Jak bezpiecznie SEKRETOWAĆ

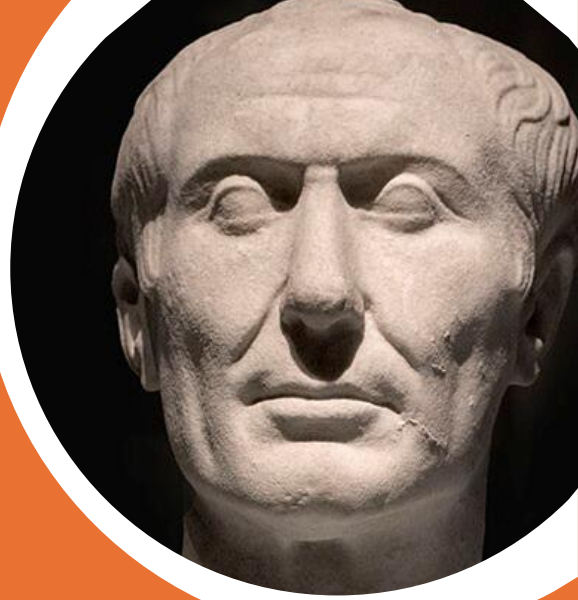
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

NAUKA O SEKRETACH

Kryptologia – dziedzina wiedzy o przekazywaniu informacji w bezpieczny sposób.

κρυπτός (*kryptos*) = ukryty

- **Kryptografia** – utajnianie wiadomości,
- **Kryptoanaliza** – łamanie zabezpieczeń.



PRZESZŁOŚĆ

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

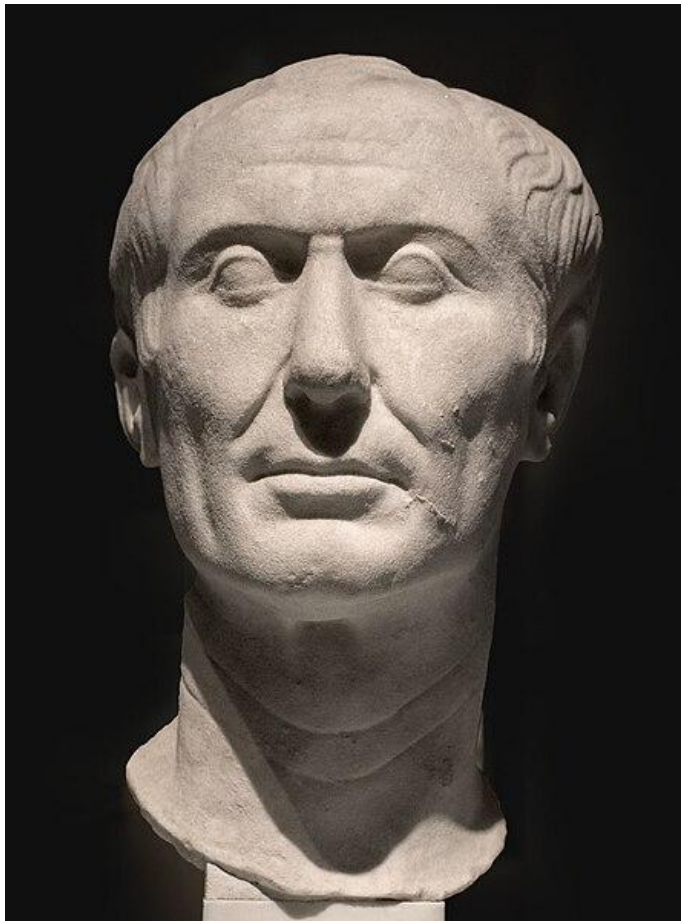
SKYTALE

- metoda szyfrowania opisana w VII w. p.n.e przez greckiego poetę,
- stosowana m.in. przez Spartan,
- tekst zapisywano na pasek skóry nawinięty na laskę. Adresat mógł szybko odczytać tekst przesłania, mając laskę o identycznej grubości.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

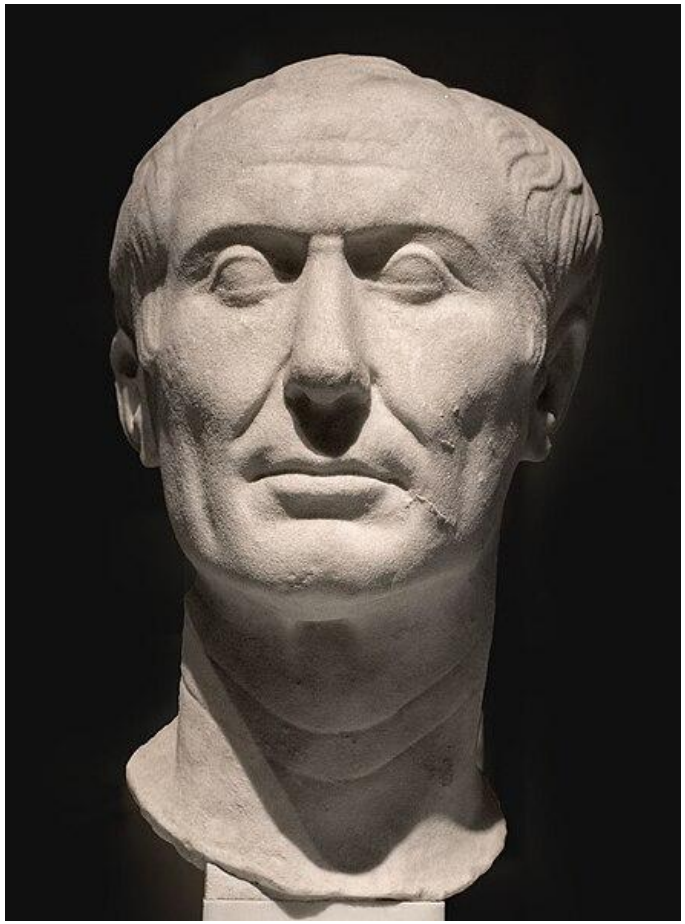


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

K O T

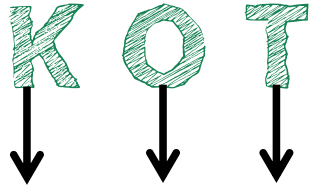
Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).



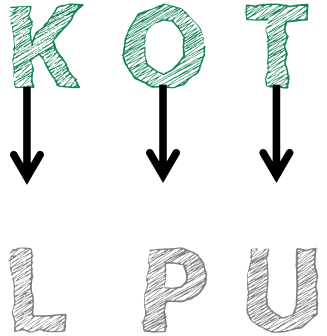
Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

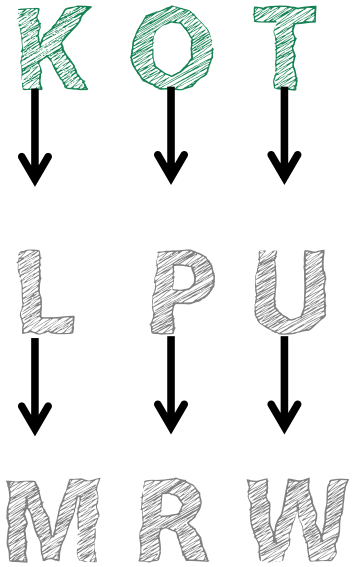


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

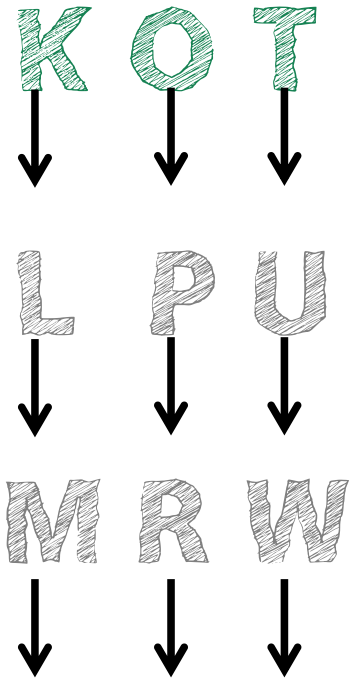


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.

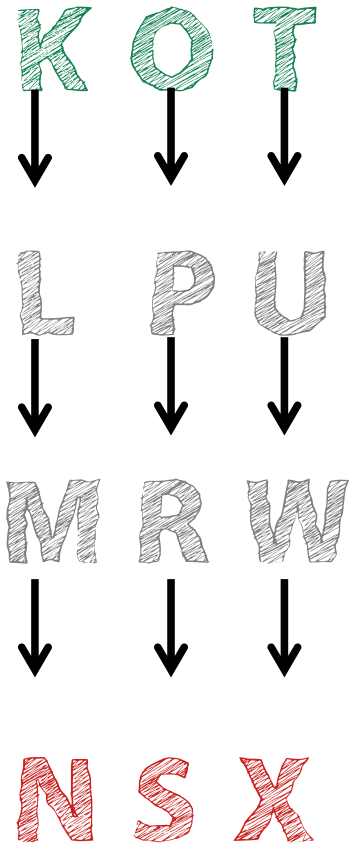


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

SZYFR CEZARA

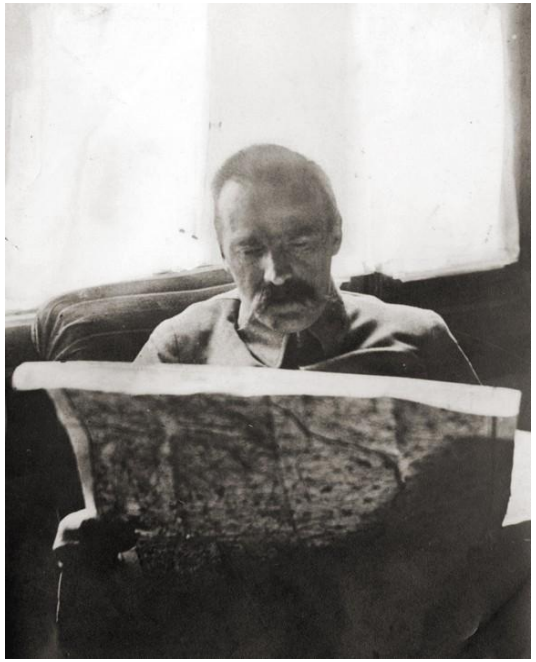
Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara (I wiek p.n.e.).

Szyfrował on korespondencję, pisząc zamiast każdej litery literę występującą w alfabecie trzy miejsca dalej.



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

CUD NAD WISŁĄ



decydująca bitwa wojny polsko-bolszewickiej,
stoczona w dniach 13-25.08.1920 r.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

- z wykształcenia chemik, oficer dawnej armii rosyjskiej,

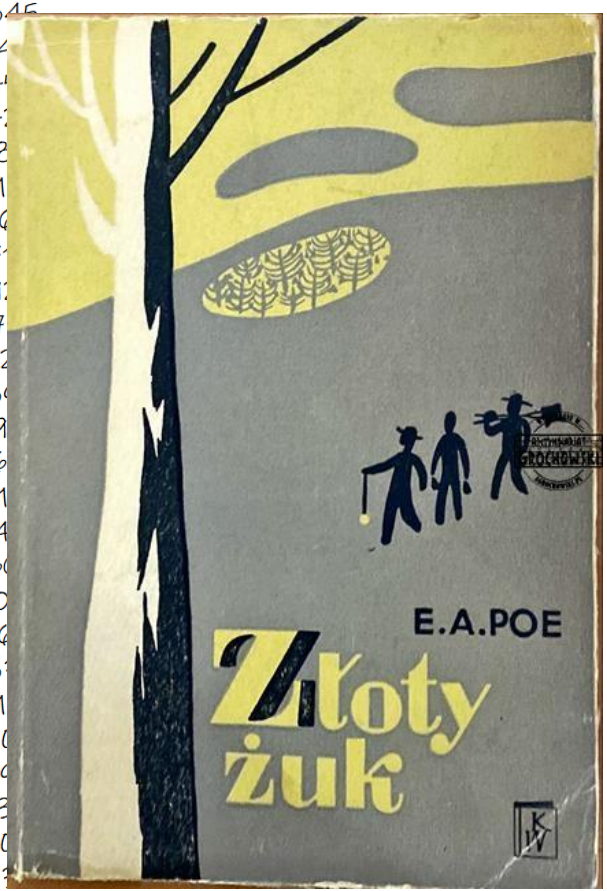
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

- z wykształcenia chemik, oficer dawnej armii rosyjskiej,

- znajomość rosyjskiego, francuskiego, niemieckiego, a także podstaw kombinatoryki,

