MAZĀ MATEMĀTIKAS UNIVERSITĀTE

LATVIJAS UNIVERSITĀTE
ANNO 1919

FIZMATI.LV

Kriptogrāfija

LU FMF profesors
Jānis Buls

LU FMF studenti
Raitis Ļebedevs, Inese Bērziņa

Mazā matemātikas universitāte
1. nodarbība, 2013. gada 5. oktobris

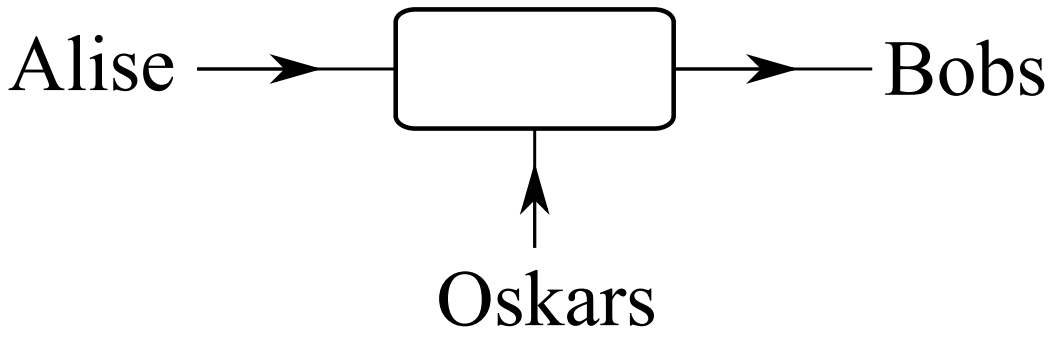
Saturs

Ievads

1. Kas ir kriptogrāfija?
2. Kad un kāpēc radās kriptogrāfija?
3. Interesantākās metodes, kā tika nosūtīta slepena informācija.

Galvenie jēdzieni

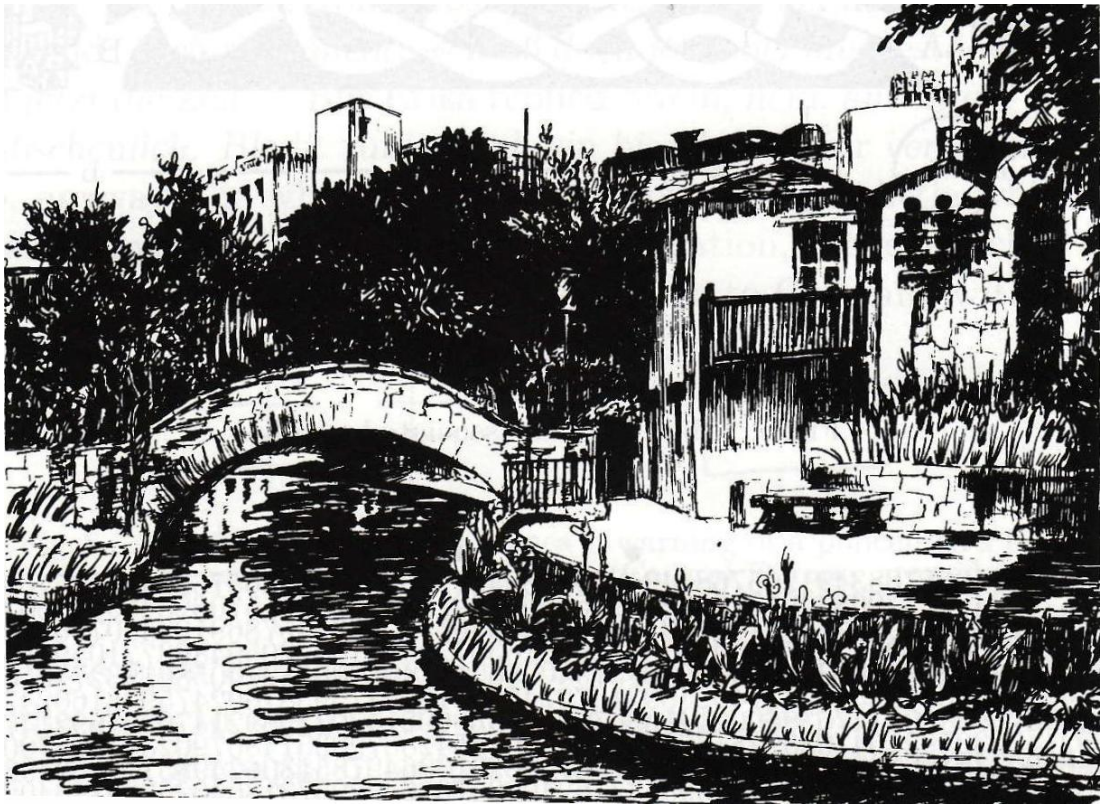
Pamatteksts, kriptoteksts, šifrs



1. Pamatteksts – slepena informācija, ko Alise vēlas nosūtīt Bobam tā, lai Oskars to neuzzinātu.
2. Kriptoteksts jeb kriptogramma – pamatteksta šifrēšanas rezultāts
3. Šifrs – invertējamu kriptogrāfisku attēlojumu kopa E.

Šifra piemēri

Gleznā apslēpts Morzes kods.



