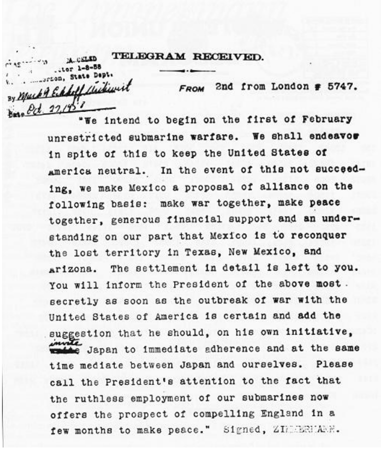
MEXICO CITY

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 3569 3670

BERNSTORFF.

Charge German Embassy.

Zimmermannov telegram



TELEGRAM RECEIVED.

DECLASSIFIED
...tor 1-8-88
...rton, State Dept.
By Mack A Eckhoff Archivist
Date Oct. 22, 1958

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, ~~[illegible]~~ 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.

Mačkovšek - Miselj

Vladimir Miselj, 1889 - 1944

Lahi pobirajo radio aparate in odstraniti je treba vse antene. Poskušali bodemo vseeno oddajati v Švico na valu 45,6m vsak torek dopoldne ob 7h po Greenwichu. Obvestite nas pod geslom "Majda" preko slovenske londonske oddaje, če ste prejeli. Na klic bo NOM deset minut, ne da bi čakali odgovor, nato oddaja. **Ključ po angleškem načinu; z uporabo Aškerca; prvi dve številki stran, drugi dve vrstica.**

Primer

p	r	e	d	s	a	m	o	s	t	a	n	o	m
10	11	4	3	12	1	5	8	13	14	2	7	9	6
p	o	š	l	j	i	n	a	m	n	o	v	i	h
v	e	s	t	i	s	t	o	p	s	m	o	š	e
v	e	d	n	o	v	b	o	d	e	č	i	ž	i
c	i	s	t	o	p	p	r	e	h	o	d	a	n
i	n	o	b	e	n	e	g	a	x	x	x	x	x

Primer

isvpn omčox ltntb šsdso ntbpe heinx voidx aoorg iššax pvvci oeein jiooe mpdea nsehx

Primer

isvpn omčox ltntb šsdso ntbpe heinx voidx aoorg iššax pvvci oeein jiooe mpdea nsehx

Šifra je primer **transpozicijske šifre**.

Kaj pa varnost transpozicijske šifre?

Kaj pa varnost transpozicijske šifre?

Najprej, dolžina ključa je (vsaj ponavadi) deljitelj števila vseh črk v sporočilu. Ko ugotovimo dolžino ključa, razdelimo tajnopis na ustrezno dolge segmente, ter poskusimo tajnopis razvozlati z anagramiranjem.

V zgornjem primeru je število vseh črk $70 = 5 \cdot 14$. Torej je ključ bodisi dolžine 5 ali dolžine 14.

V zgornjem primeru je število vseh črk $70 = 5 \cdot 14$. Torej je ključ bodisi dolžine 5 ali dolžine 14. Če je ključ dolžine 14, potem pogledamo črke prve vrstice sporočila (vsaka peta črka tajnopisa):

i, o, l, š, n, h, v, a, i, p, o, j, m, n

V zgornjem primeru je število vseh črk $70 = 5 \cdot 14$. Torej je ključ bodisi dolžine 5 ali dolžine 14. Če je ključ dolžine 14, potem pogledamo črke prve vrstice sporočila (vsaka peta črka tajnopisa):

i, o, l, š, n, h, v, a, i, p, o, j, m, n

S pomočjo anagramiranja potem poskusimo iz tega sestaviti smiselne besede:

pošlji nam novih

Dobri vojak Švejk

Pokorno javljam ...