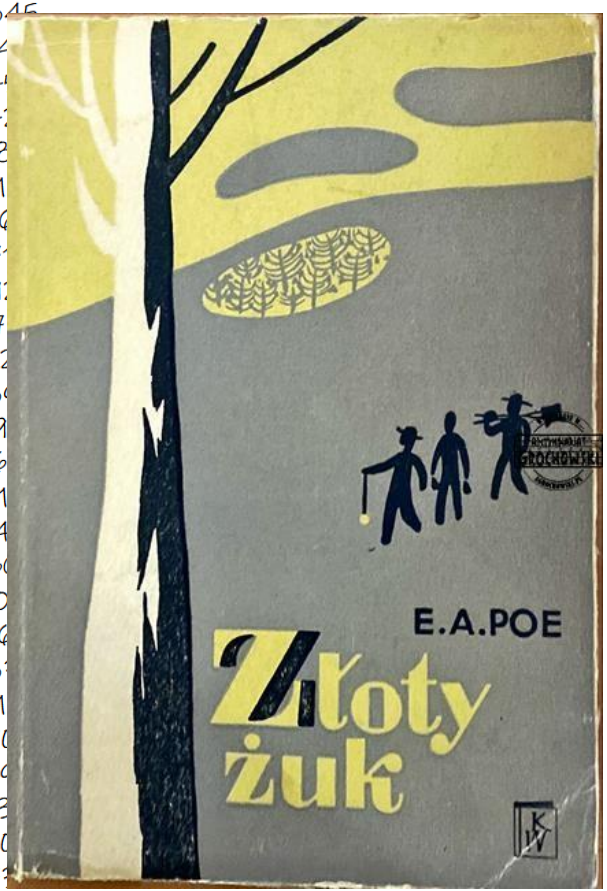
41202343
69866595
43855531
36533257
594817981
16998443
POR. JAN KOWALEWSKI



- z wykształcenia chemik, oficer dawnej armii rosyjskiej,
- znajomość rosyjskiego, francuskiego, niemieckiego, a także podstaw kombinatoryki,
- znajomość kryptografii – z lektury „*Sherlocka Holmesa*" oraz „*Złotego Żuka*" Edgara Allana Poe,

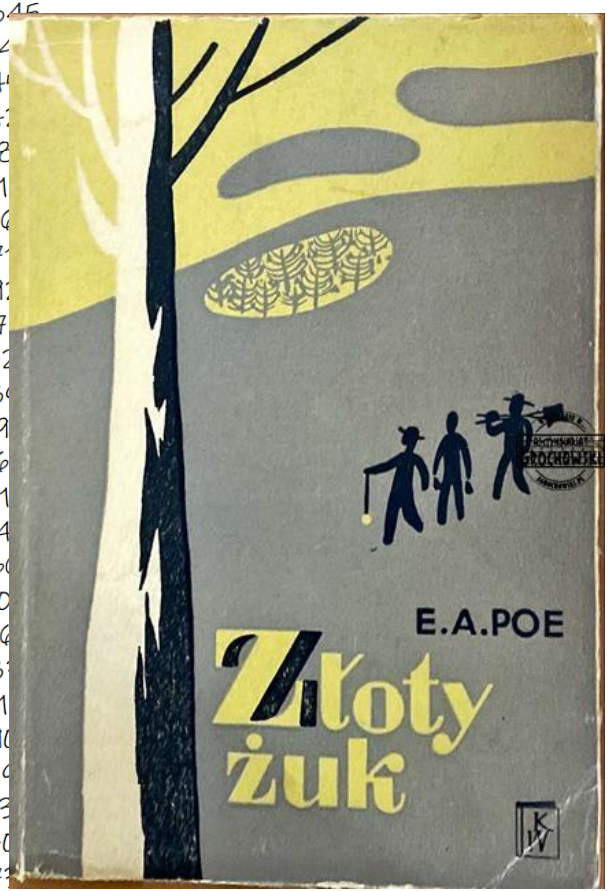
41202343
69866595
43855531
36533257
594817981
16998443
279828
455626
387644
652484
198098
042316
418792
420247
886949
609317
750334
309823
485150
490910
026986
186270
488086
705649
903653
886743
317208
041051
642547
282601
257624
394637
69391

POR. JAN KOWALEWSKI



- z wykształcenia chemik, oficer dawnej armii rosyjskiej,
- znajomość rosyjskiego, francuskiego, niemieckiego, a także podstaw kombinatoryki,
- znajomość kryptografii – z lektury „*Sherlocka Holmesa*" oraz „*Złotego Żuka*" Edgara Allana Poe,
- w sierpniu 1919 r. trafił na nocny dyżur w sekcji szyfrów na zastępstwo za kolegę, który udał się na ślub siostry,

41202343
69866595
43855531
36533257
594817981
16998443
POR. JAN KOWALEWSKI



- z wykształcenia chemik, oficer dawnej armii rosyjskiej,
- znajomość rosyjskiego, francuskiego, niemieckiego, a także podstaw kombinatoryki,
- znajomość kryptografii – z lektury „*Sherlocka Holmesa*" oraz „*Złotego Żuka*" Edgara Allana Poe,
- w sierpniu 1919 r. trafił na nocny dyżur w sekcji szyfrów na zastępstwo za kolegę, który udał się na ślub siostry,
- zamiast sortować depesze, zaczął bawić się w ich rozszyfrowywanie.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

- W radzieckich szyfrogramach każda litera odpowiadała cyfrze lub też kilku cyfrom,

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

дивизия

diwizija

- W radzieckich szyfrogramach każda litera odpowiadała cyfrze lub też kilku cyfrom,

- Kowalewski zaczął szukać wystąpień tych samych cyfr za pomocą grzebienia z wyłamanymi zębami (diwizija, Odessa, podpis szyfrującego). Korzystał też z analizy statystycznej.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

дивизия

diwizija

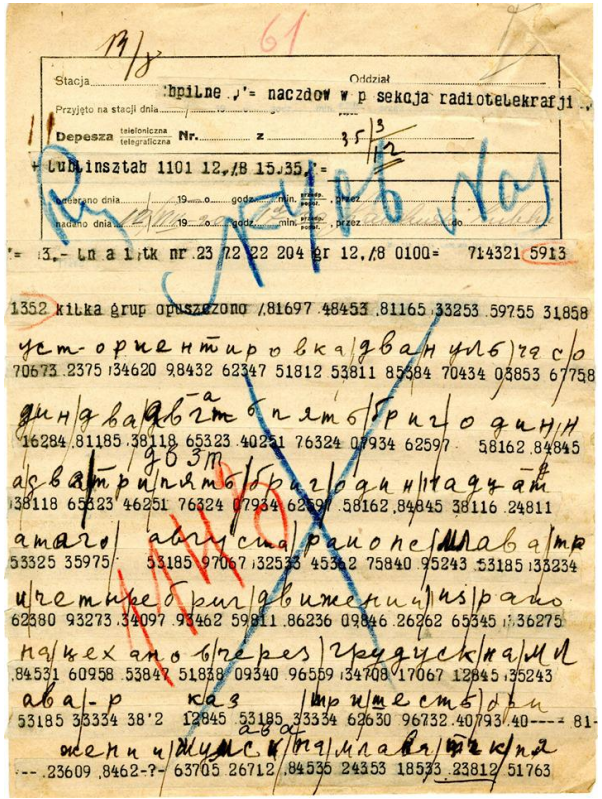
- W radzieckich szyfrogramach każda litera odpowiadała cyfrze lub też kilku cyfrom,

- Kowalewski zaczął szukać wystąpień tych samych cyfr za pomocą grzebienia z wyłamanymi zębami (diwizija, Odessa, podpis szyfrującego). Korzystał też z analizy statystycznej.

- Do łamania dalszych szyfrogramów zaprosił matematyków: Wacława Sierpińskiego, Stefana Mazurkiewicza i Stanisława Leśniewskiego.

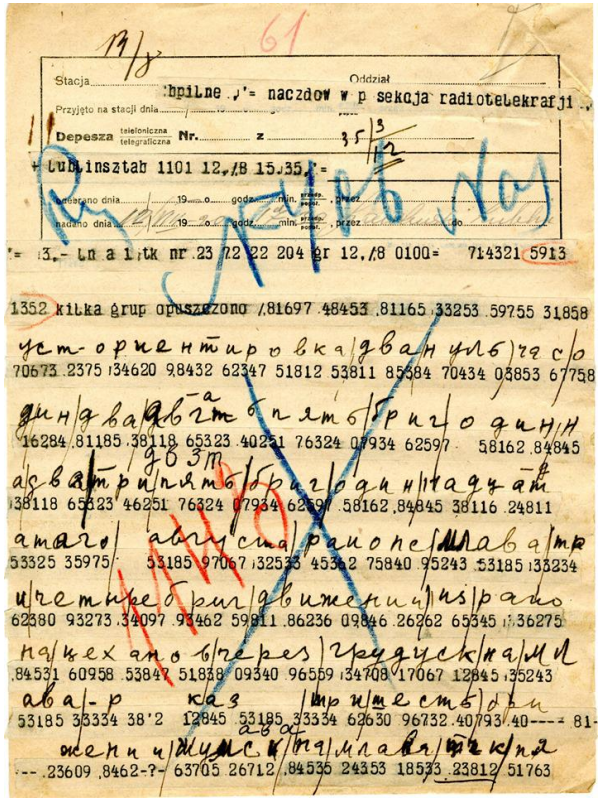
41202343
699866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

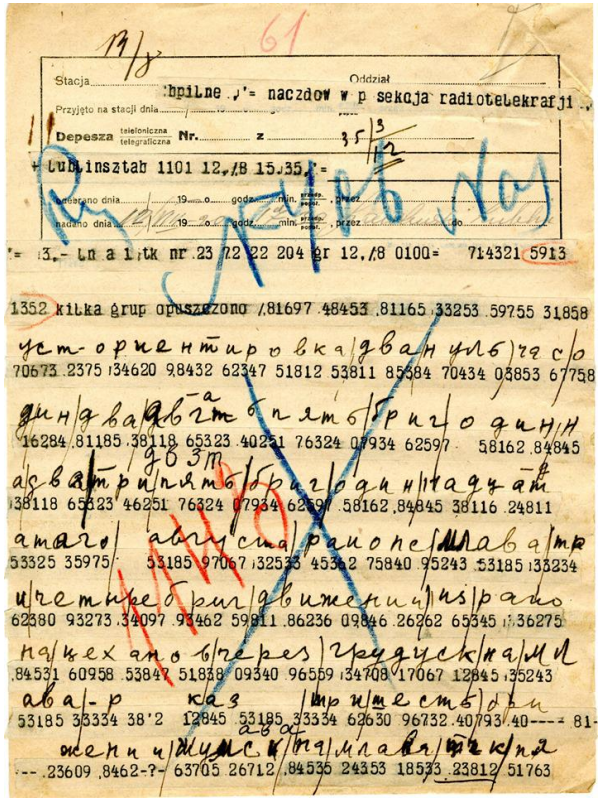
POR. JAN KOWALEWSKI


Stacja ... Oddział ...
Przyjęto na stacji dnia ...
Depesza telefoniczna telegraficzna Nr. ... z ...
Lublinsztab 1101 12./8 15.35.
Oddano dnia ... 19... o godz. ... min. przez ... do
Nadano dnia ... 19... o godz. ... min. przez ... do
3.- Ln a 1 tk nr 23 72 22 204 gr 12./8 0100= 714321 5913
1352 kilka grup opuszczono /.81697 48453 .81165 33253 59755 31858
70673 .2375 134620 98432 62347 51812 53811 85584 70434 03853 67758
16284 .81185 .38118 65323 40251 76324 07934 62597 58162 .84845
38118 65323 46251 76324 07934 62597 58162 .84845 38116 .24811
53325 35975 53185 97067 32533 45362 75840 95243 53185 33234
62380 93273 .34097 93462 59811 .86236 09846 .26762 65345 .36275
.84531 60958 .53847 51838 09340 96559 .34708 17067 12845 .35243
53185 33334 38'2 12845 53185 33334 62630 96732 40793 40--- = 81-
--- .23609 .8462-?- 63705 26712 .84536 24353 18533 .23812 51763

- Efekt pracy: rozkodowanie kilku tysięcy szyfrogramów Armii Czerwonej w latach 1919–1920.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POR. JAN KOWALEWSKI

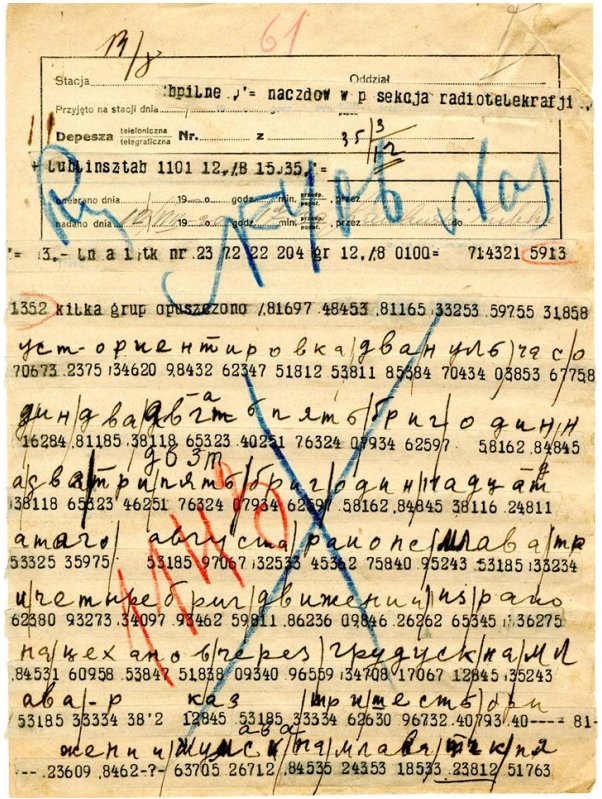


- Efekt pracy: rozkodowanie kilku tysięcy szyfrogramów Armii Czerwonej w latach 1919–1920.