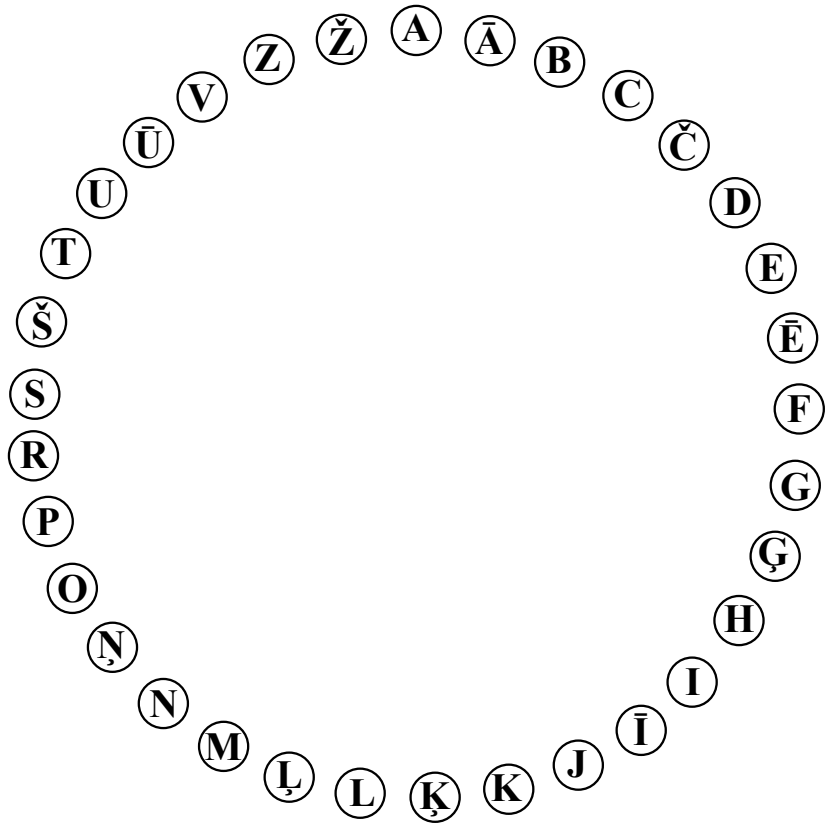
Šifra piemēri

Cēzara šifrs – katrs burts tiek aizstāts ar burtu, kas atrodas 3 vietas tālāk pulksteņa rādītāja virzienā:

A, Ā, B, C, Č, D, E, Ē, F, G, Ģ, H, I, Ī, J, K, Ķ, L, Ļ, M, N, Ņ, O, P, R, S, Š, T, U, Ū, V, Z, Ž

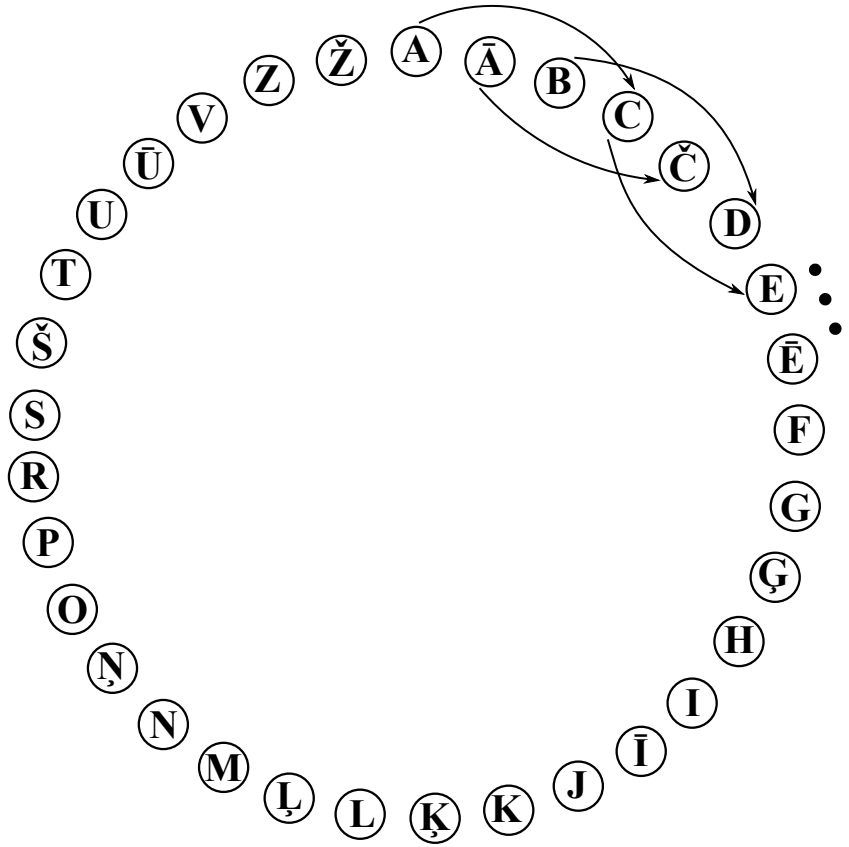
Šifra piemēri

Cēzara šifrs – katrs burts tiek aizstāts ar burtu, kas atrodas 3 vietas tālāk pulksteņa rādītāja virzienā:



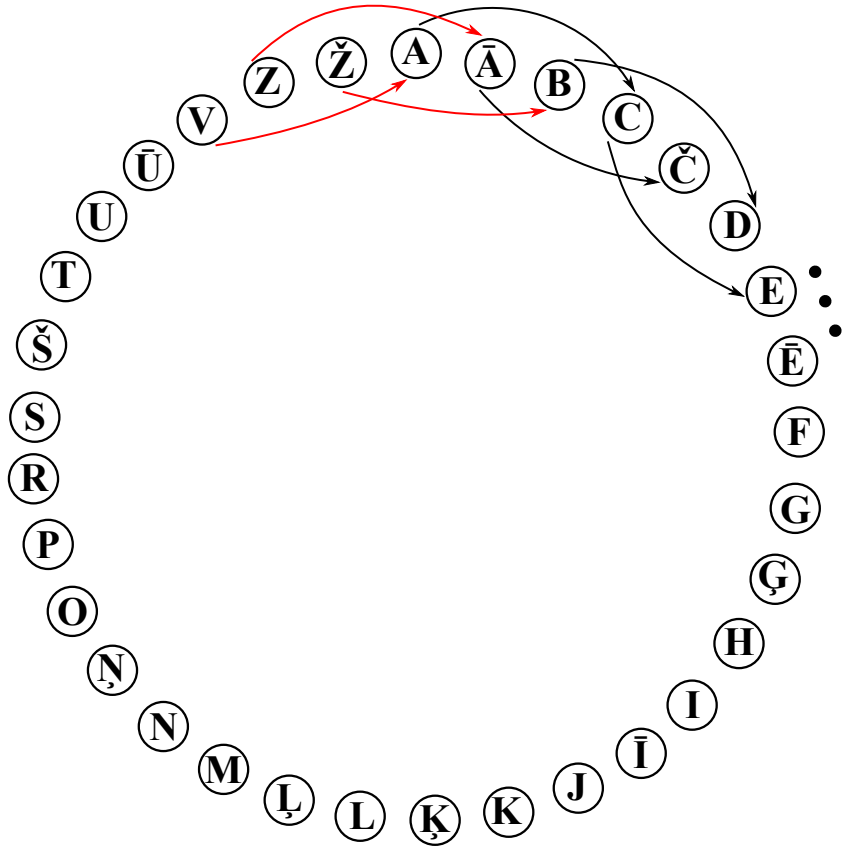
Šifra piemēri

Cēzara šifrs – katrs burts tiek aizstāts ar burtu, kas atrodas 3 vietas tālāk pulksteņa rādītāja virzienā:



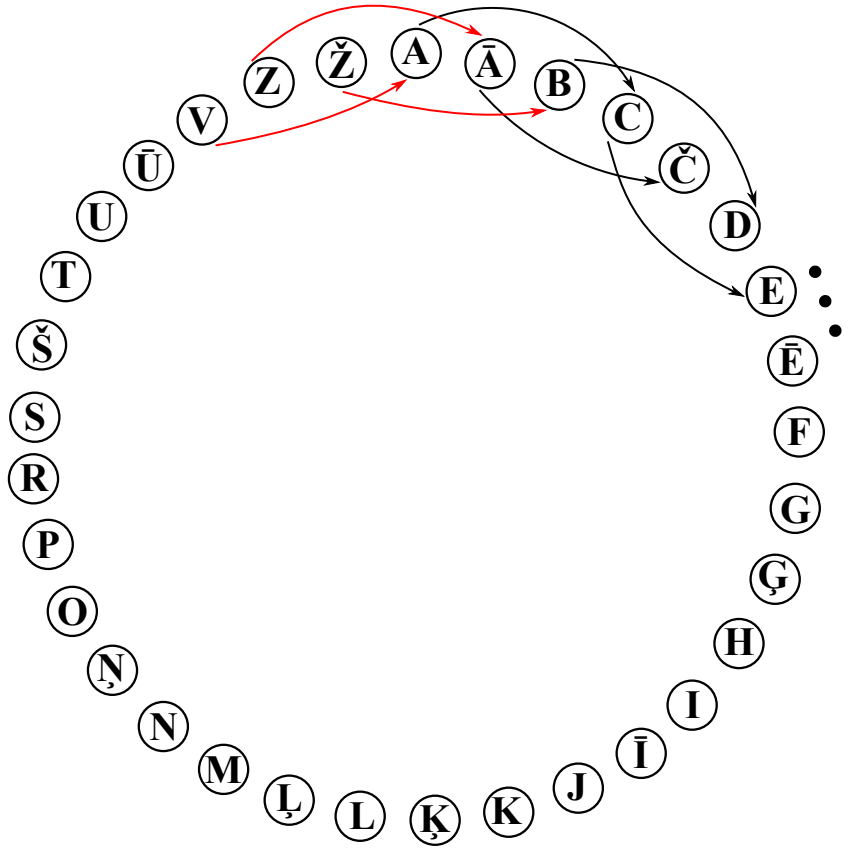
Šifra piemēri

Cēzara šifrs – katrs burts tiek aizstāts ar burtu, kas atrodas 3 vietas tālāk pulksteņa rādītāja virzienā:



Šifra piemēri

Cēzara šifrs – katrs burts tiek aizstāts ar burtu, kas atrodas 3 vietas tālāk pulksteņa rādītāja virzienā:



Z	I	E	M	A
Ā	K	G	O	C

Atslēga

- Atslēga – parametra vērtība, ar ko saista katru šifra attēlojumu.

Piemērs

Cēzara šifrā tiek izmantota burtu nobīde par 3 pozīcijām, tātad varam uzskatīt, ka mums ir dots burtu nobīdes šifrs ar atslēgas vērtību $k = 3$. Protams, varam izvēlēties nobīdi arī par 1, 2, 4, 5,... pozīcijām. Izvēloties citu k vērtību, iegūsim citu šifru.

Kriptosistēma

Definīcija

Kortežu $\langle \mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$ sauc par kriptosistēmu, ja

- $\mathcal{P}$ — pamattekstu kopa;
- $\mathcal{C}$ — kriptotekstu kopa;
- $\mathcal{K}$ — atslēgu kopa;
- $\mathcal{E} : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ — šifrs
- $D : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$ — dešifrējošais attēlojums

un katram pamattekstam $x \in \mathcal{P}$, katrai atslēgai $k \in \mathcal{K}$ ir spēkā vienādība