- Dzięki temu prawie równocześnie z odebraniem propozycji pokojowej od bolszewików, wiedziano o ich dalszych planach wojennych.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

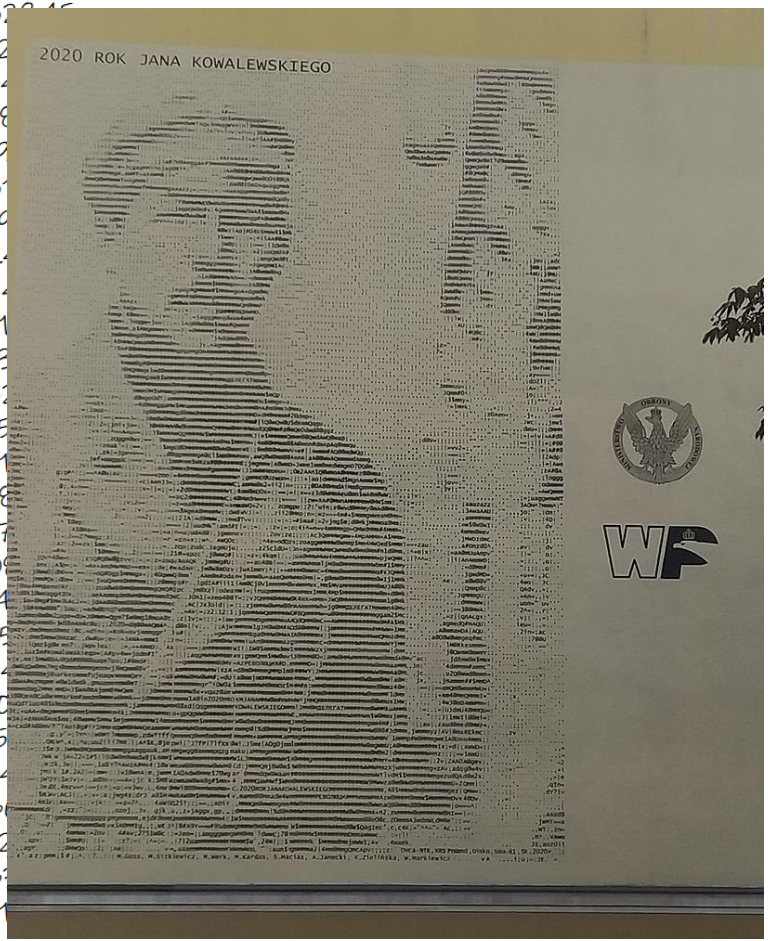
POR. JAN KOWALEWSKI



- Efekt pracy: rozkodowanie kilku tysięcy szyfrogramów Armii Czerwonej w latach 1919–1920.
- Dzięki temu prawie równocześnie z odebraniem propozycji pokojowej od bolszewików, wiedziano o ich dalszych planach wojennych.
- Znajomość planów wroga znacznie ułatwiła Piłsudzkiemu manewry.

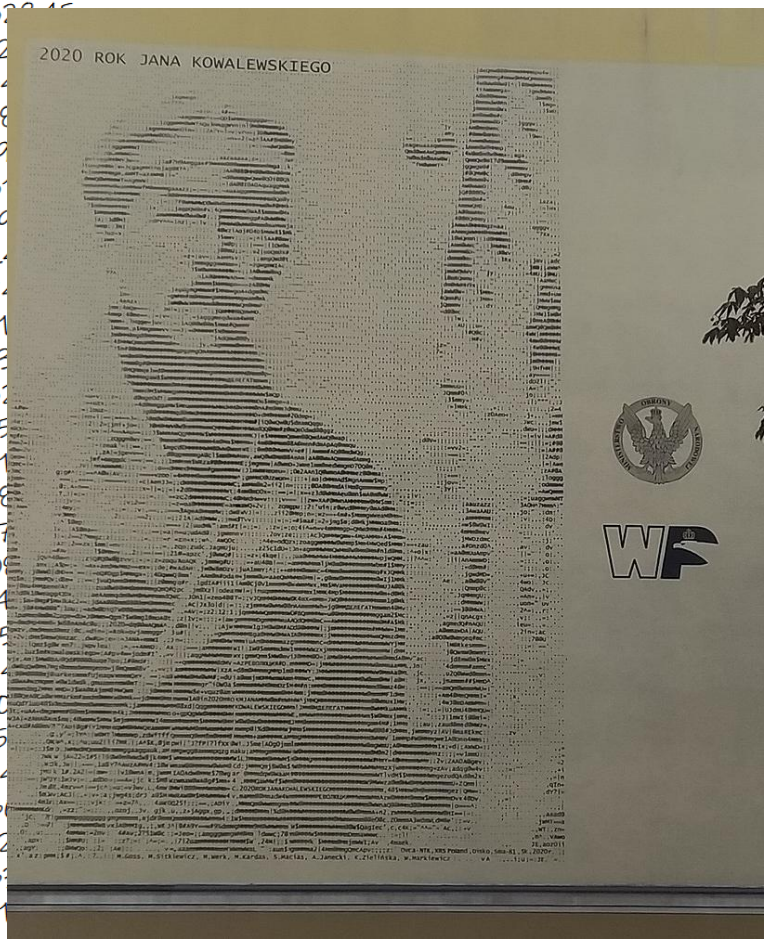
41202343
69866595
43855531
36533257
594817981
16998443
279823 45
45562
38764
65248
19809
04231
41879
42024
88694
60931
75033
30982
48515
49091
02698
18627
48809
70564
90365
88674
31720
04105
64254
28266
25762
39461
69391

POR. JAN KOWALEWSKI



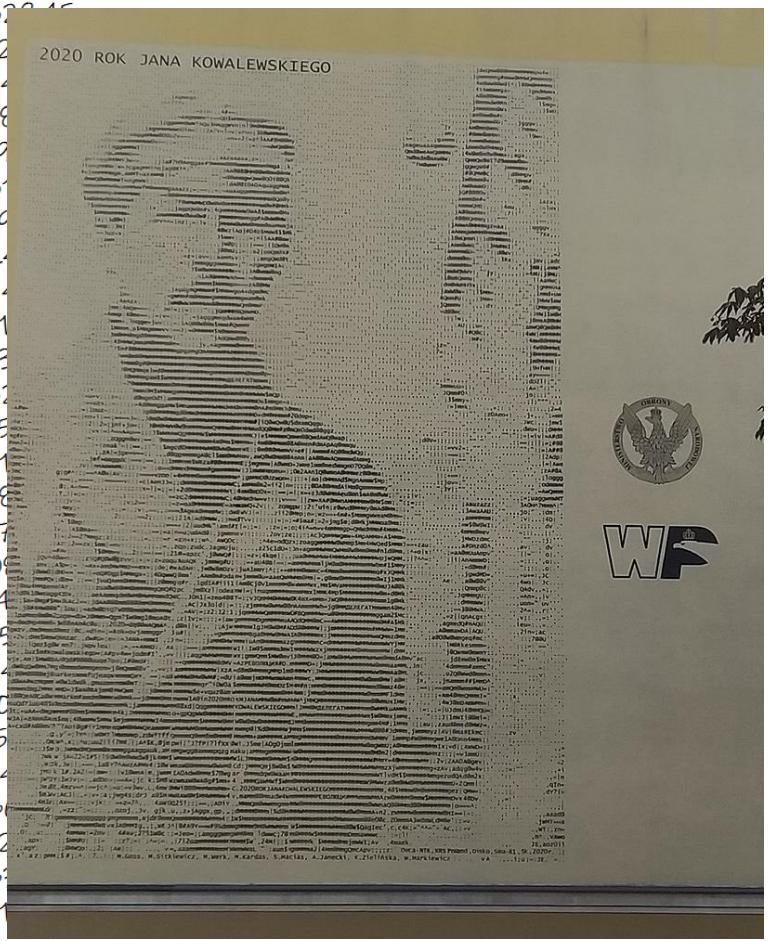
41202343
69866595
43855531
36533257
594817981
16998443
279823 45
45562
38764
65248
19809
04231
41879
42024
88694
60931
75033
30982
48515
49091
02698
18627
48809
70564
90365
88674
31720
04105
64254
28266
25762
39461
69391

POR. JAN KOWALEWSKI



- W kilka lat po wojnie szkolił w Tokio japońskich oficerów wywiadu.

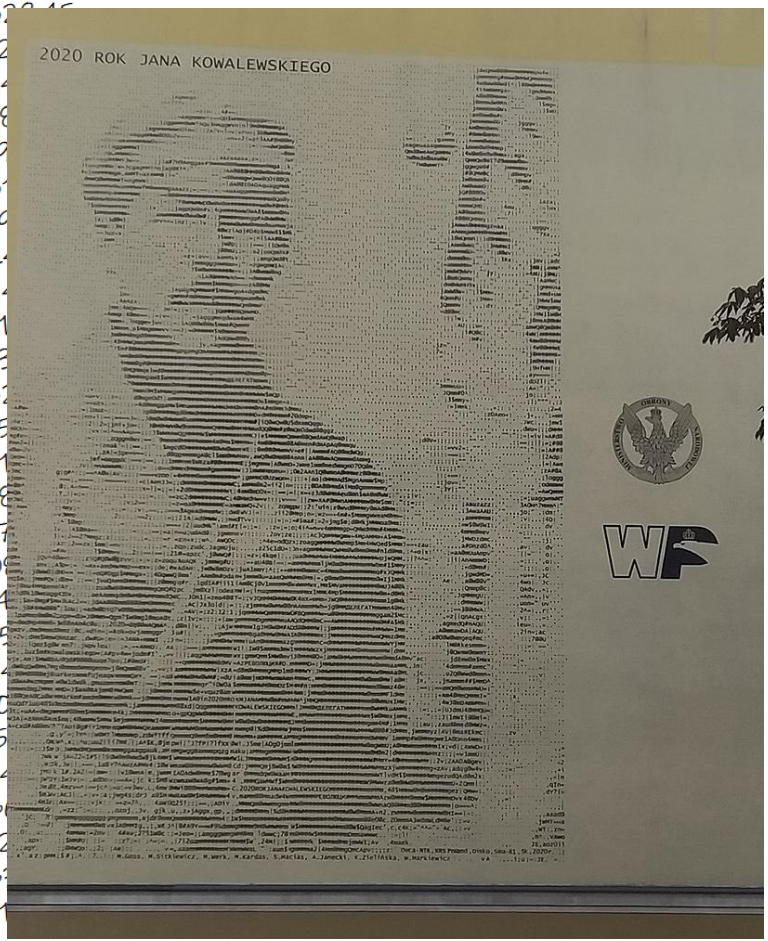
POR. JAN KOWALEWSKI



- W kilka lat po wojnie szkolił w Tokio japońskich oficerów wywiadu.

- Gen. Sikorski, wręczając order Virtuti Militari Kowalewskiemu, mrugnął okiem i powiedział: „Za wygraną wojnę!”.

POR. JAN KOWALEWSKI



- W kilka lat po wojnie szkolił w Tokio japońskich oficerów wywiadu.

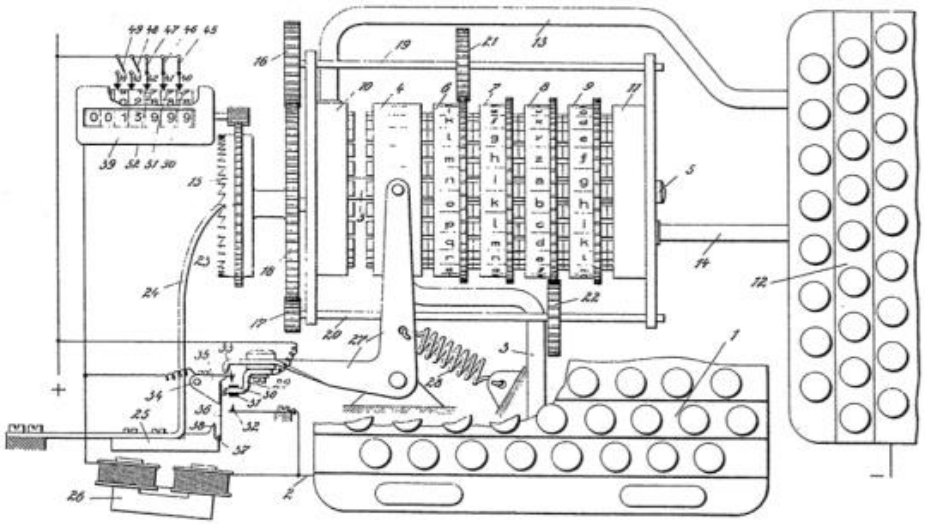
- Gen. Sikorski, wręczając order Virtuti Militari Kowalewskiemu, mrugnął okiem i powiedział: „Za wygraną wojnę!”.

- Senat RP przyjął uchwałę dotyczącą ustanowienia roku 2020 rokiem podpułkownika Jana Kowalewskiego.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA

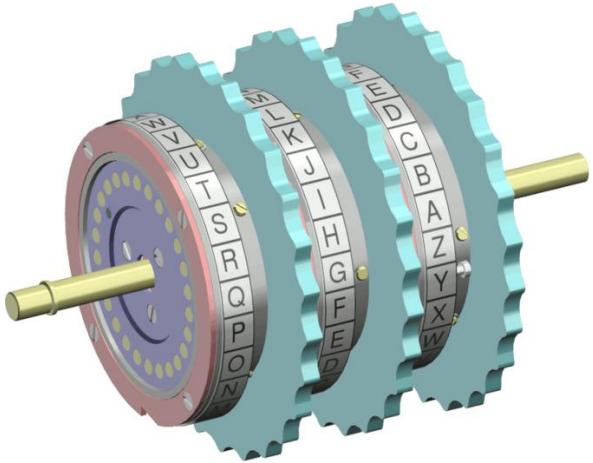
W 1918 roku niemiecki inżynier Artur Scherbius wraz z Richardem Ritterem złożył wniosek o przyznanie patentu na wirnikową maszynę szyfrującą.



Początkowo model do celów komercyjnych, od 1926 r. do celów wojskowych.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA



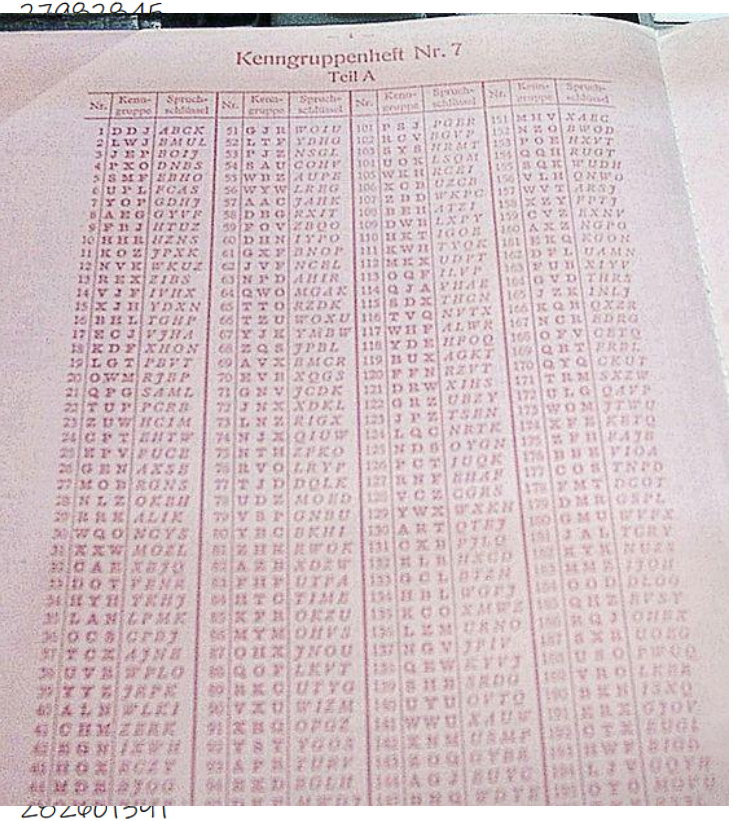
Maszyna składała się z klawiatury, podłączonej do systemu wirników.

Każdy wirnik przestawiał litery w alfabecie.

Dodatkowo, po kliknięciu klawisza, każdy z wirników obracał się o inny kąt.

41202343
69866595
43855531
36533257
594817981
16998443
27082845

ENIGMA



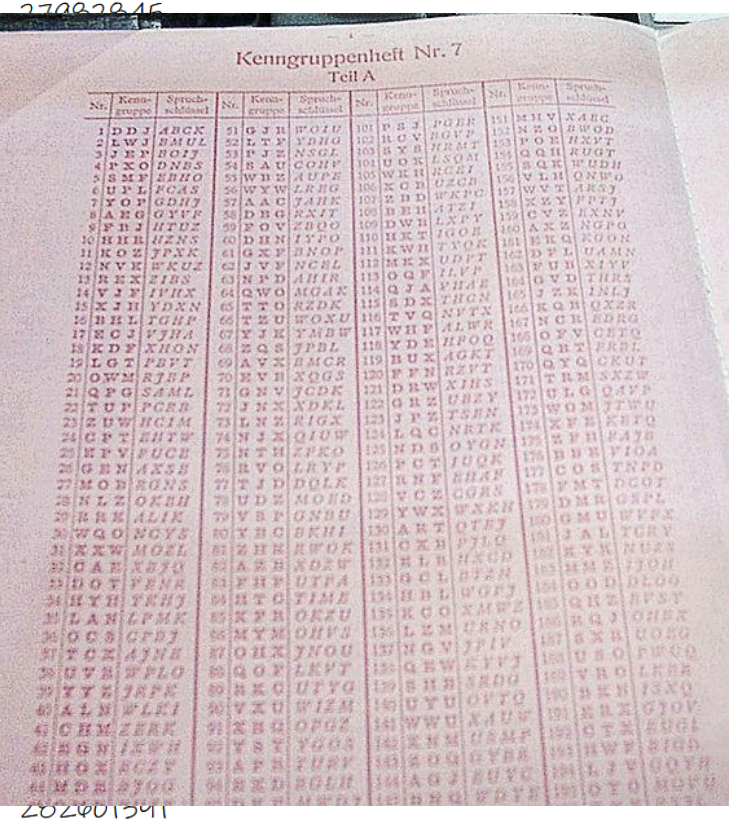
Kenngruppenheft Nr. 7
Teil A

Nr.	Kenngruppe	Spruchschlüssel
1	DDJ	ABGK
2	LWJ	BMUL
3	JEP	BOIJ
4	PXO	DNBS
5	SMP	EBHO
6	UPL	FCAS
7	YOP	GDHJ
8	AEG	GYVF
9	FBJ	HTUZ
10	HHR	HZNS
11	KOZ	JPXK
12	NVX	WKUZ
13	REX	ZIBS
14	VJF	IVHX
15	XJH	YDXN
16	BHL	TGHP
17	ECJ	PJHA
18	KDF	XHON
19	LGT	PBVT
20	OWM	RJBP
21	QPG	SAML
22	TUP	PCEB
23	ZUW	HCIM
24	CFT	EHTW
25	HFV	FUCE
26	GEN	AXSS
27	MOB	EONS
28	NLZ	OKBH
29	RRK	ALIK
30	WQO	NCYS
31	XXW	MOEL
32	CAE	XBJQ
33	DOT	YENA
34	HYH	YKHJ
35	LAN	LPMK
36	OCS	GTDJ
37	TCZ	AJNE
38	UYS	WFLO
39	TTZ	JRPE
40	ALN	WLKI
41	CHM	ZERK
42	EGH	IXWH
43	HGX	BCAY
44	MOB	ZJOG
45		
46		
47		
48		
49		
50		
51	GJR	WOIU
52	LTF	YBHG
53	PJZ	NSGL
54	SAU	COHV
55	WRZ	AUPE
56	WXW	LRHG
57	AAC	JAHK
58	DBG	RXIT
59	FOV	ZBQO
60	DHN	IYPO
61	GXF	BNOP
62	JVF	NCBL
63	NPD	AHIR
64	QWO	MGAK
65	TTO	RZDK
66	TZU	WOXU
67	YJK	YMBW
68	ZQS	JPBL
69	AVX	BMCR
70	RVB	XQGS
71	GNV	JCDK
72	JNX	XDKL
73	LNZ	RIGX
74	NJX	QIUW
75	RTH	ZFKO
76	RVO	LRYP
77	TJD	DOLE
78	UDZ	MOHD
79	VBP	GNBU
80	YBC	BKHI
81	ZHR	RWOK
82	AZB	XDZW
83	FHP	UTPA
84	HTC	TIME
85	KPB	OKZU
86	MYM	OHVS
87	OHX	JNOU
88	QOY	LKVT
89	RKC	UTYO
90	VXU	WIZH
91	XBQ	OPQZ
92	YSY	YGOS
93	APB	TURV
94	BED	BOLH
95		
96		
97		
98		
99		
100		
101	PSJ	PQBR
102	RCV	BGVP
103	SYB	HRMT
104	UOX	ESQM
105	WKH	RCEI
106	XOB	UZCB
107	ZDD	WKPC
108	BEH	ATZI
109	DWB	LXPY
110	HKT	IGOR
111	KWH	TWOK
112	MKX	UDPT
113	OQF	ILVP
114	QJA	YHAE
115	SDX	THGN
116	TVQ	NFTX
117	WHF	ALWR
118	YDE	HPOQ
119	BUX	AGKT
120	EFN	RZVT
121	DRW	XIHS
122	GRZ	UBZY
123	JPZ	TSHN
124	LQC	NRTK
125	NDS	OYGN
126	PCT	IUQK
127	RNE	EHAP
128	VCZ	CGRS
129	YWX	WXKH
130	ART	QTEJ
131	CXB	PJLG
132	ELB	HXGD
133	GCL	BIZH
134	HBL	WQFJ
135	KCO	XMWF
136	LZM	URNO
137	NGV	JPIV
138	QEW	EVYJ
139	SHB	SRDQ
140	UYU	OVTO
141	WWU	XAUW
142	XNM	USMF
143	ZOQ	GYBE
144	AGJ	BUYC
145		
146		
147		
148		
149		
150		
151	MHV	XARG
152	NZO	BWØD
153	POE	HXVT
154	QQH	RUGT
155	RQK	WUDH
156	VLH	QNWO
157	WVT	AKSJ
158	XZY	PPIJ
159	CVZ	EXNV
160	AXZ	NGPO
161	EKQ	KOON
162	DPL	UAMN
163	FUB	XIYV
164	GVD	THRS
165	JZK	INLJ
166	KQH	QXZR
167	NCH	EDRG
168	OYV	CETQ
169	QHT	FRBL
170	QYQ	CKUT
171	TRM	SXZW
172	ULG	QAVP
173	WOM	JTWU
174	XFE	KBTQ
175	ZFH	PAJB
176	BBE	VIOA
177	COS	TNPD
178	FMT	DGOT
179	DMR	GSPL
180	GMU	WFFX
181	JAL	YGRY
182	KTK	NUZS
183	HME	IJOH
184	OOD	DLOG
185	QHZ	AVSY
186	RQJ	OHBX
187	SXB	UOSG
188	USO	PWQE
189	VRO	LKBA
190	BKN	ISXQ
191	KBX	GIOV
192	CTK	EUGL
193	HWF	RIGD
194	LJV	QOYR
195	OYO	MOVU
196		
197		
198		
199		
200		

202601341
25762403
39463732
69391

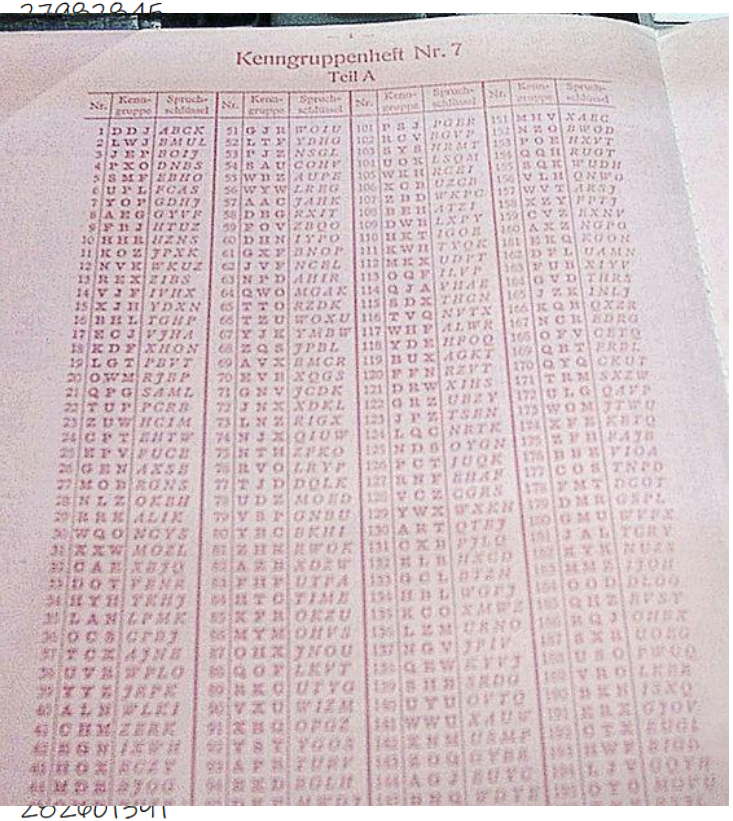
41202343
69866595
43855531
36533257
594817981
16998443
27082845

ENIGMA


Kenngruppenheft Nr. 7
Teil A

- Specjalne księgi zawierały ustawienia maszyny (m.in. pozycje startowe i kolejność wirników) na każdy dzień ważności księgi. Część tych danych była znana szyfrantom, część tylko oficerom.