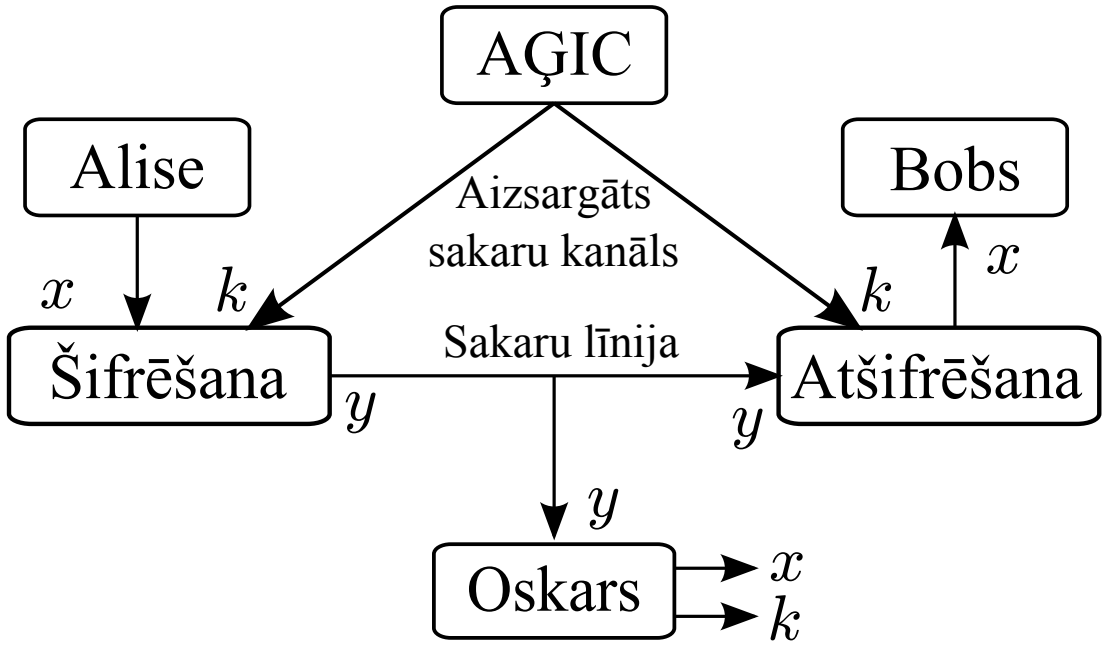
$$\mathcal{D}(\mathcal{E}(x, k), k) = x.$$

Galvenie kriptosistēmu veidi

Galvenie kriptosistēmu veidi:

1. Slepenās atslēgas kriptosistēma,
2. Publiskās atslēgas kriptosistēma,
3. Hibrīdās kriptosistēmas.

Slepenās atslēgas kriptosistēma



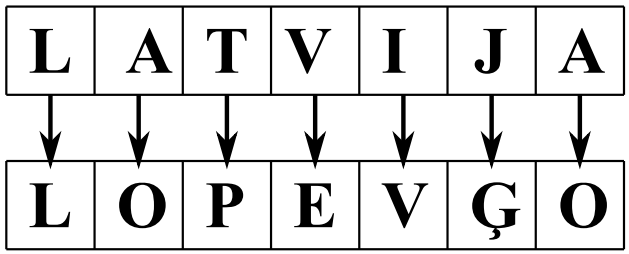
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



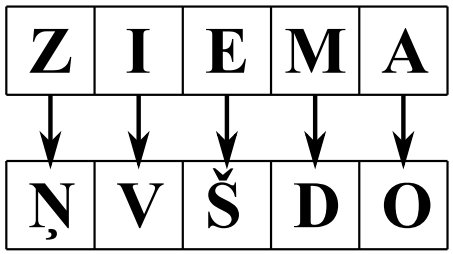
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



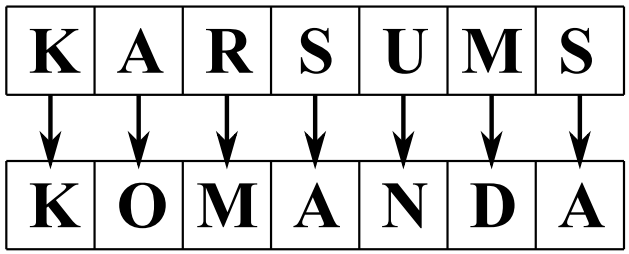
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



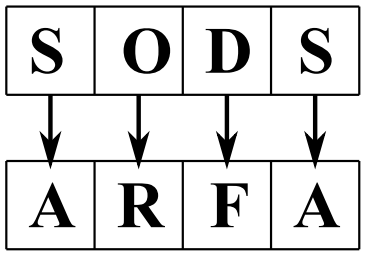
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



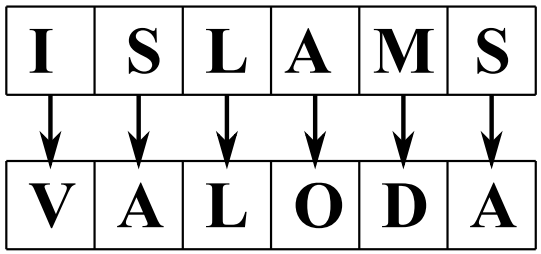
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



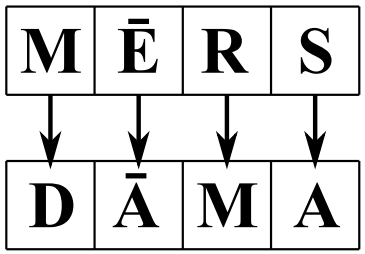
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



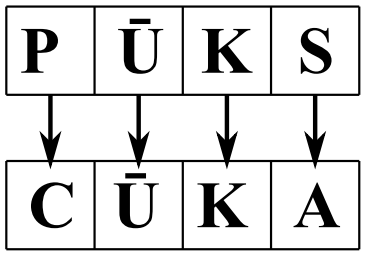
Substitūciju šifrs

Substitūciju šifrā katram alfabēta burtam piekārto 1 citu (var to pašu) burtu, piemēram,

A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K	Ķ
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
O	G	Č	Ķ	J	F	Š	Ā	H	Ē	Ļ	Ī	V	I	Ģ	K	T

L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	U	D	Z	Ž	R	C	M	A	S	P	N	Ū	E	Ņ	B

Iegūstam:



Šifrs ar "Kardano sietu" kā atslēgu

- "Kardano siets" pazīstams vairāk kā 400 gadus.
- "Kardano siets" ir kvadrātiska tabula ar izmēru $2n \times 2n$, kur $n \in \mathbb{N}$, kurā ceturtā daļa pozīciju (kopumā n^2) izdalītas pamatteksta pierakstam.
- Šie n^2 lodziņi nejaušā veidā mazāk vai vairāk vienmērīgi sadalīti pa kvadrāta laukumu tā, lai pagriežot kvadrātu ap tā centru par 90^0, 180^0, 270^0 un 360^0 iespējams noklāt visus $4n^2$ kvadrāta lauciņus.