25762403
39463732
69391

41202343
69866595
43855531
36533257
594817981
16998443

Kenngruppenheft Nr. 7
Teil A
202601541
25762403
39463732
69391

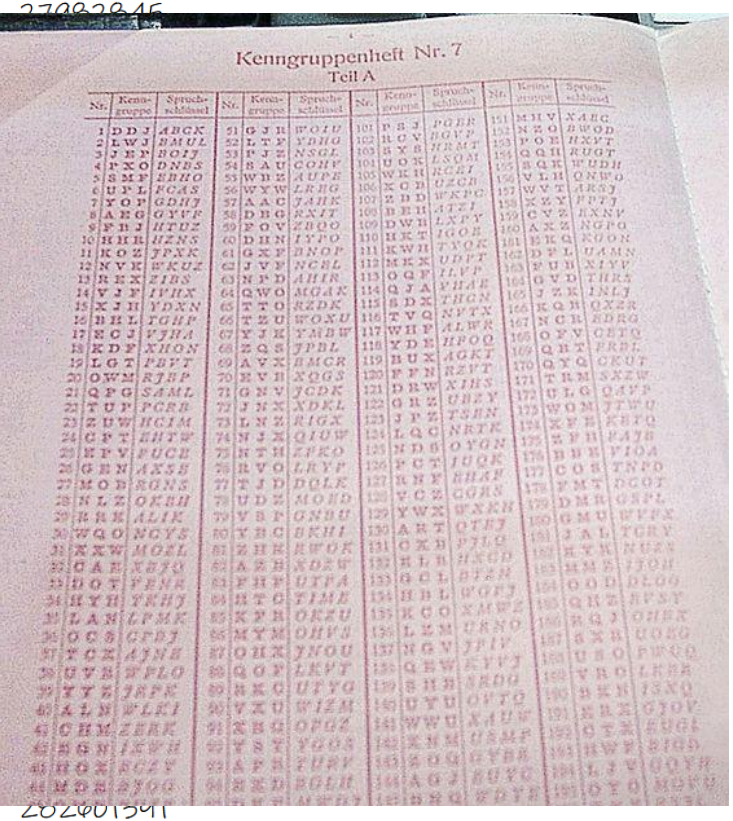
ENIGMA

- Specjalne księgi zawierały ustawienia maszyny (m.in. pozycje startowe i kolejność wirników) na każdy dzień ważności księgi. Część tych danych była znana szyfrantom, część tylko oficerom.

- Dodatkowo, każda depesza miała indywidualny klucz, nadawany na początku wiadomości dwukrotnie.

41202343
69866595
43855531
36533257
594817981
16998443
27082845

ENIGMA


Kenngruppenheft Nr. 7
Teil A

Nr.	Kenngruppe	Spruchschlüssel
1	DDJ	ABGK
2	LWJ	BMUL
3	JEP	BOIJ
4	PXO	DNBS
5	SMP	EBHO
6	UPL	FCAS
7	YOP	GDHJ
8	AEG	GYVF
9	FBJ	HTUZ
10	HHR	HZNS
11	KOZ	JPXK
12	NVX	WKUZ
13	REX	ZIBS
14	VJF	IVHX
15	XJH	YDXN
16	BHL	TGHP
17	ECJ	YJHA
18	KDF	XHON
19	LGT	PBVT
20	OWM	RJBP
21	QPG	SAML
22	TUP	PCRB
23	ZUW	HCIM
24	CFT	EHTW
25	EFV	FUCE
26	GEN	AXSS
27	MOB	RONS
28	NLZ	OKBH
29	RRK	ALIK
30	WQO	NCYS
31	XXW	MOZL
32	CAE	XBJQ
33	DOT	YFNA
34	HYH	YKHJ
35	LAN	LPMK
36	OCS	GTDJ
37	TCZ	AJNE
38	UYB	WPLO
39	TTZ	JRPE
40	ALN	WLKI
41	CHM	ZERK
42	EGH	IXVH
43	HOX	BCZY
44	MOB	JYQG
45	NLZ	PLBH
46	RRK	LIKA
47	WQO	CSYN
48	XXW	ZOLM
49	CAE	BQJX
50	DOT	HNAF
51	GJR	FOIU
52	LTF	YBHG
53	PJZ	NSGL
54	SAU	CONV
55	WBZ	AUPE
56	WXW	LRHG
57	AAC	JAHK
58	DBG	RXIT
59	EOV	ZBQO
60	DHN	IYPO
61	GXF	BNOP
62	JVY	NCBL
63	NPD	AHIR
64	QWO	MGAK
65	TTO	RZDK
66	TZU	WOXU
67	YJE	YMBW
68	ZQS	JPBL
69	AVX	BMCR
70	EVB	XQGS
71	GNV	JCDK
72	JNX	XDKL
73	LNZ	RIGX
74	NJX	QIUW
75	RTH	ZFKO
76	RVO	LRYP
77	TJD	DOLE
78	UDZ	MOHD
79	VBP	GNBU
80	YBC	BKHI
81	ZHR	RWOK
82	AEB	XOZW
83	FHP	UTFA
84	HTC	TIME
85	KPB	OKZU
86	MYM	OHVS
87	OHX	JNOU
88	QOY	LKVT
89	RKC	UTYO
90	VXU	WIZM
91	ZBQ	OPQZ
92	TST	YGOS
93	AFB	TURY
94	BED	BOLH
95	PSJ	PGBR
96	RCV	BGVP
97	SYB	HRMI
98	UOX	ESQM
99	WCH	RCAI
100	XCD	UZCB
101	ZDD	WKPC
102	BEU	ATFI
103	DWB	LXFY
104	HXT	IGOR
105	KWH	TYOK
106	MKX	UPFT
107	OQF	ILVP
108	QJA	YHAE
109	SDX	THGN
110	TVQ	NFTX
111	WHF	ALWR
112	YDE	HPOQ
113	BUX	AGKT
114	FFN	RZVT
115	DRW	XIHS
116	GRZ	UBZY
117	JFZ	TSEN
118	LQC	NRTK
119	NDS	OYGN
120	PCT	IUQK
121	RHE	EHAP
122	VCZ	CGRS
123	YWX	FXKH
124	ART	QTEJ
125	CXB	PJLG
126	ELR	HXCD
127	GCL	BIAN
128	HBL	WQFJ
129	KCO	XMWZ
130	LZM	UKNO
131	NGV	JPIV
132	QEW	EVYJ
133	SHB	SRDG
134	UYU	OVTO
135	WWU	XAUW
136	XNM	USMF
137	ZOQ	GYBE
138	AGJ	BUYC
139	BRD	IWZA
140	DVS	MFSL
141	MIV	XARG
142	NZO	BWOD
143	POE	HXVT
144	QQH	RUGT
145	SQK	WUDH
146	VLH	QNWO
147	WVT	AKSY
148	XZY	FPTJ
149	CVZ	EXNV
150	AXZ	NGPO
151	EKQ	KOON
152	DFL	UAMN
153	FUB	XIYV
154	GVD	THRS
155	JZK	INLJ
156	KQB	QXZR
157	NCH	EDRG
158	OYV	CETO
159	QBT	ZRBL
160	QYQ	CKUT
161	TRM	SXZW
162	ULG	QAVP
163	WOM	JTWU
164	XFE	KBTO
165	ZPB	PAJB
166	BHE	FIOA
167	COS	TNPD
168	FMT	DGOT
169	DMR	GSPL
170	GMU	WYFX
171	JAL	YGRY
172	KTK	NUZS
173	MME	IJOH
174	OOD	DLOG
175	QHZ	AVSY
176	RQJ	OHBX
177	SXB	UOSG
178	UBO	PWQC
179	VRO	LKBA
180	XKN	ISXQ
181	ZRX	GJOV
182	CTE	EUGI
183	HWF	RIGD
184	LJV	QOYH
185	OYQ	MOKU

- Specjalne księgi zawierały ustawienia maszyny (m.in. pozycje startowe i kolejność wirników) na każdy dzień ważności księgi. Część tych danych była znana szyfrantom, część tylko oficerom.

- Dodatkowo, każda depesza miała indywidualny klucz, nadawany na początku wiadomości dwukrotnie.

- Liczba stanów:

619 953 965 349 522 804 000 000

25762403
39463732
69391

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA A POLACY

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA A POLACY

- W 1929 r. na lotnisku w Warszawie pojawiła się paczka, która wzbudziła podejrzenia celników. Przez weekend dyskretnie otworzyli paczkę i zbadali jej zawartość.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA A POLACY

- W 1929 r. na lotnisku w Warszawie pojawiła się paczka, która wzbudziła podejrzenia celników. Przez weekend dyskretnie otworzyli paczkę i zbadali jej zawartość.

- Ponadto Biuro Szyfrów zdołało zdobyć komercyjny model ENIGMy.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
60931776
75033421
30982397
48515094
49091069
02698610
18627041
48808669
70564902
90365365
88674337
31720813
04105190
64254793
28260139
25762403
39463732
69391

ENIGMA A POLACY

- W 1929 r. na lotnisku w Warszawie pojawiła się paczka, która wzbudziła podejrzenia celników. Przez weekend dyskretnie otworzyli paczkę i zbadali jej zawartość.

- Ponadto Biuro Szyfrów zdołało zdobyć komercyjny model ENIGMy.

- Biuro Szyfrów nawiązało współpracę z Uniwersytetem Poznańskim oraz prof. Krygowskim z Instytutu Matematyki.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA A POLACY

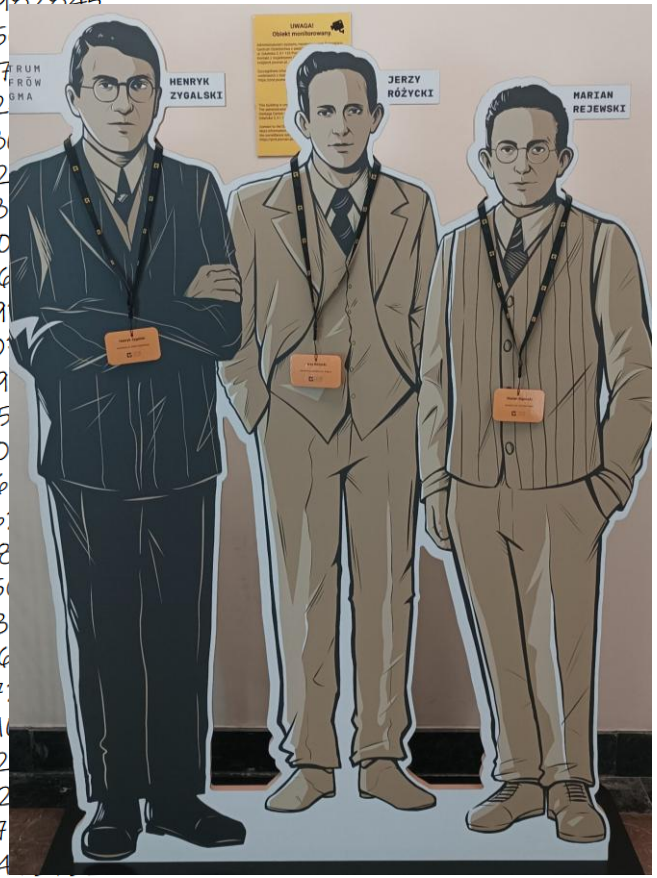
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ENIGMA A POLACY

- Prof. Krygowski wybrał zdolnych studentów, którzy uczestniczyli w kursie kryptologii, organizowanym przez Biuro Szyfrów na Cytadeli.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
455
387
652
198
042
418
420
886
609
750
309
485
490
026
186
488
705
903
886
317
041
642
282
257
394
69391