Šifrs ar "Kardano sietu" kā atslēgu

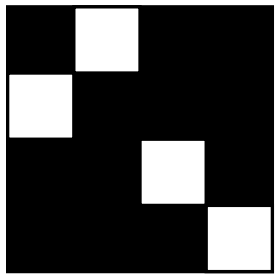
Lai šifrētu ar "Kardano sietu":

1. to uzliek uz tāda paša izmēra kvadrāta ar tukšiem lauciņiem;
2. redzamajos lauciņos secīgi saraksta pirmos n^2 pamatteksta simbolus;
3. pagriež par 90^0 un ieraksta nākamos n^2 pamatteksta simbolus;
4. pagriež par 90^0 (šis stāvoklis atbilst 180^0) un ieraksta nākamos n^2 pamatteksta simbolus;
5. pagriež par 90^0 (stāvoklis atbilst 270^0) un ieraksta pēdējos n^2 pamatteksta simbolus.

Šifrs ar “Kardano sietu” kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

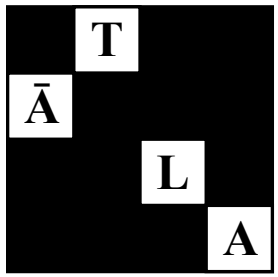
TĀLAVAS TAURĒTĀJS



Šifrs ar “Kardano sietu” kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

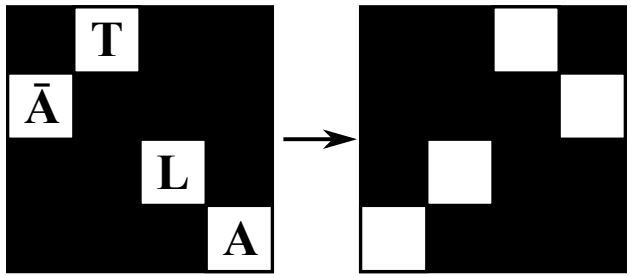
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

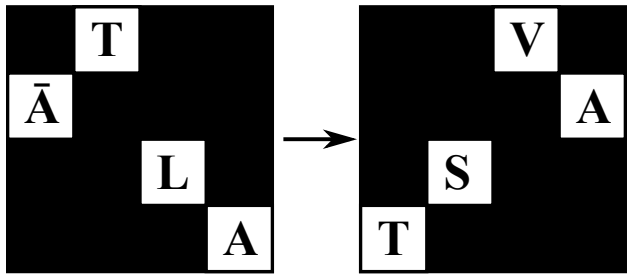
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

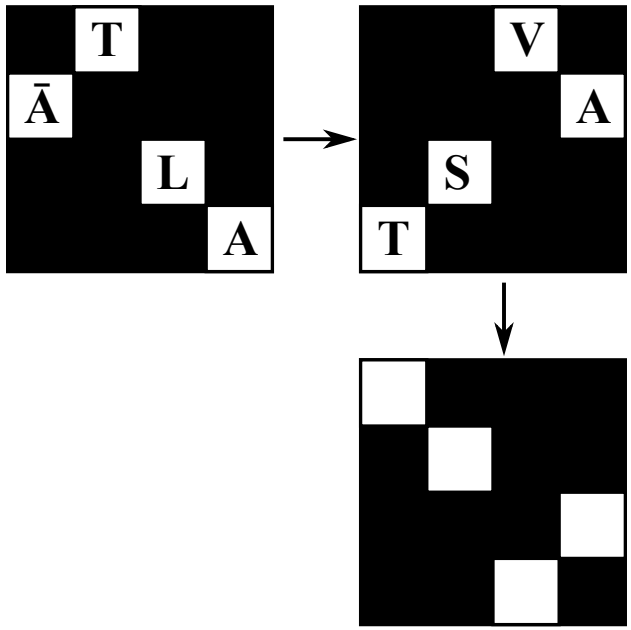
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

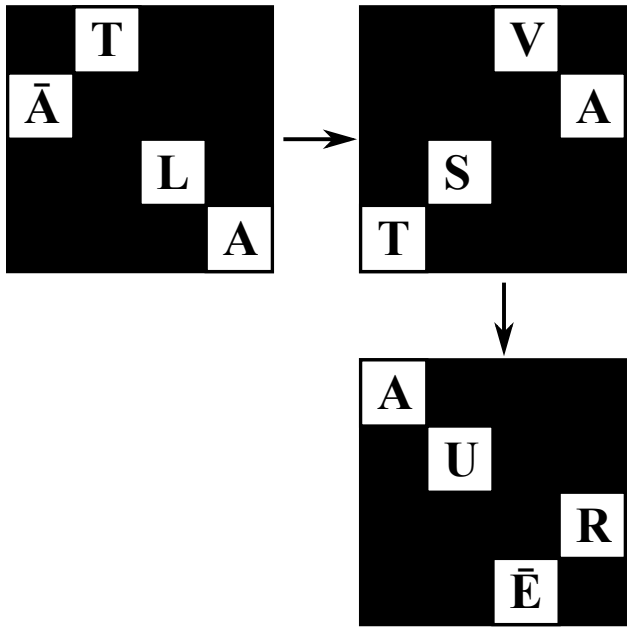
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