ENIGMA A POLACY

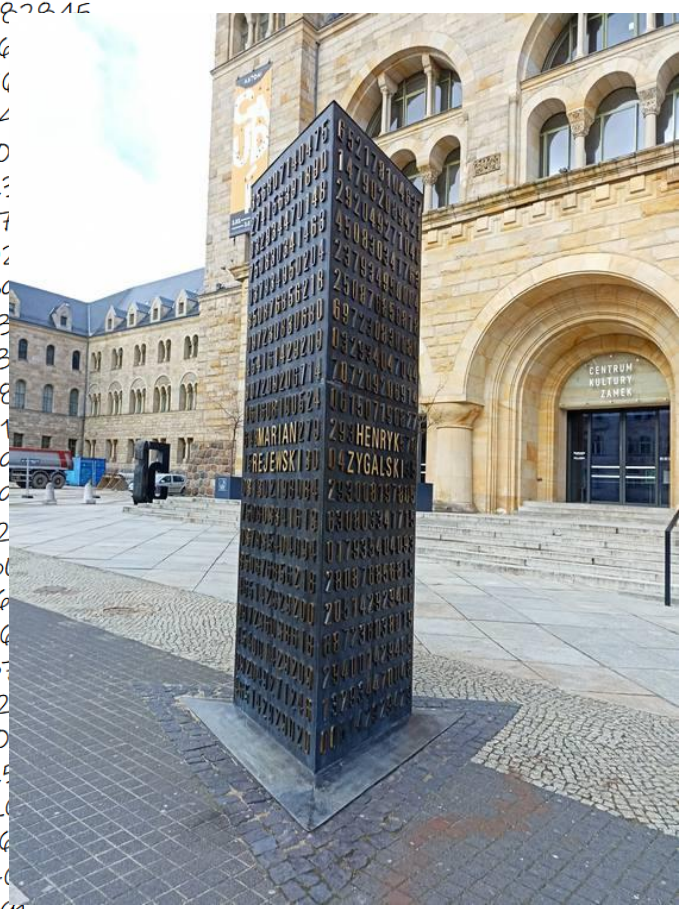


- Prof. Krygowski wybrał zdolnych studentów, którzy uczestniczyli w kursie kryptologii, organizowanym przez Biuro Szyfrów na Cytadeli.

- Na przełomie 1932 i 1933 r. Marian Rejewski złamał pierwszy szyfrogram ENIGMy. W dalszych sukcesach pomogli mu Henryk Żygalski i Jerzy Różycki.

41202343
69866595
43855531
36533257
594817981
16998443
279
455
387
652
198
042
418
420
886
609
750
309
485
490
026
186
488
705
903
886
317
041
642
282
257
394
693

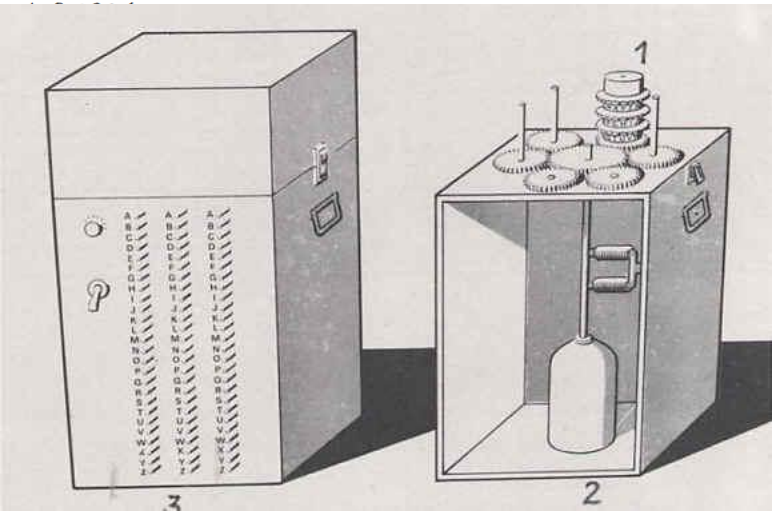
ENIGMA A POLACY



- Stopniowo Niemcy udoskonalali Enigmę.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618

ENIGMA A POLACY



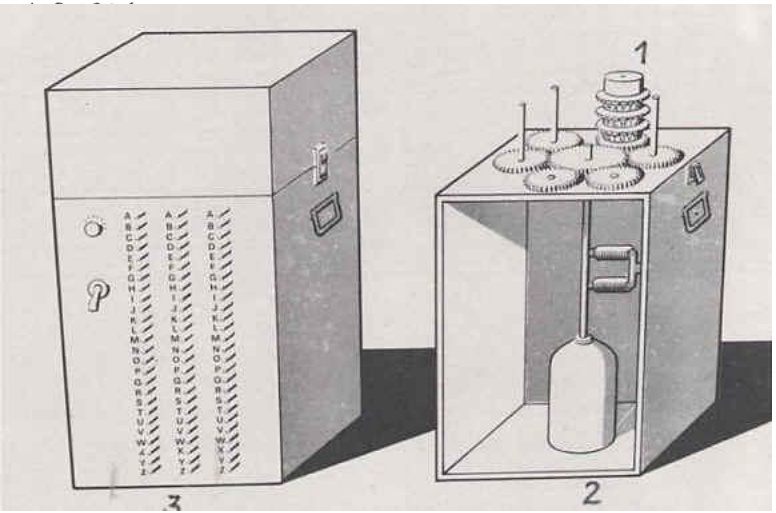
041051908
64254793
282601391
25762403
39463732
69391

- Stopniowo Niemcy udoskonalali Enigmę.

- W odpowiedzi na to, poznański kryptolodzy stworzyli „bombę" kryptograficzną - urządzenie mechaniczno-elektryczne do automatycznego łamania szyfrogramów.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618

ENIGMA A POLACY



041051908
64254793
282601391
25762403
39463732
69391

- Stopniowo Niemcy udoskonalali Enigmę.

- W odpowiedzi na to, poznański kryptolodzy stworzyli „bombę" kryptograficzną - urządzenie mechaniczno-elektryczne do automatycznego łamania szyfrogramów.

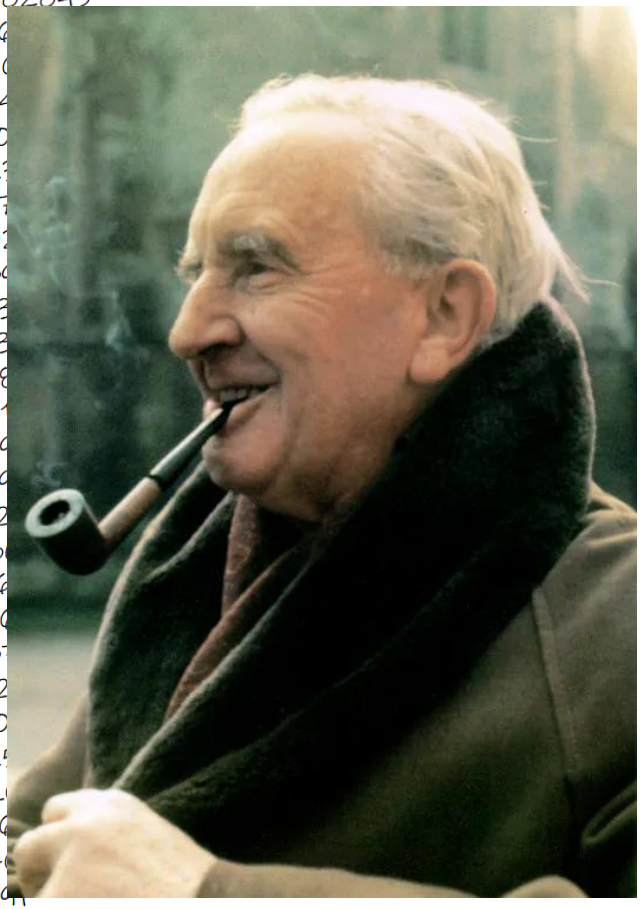
- Z początkiem wojny członkowie Biura Szyfrów musieli uciekać z Polski. Po licznych perypetiach udało im się przekazać zdobytą wiedzę sojusznikom.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

BLETCHLEY PARK

41202343
69866595
43855531
36533257
594817981
16998443
27982845
455
387
652
198
042
418
420
886
609
750
309
485
490
026
186
488
705
903
886
317
041
642
282
257
394
693

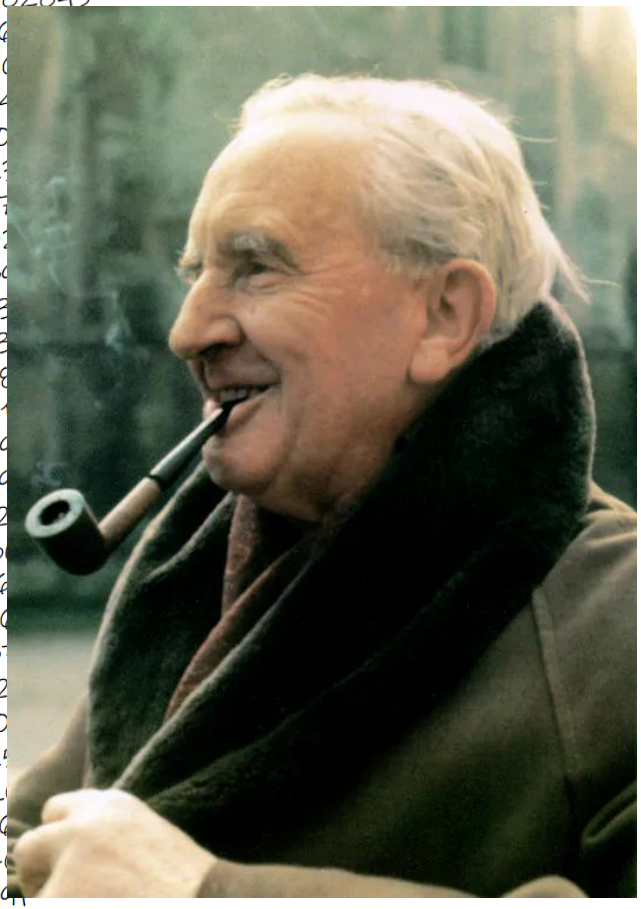
BLETCHLEY PARK



- Brytyjczycy zaczęli kompletować zespół kryptologiczny tuż przed wojną. Początkowo mieli przekonanie, że powinni zajmować się tym germaniści, filolodzy, historycy sztuki, itp. Kandydatem był m.in. ...

41202343
69866595
43855531
36533257
594817981
16998443
27982845
455
387
652
198
042
418
420
886
609
750
309
485
490
026
186
488
705
903
886
317
041
642
282
257
394
693

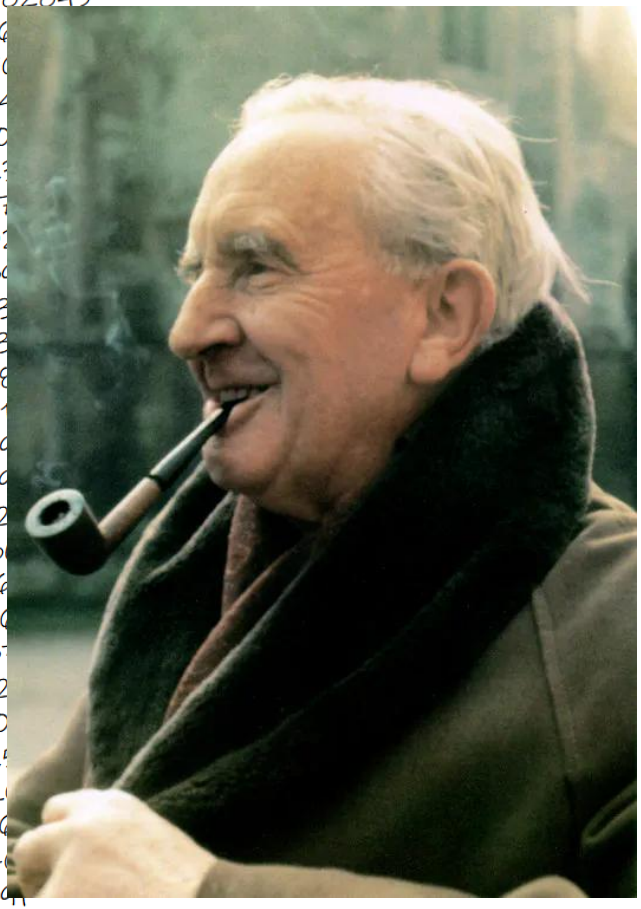
BLETCHLEY PARK



- Brytyjczycy zaczęli kompletować zespół kryptologiczny tuż przed wojną. Początkowo mieli przekonanie, że powinni zajmować się tym germaniści, filolodzy, historycy sztuki, itp. Kandydatem był m.in. ... Tolkien

41202343
69866595
43855531
36533257
594817981
16998443
27982845
455
387
652
198
042
418
420
886
609
750
309
485
490
026
186
488
705
903
886
317
041
642
282
257
394
693

BLETCHLEY PARK

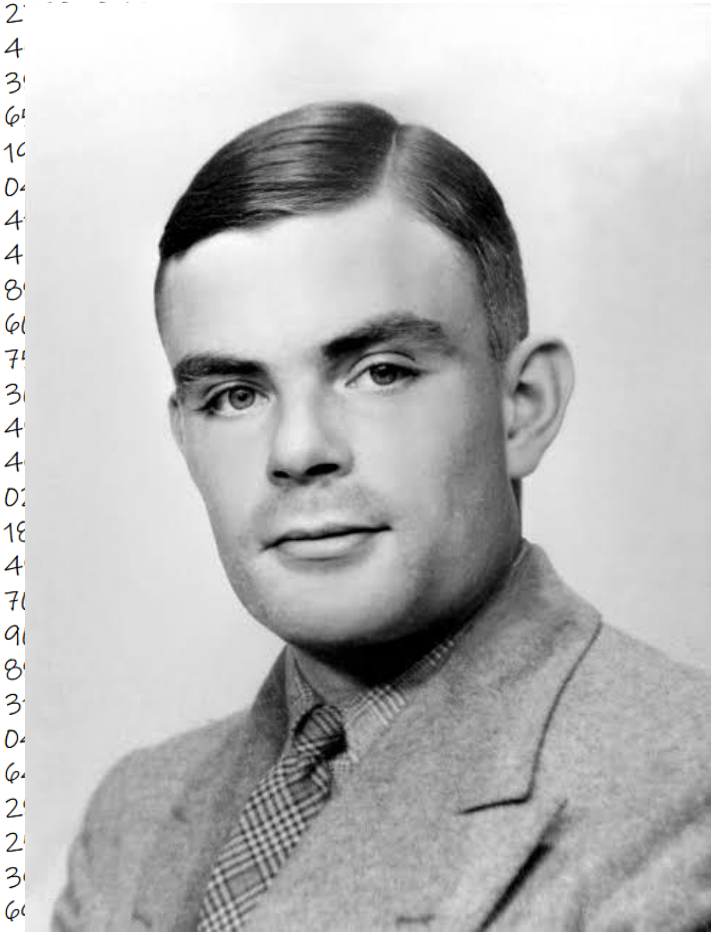


- Brytyjczycy zaczęli kompletować zespół kryptologiczny tuż przed wojną. Początkowo mieli przekonanie, że powinni zajmować się tym germaniści, filolodzy, historycy sztuki, itp. Kandydatem był m.in. ... Tolkien

- Osoby ścisłe były uważane za „dziwnych i całkowicie niepraktycznych facetów", mówiono też o „godnej pożałowania konieczności ich zatrudnienia".

41202343
69866595
43855531
36533257
594817981
16998443

BLETCHLEY PARK



- Brytyjczycy zaczęli kompletować zespół kryptologiczny tuż przed wojną. Początkowo mieli przekonanie, że powinni zajmować się tym germaniści, filolodzy, historycy sztuki, itp. Kandydatem był m.in. ... Tolkien

- Osoby ścisłe były uważane za „dziwnych i całkowicie niepraktycznych facetów", mówiono też o „godnej pożałowania konieczności ich zatrudnienia".

- Czterech matematyków, w tym Alan Turing.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

BLETCHLEY PARK

Siedziba – posiadłość Bletchley Park pod Londynem.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

BLETCHLEY PARK

Turing i jego zespół udoskonalili metody poznaniaków, konstruując nowe wersje „bomb" kryptograficznych.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

BLETCHLEY PARK

- W szczytowym momencie w BP pracowało ok. 10 tysięcy osób (większość: kobiety),

- Informacje zdobyte dzięki złamaniu Enigmy miały kluczowe znaczenie m.in. w bitwie o Atlantyk.

- Turing – „ojciec komputerów”.

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

TERAŹNIEJSZOŚĆ

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Przypomnijmy szyfr Cezara:

KOT

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

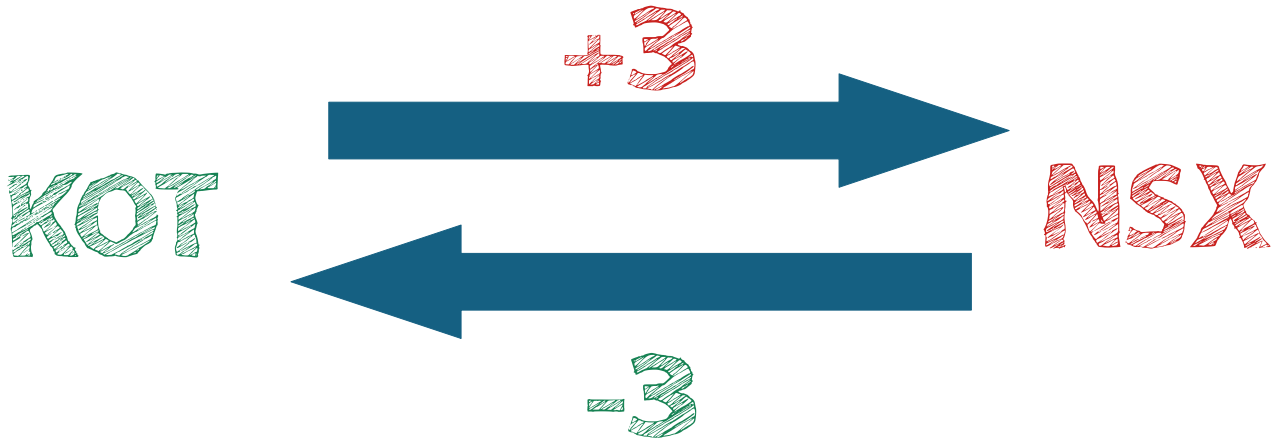
Przypomnijmy szyfr Cezara:

klucz +3 służył do szyfrowania wiadomości,

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Przypomnijmy szyfr Cezara:



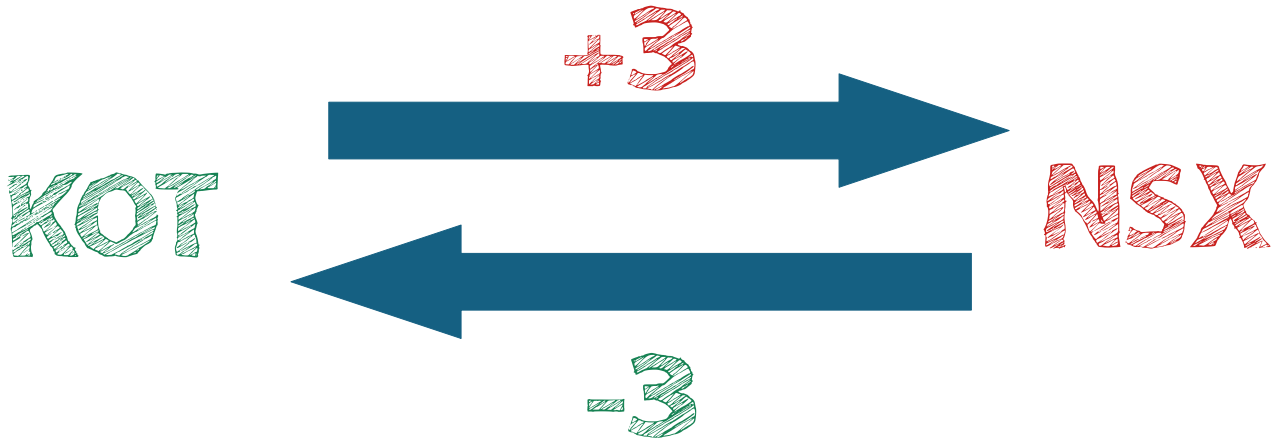
klucz +3 służył do szyfrowania wiadomości,

zaś klucz -3 do deszyfrowania szyfrogramu.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Przypomnijmy szyfr Cezara:



klucz +3 służył do szyfrowania wiadomości,

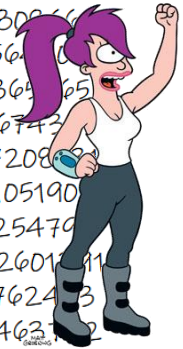
zaś klucz -3 do deszyfrowania szyfrogramu.

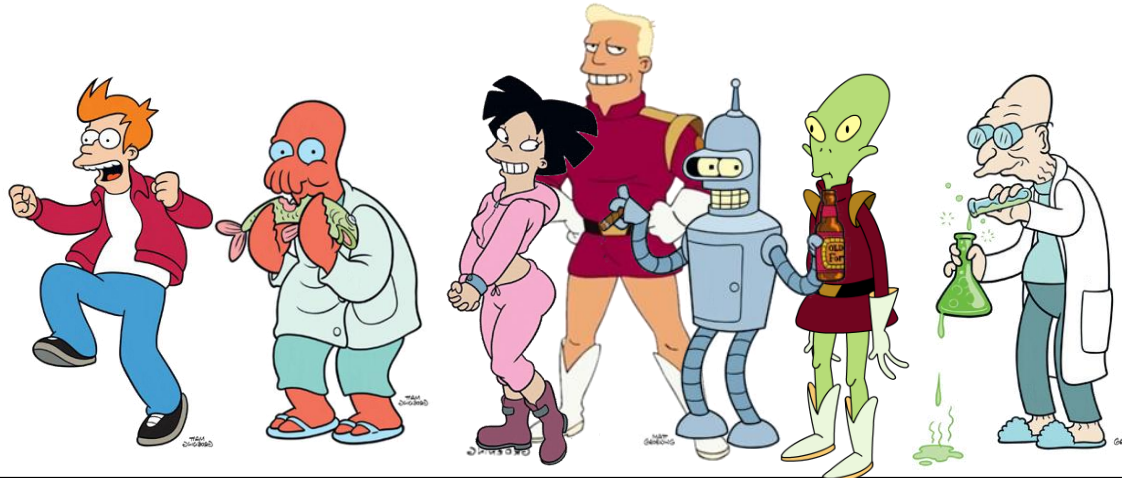
W tym wypadku, znając klucz szyfrujący, bardzo łatwo „obliczyć" klucz deszyfrujący!

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.

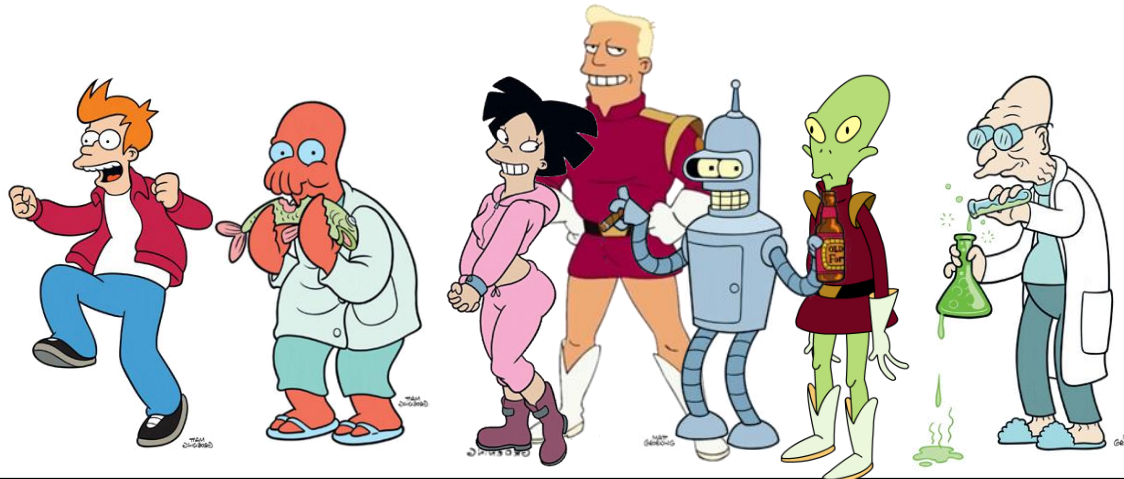




KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

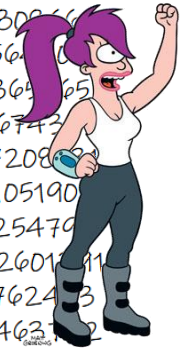
- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.