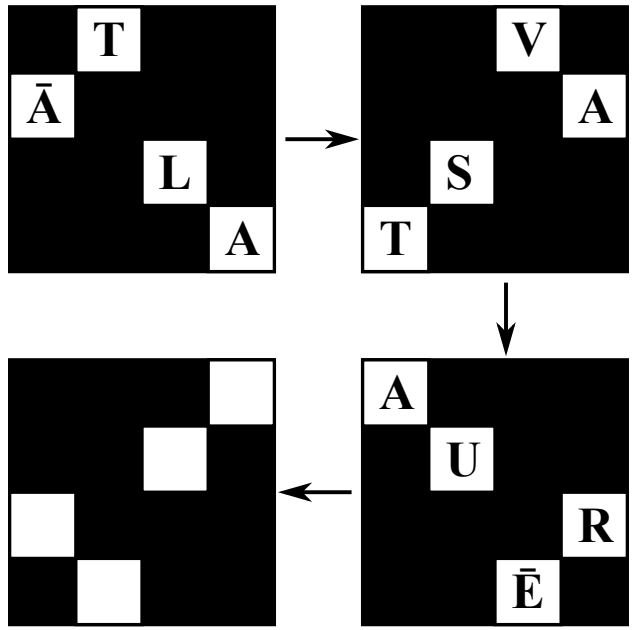
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

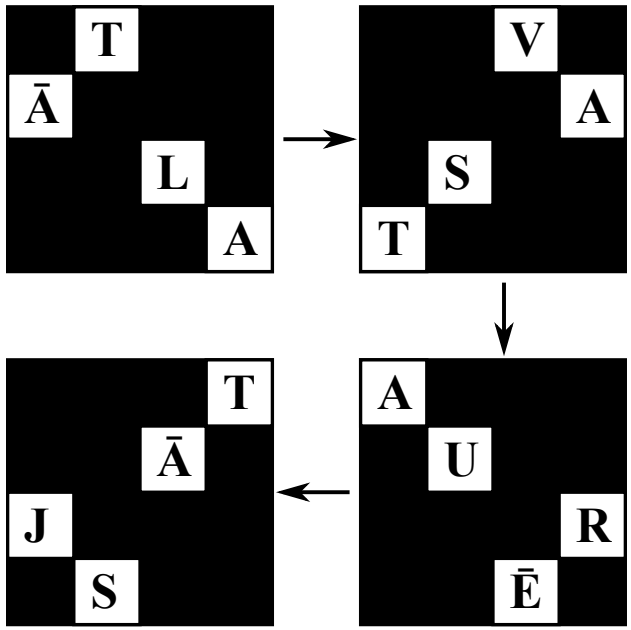
TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

TĀLAVAS TAURĒTĀJS



Šifrs ar "Kardano sietu" kā atslēgu

Pie $n = 2$ mums ir 4×4 kvadrāts. Nošifrēsim tekstu

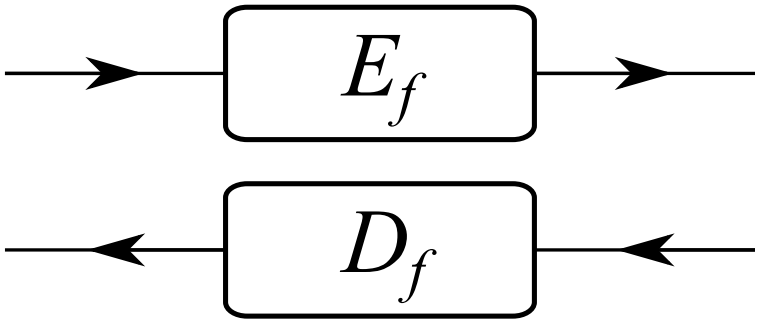
TĀLAVAS TAURĒTĀJS

A	T	V	T
Ā	U	Ā	A
J	S	L	R
T	S	Ē	A

Publiskās atslēgas kriptosistēma

NB!

Slepenās atslēgas kriptosistēmās tiek izmantota viena atslēga, bet publiskās atslēgas kriptosistēmās izmanto divas atslēgas: vienu šifrēšanai, otru – dešifrēšanai.



Publiskās atslēgas kriptosistēma

Darbību secība

1. Alise un Bobs vienojas par publiskās atslēgas kriptosistēmu.
2. Bobs nosūta Alisei publisko atslēgu k.
3. Alise izveido kriptogrammu $y = E_k(x)$.
4. Kriptogramma y tiek nosūtīta Bobam pa sakaru līniju.
5. Bobs atšifrē kriptogrammu, izmantojot privāto atslēgu z, t.i., $x = E_z(y)$.

Darbības pēc moduļa jeb darbības ar atlikumiem

Apskatīsim darbības pēc moduļa 6:

1. saskaitīšana
   - $(2+3)$ mod $6 = 5$, jo $5 : 6 = 0$ atlikumā 5.
   - $(4+5)$ mod $6 = 3$, jo $9 : 6 = 1$ atlikumā 3.
2. reizināšana un kāpināšana
   - $(2 \cdot 3)$ mod $6 = 0$, jo 6 dalās ar 6 (atlikums ir 0);
   - 2^3 mod $6 = 2$, jo $8 = 2^3$ dod atlikumu 2, dalot ar 6;

RSA kriptosistēma (1)

RSA – saīsinājums no Rivest R., Shamir A., Adleman L.

Algoritms atslēgas ģenerēšanai.

1. Izvēlas 2 lielus pirmskaitļus p un q.
2. Aprēķina $n = pq$.
3. Aprēķina $\varphi(n) = (p-1)(q-1)$.
4. Izvēlas $e \in \mathbb{N}$ tādu, ka $1 < e < \varphi(n)$ un $LKD\left(\varphi(n), e\right) = 1$.
5. Aprēķina skaitli d tādu, ka $(d \cdot e)$ mod $\varphi(n) = 1$.

Publiskā atslēga ir (n, e), privātā – d.

RSA kriptosistēma (2)

Šifrēšana, atšifrēšana:

1. Bobs nosūta Alisei publisko atslēgu (n, e).
2. Alise izsaka pamattekstu kā skaitli m intervālā $[0, n-1]$.
3. Alise atrod $c = m^e \bmod n$.
4. Alise nosūta kriptogrammu c Bobam.
5. Bobs izmanto privāto atslēgu, lai atšifrētu kriptogrammu: $m = c^d \bmod n$.

Burtu kodējums

1. Sanumurējam teksta burtus un atstarpes, sākot ar 0:

T	A	S		I	R
0	1	2	3	4	5

Burtu kodējums

1. Sanumurējam teksta burtus un atstarpes, sākot ar 0:

T	A	S		I	R
0	1	2	3	4	5

2. Katram burtam piekārtojam tā kārtas numuru alfabētā, bet atstarpei piekārtojam skaitli 0, t.i.,

	A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Ķ	L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Burtu kodējums

1. Sanumurējam teksta burtus un atstarpes, sākot ar 0:

T	A	S		I	R
0	1	2	3	4	5

2. Katram burtam piekārtojam tā kārtas numuru alfabētā, bet atstarpei piekārtojam skaitli 0, t.i.,

	A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ķ	L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z	Ž
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

3. Aprēķinām attiecīgo skaitli:

$$\begin{aligned} S_{\text{TAS IR}} &= 28 \cdot 34^0 + 1 \cdot 34^1 + 26 \cdot 34^2 + 0 \cdot 34^3 + 13 \cdot 34^4 + 25 \cdot 34^5 \\ &= 1153288086 \end{aligned}$$

RSA Piemērs

Alise vēlas nosūtīt Bobam ziņu "JĀ".

Atslēgas ģenerēšana:

1. Izvēlamies $p = 43$, $q = 41$, tad $n = 1763$
2. $\varphi(n) = (43 - 1)(41 - 1) = 1680$.
3. Izvēlamies $e = 11$, tad $d = 611$.
   Varam pārliecināties, ka $e \cdot d = 11 \cdot 611 = 6721$ un $6721 : 1680 = 4$ atl. 1.
4. Publiskā atslēga ir $(1763, 11)$, privātā – 611

RSA piemērs

Šifrēšana, atšifrēšana:

1. Bobs nosūta Alisei publisko atslēgu $(1763, 11)$.
2. Alise izsaka pamattekstu "JĀ" kā skaitli, t.i.,

$$\text{JĀ} = 15 \cdot 34^0 + 2 \cdot 34^1 = 15 + 68 = 83$$

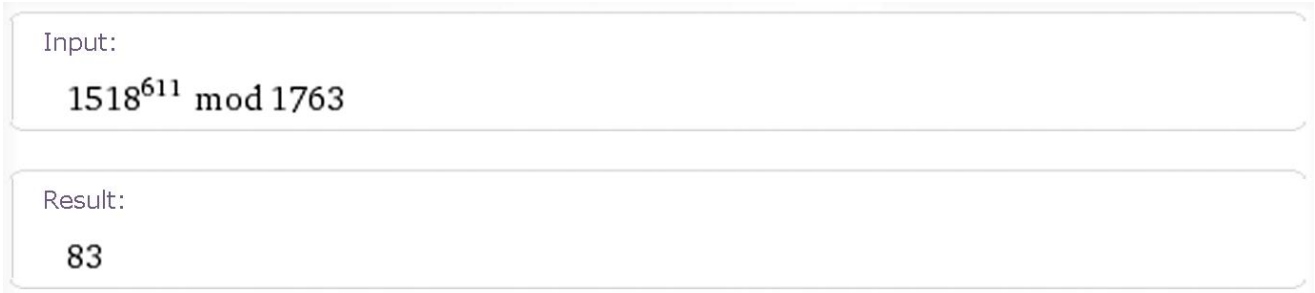
3. Alise aprēķina $c = 83^{11} \bmod 1763 = 1518$.
4. Alise nosūta kriptogrammu $c = 1518$ Bobam.
5. Bobs izmanto privāto atslēgu, lai atšifrētu kriptogrammu: $m = 1518^{611} \bmod 1763 = 83$.

Atkāpe

Padoms, kā aprēķināt a mod b lieliem skaitļiem:

1. MS Excel nerēķina 1518^{611} mod $1763 = 83$;
2. Var izmantot `http://www.wolframalpha.com/`
3. ierakstām formulu

4. Nospiežam "="
5. Wolfram Alfa izdod atbildi:



Kriptoanalīze

Tiek pieņemts, ka kriptoanalītiķis Oskars:

1. kontrolē sakaru līniju;
2. zina šifra īpašības;
3. nezina atslēgu k.

Paroļu drošība

Pieņemam, ka Alisei ir parole “bembītis”:

1. Ja izmantojam tikai mazos burtus, tad Oskaram jāpārbauda aptuveni 100 000 vārdi.
2. Ja papildus pamainām mazos burtus ar lielajiem (katru burtu skaita 2 reizes):
   - 1.burtu $\rightarrow$ 200 000 vārdi
   - arī 2.burtu $\rightarrow$ 400 000 vārdi

     ...
   - arī 8.burtu $\rightarrow$ $2^8 \cdot 100\ 000 = 25\ 600\ 000$ vārdi

     ...

Paroļu drošība

3. Alise var sarežģīt paroli, pieliekot ciparus beigās, piem., pieliekot 2005, tā tiek sarežģīta vēl 10 000 reizes, tātad 25 600 000 000 vārdi
4. Aizstājam dažus burtus ar cipariem, kādu burtu kombināciju ar citu, piem., b$\rightarrow$B, ī$\rightarrow$1, tis$\rightarrow$c, tad

$$\text{bembītis2005} \longrightarrow \text{BemB1c2005}$$

Pieņemsim, ka tas sarežģa paroli vēl 1000 reizes, .t.i, tagad Oskaram jāpārbauda 25 600 000 000 000 vārdi.

Paroļu drošība

Cik tas ir droši?!

- $26^8 \sim 2^{38}$, t.i., paroles no 8 mazajiem burtiem, pārbauda minūtes laikā.
- $256 \cdot 10^{11} \sim 2^{45} = 2^7 \cdot 2^{38}$ atšifrēs aptuveni $2^7 = 128$ minūtēs jeb $\sim$ 2 stundās.
- $62^8 \sim 2^{48} = 2^{10} \cdot 2^{38}$, t.i., lielie burti + mazie + cipari, pārbaudīs 1024 min jeb 17h laikā.
- $62^{12} \sim 2^{72} = 2^{34} \cdot 2^{38}$ pārbaudīs 2^{34} min jeb 29 000 gados.

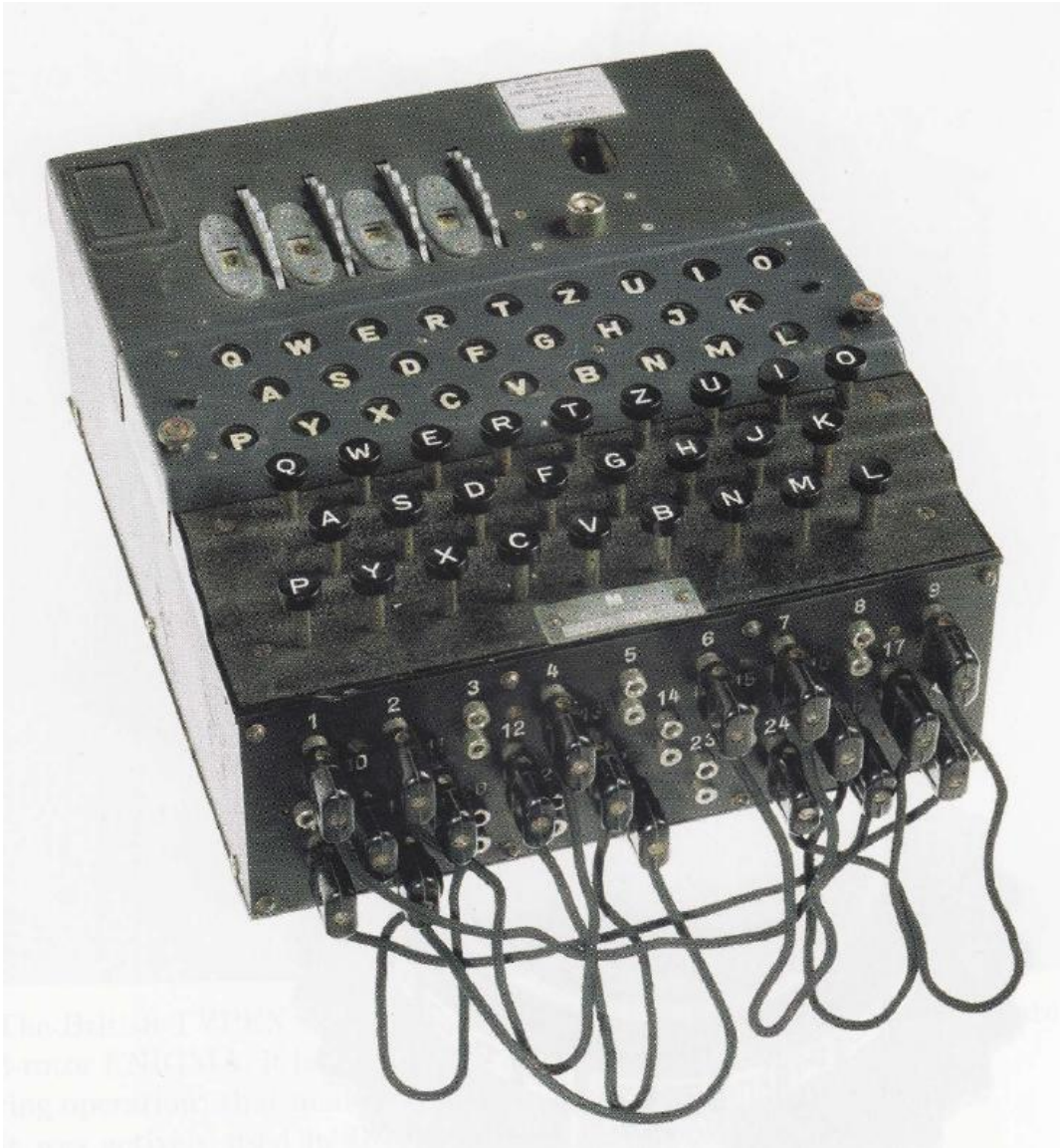
Kā uzkonstruēt drošu paroli?

1. Neviens nevar atcerēties nejaušu paroli,
2. Var izvēlēties kādas frāzes pirmos burtus.
   - Bībeli labāk neizvēlēties,
   - Neizvēlēties frāzi, ko kāds ar jums saista, var iedomāties.

Dešifrēšanas uzdevumi:

1. uzbrukums, izmantojot tikai kriptotekstu;
2. uzbrukums, izmantojot zināmu pamattekstu;
3. uzbrukums, izmantojot izvēlētu pamattekstu;
4. uzbrukums, izmantojot izvēlētu kriptotekstu.

Enigma (1919)



CRAY-1 S (1979)

Statistika:

Burtu biežums dažādās valodās

Valoda	Alfabēta burts/ izmantošanas biežums %					
Angļu	E/ 12,86	T/ 9,72	A/ 7,96	I/ 7,77	N/ 7,51	R/ 7,03
Latviešu	A/ 9,81	I/ 7,70	S/ 7,31	T/ 5,11	E/ 5,11	U/ 5,02
Spāņu	E/ 14,15	A/ 12,90	O/ 8,84	S/ 7,64	R/ 7,01	T/ 6,95
Itāļu	I/ 12,04	E/ 11,63	A/ 11,12	O/ 8,92	N/ 7,68	T/ 7,07
Vācu	E/ 19,18	N/ 10,20	I/ 8,21	S/ 7,07	R/ 7,01	T/ 5,86
Franču	E/ 17,76	S/ 8,23	A/ 7,86	N/ 7,61	T/ 7,30	I/ 7,23
Krievu	O/ 11,0	/ 8,9	E/ 8,3	A/ 7,9	H/ 6,9	T/ 6,0

PALDIES PAR UZMANĪBU!