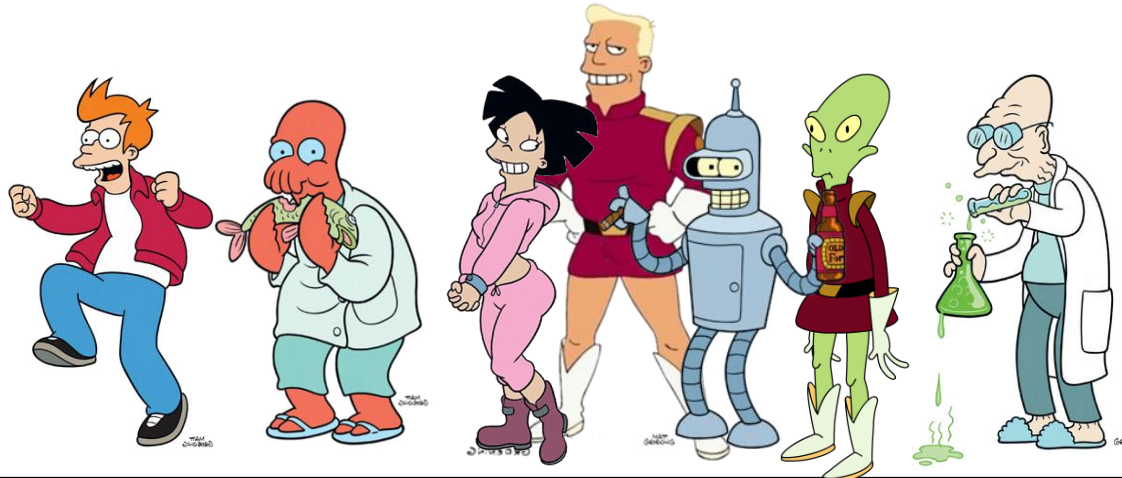


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.

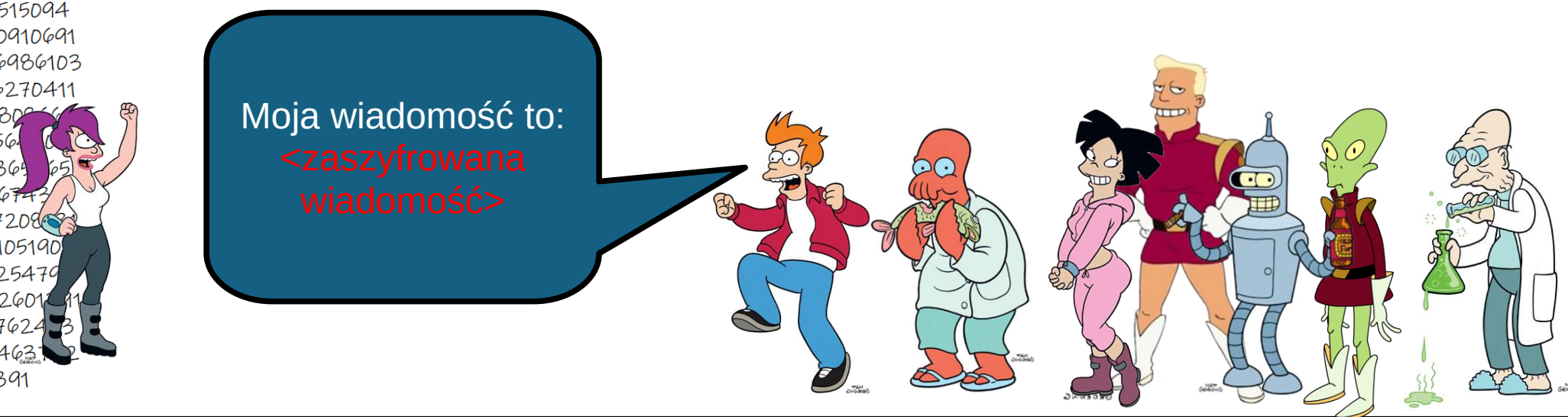




KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

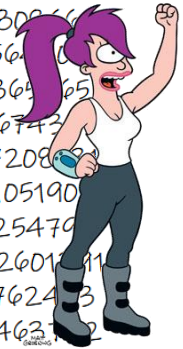
- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.

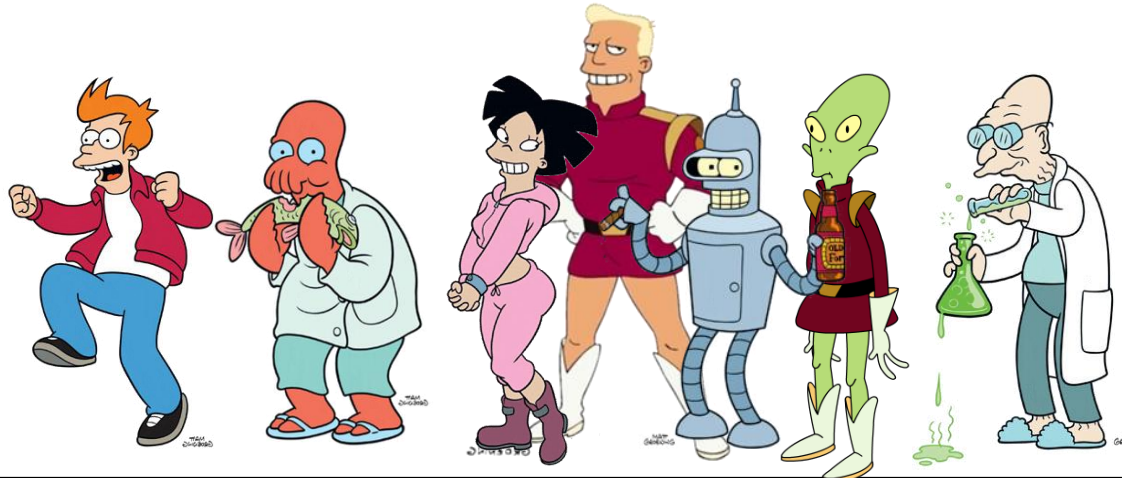


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.





KLUCZ PUBLICZNY, KLUCZ PRYWATNY

W kryptografii klucza publicznego również istnieją dwa klucze:

- publiczny (do szyfrowania) – znany wszystkim,
- prywatny (do deszyfrowania wiadomości) – znany tylko odbiorcy.

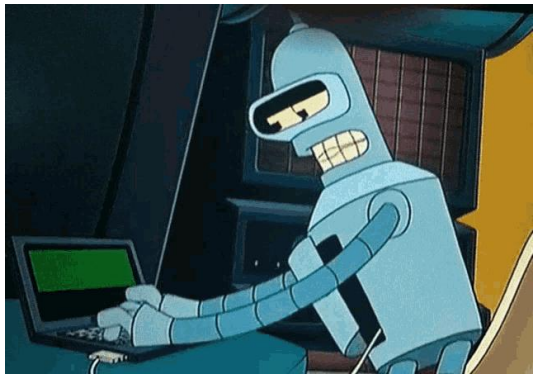
KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

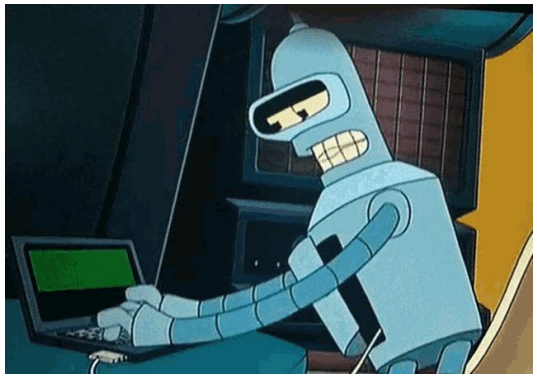
- W teorii zawsze z klucza publicznego możemy otrzymać klucz prywatny.



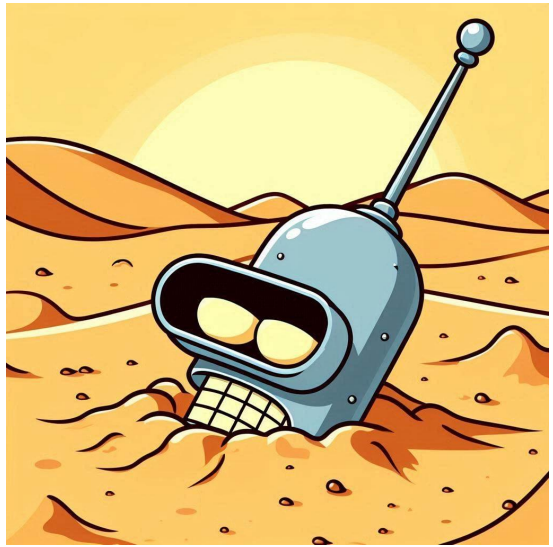
41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

- W teorii zawsze z klucza publicznego możemy otrzymać klucz prywatny.
- W praktyce zajęło by to jednak miliony lat!



MILIONY LAT



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Aby stworzyć kryptosystem z kluczem publicznym, zawsze potrzebny jest problem matematyczny:

41202343
698666595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Aby stworzyć kryptosystem z kluczem publicznym, zawsze potrzebny jest problem matematyczny:

operacja, którą można szybko wykonać,
ale której odwrócenie zajmuje wieki.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Aby stworzyć kryptosystem z kluczem publicznym, zawsze potrzebny jest problem matematyczny:

operacja, którą można szybko wykonać, ale której odwrócenie zajmuje wieki.

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Aby stworzyć kryptosystem z kluczem publicznym, zawsze potrzebny jest problem matematyczny:

operacja, którą można szybko wykonać, ale której odwrócenie zajmuje wieki.

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

Aby stworzyć kryptosystem z kluczem publicznym, zawsze potrzebny jest problem matematyczny:

operacja, którą można szybko wykonać, ale której odwrócenie zajmuje wieki.

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Nie wiemy na 100%, czy jakakolwiek taka operacja istnieje. Dotyczy tego hipoteza P kontra NP (warta 1 000 000 $). Przedstawimy kilka przykładów operacji, które prawdopodobnie mają tą własność.

LICZBY PIERWSZE

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Pierwszy przykład takiej operacji związany jest z liczbami pierwszymi (takimi, które mają tylko dwa dzielniki – jedynkę oraz samą siebie):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Pierwszy przykład takiej operacji związany jest z liczbami pierwszymi (takimi, które mają tylko dwa dzielniki – jedynkę oraz samą siebie):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

Przemnożenie przez siebie dwóch liczb pierwszych

zajmuje mało czasu:

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Pierwszy przykład takiej operacji związany jest z liczbami pierwszymi (takimi, które mają tylko dwa dzielniki – jedynkę oraz samą siebie):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

Przemnożenie przez siebie dwóch liczb pierwszych

zajmuje mało czasu:

$$34359738337 \times 34359738319$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Pierwszy przykład takiej operacji związany jest z liczbami pierwszymi (takimi, które mają tylko dwa dzielniki – jedynkę oraz samą siebie):

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

Przemnożenie przez siebie dwóch liczb pierwszych

zajmuje mało czasu:

$$34359738337 \times 34359738319 = 1180591617968632235503$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Rozkład na czynniki jest o wiele trudniejszym zadaniem:

$$11805916179686322235503 = ? \times ?$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Rozkład na czynniki jest o wiele trudniejszym zadaniem:

$$11805916179686322235503 = ? \times ?$$

(potrzebujemy $\sqrt{11805916179686322235503}$ dzieleń).

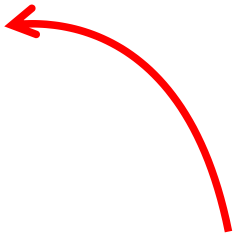
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

LICZBY PIERWSZE

Rozkład na czynniki jest o wiele trudniejszym zadaniem:

$$1180591617968632235503 = ? \times ?$$

(potrzebujemy $\sqrt{1180591617968632235503}$ dzieleń).



Ta liczba jest iloczynem dwóch liczb pierwszych. Nikt na świecie (oprócz RSA Security) nie wie jakich! Do niedawna za znalezienie czynników tej liczby wygrać można było 75 000 $. Ma ona 270 cyfr.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

GRUPY

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

GRUPY

Grupą nazywamy zbiór G wraz z działaniem

$$*: G \times G \to G,$$

które spełnia następujące własności:

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

GRUPY

Grupą nazywamy zbiór G wraz z działaniem

$$*: G \times G \to G,$$

które spełnia następujące własności:

(1) **(łączność)** dla dowolnych $a, b, c \in G$:

$$(a*b)*c = a*(b*c),$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

GRUPY

Grupą nazywamy zbiór G wraz z działaniem

$$*: G \times G \to G,$$

które spełnia następujące własności:

(1) **(łączność)** dla dowolnych $a, b, c \in G$:

$$(a*b)*c = a*(b*c),$$

(2) **(istnienie elementu neutralnego)** istnieje $e \in G$ takie, że dla dowolnego $a \in G$:

$$a*e = e*a = a,$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

GRUPY

Grupą nazywamy zbiór G wraz z działaniem

$$*: G \times G \to G,$$

które spełnia następujące własności:

(1) **(łączność)** dla dowolnych $a, b, c \in G$:

$$(a*b)*c = a*(b*c),$$

(2) **(istnienie elementu neutralnego)** istnieje $e \in G$ takie, że dla dowolnego $a \in G$:

$$a*e = e*a = a,$$

(3) **(istnienie elementu odwrotnego)** dla każdego $a \in G$ istnieje $a^{-1} \in G$ takie, że

$$a^{-1}*a = a*a^{-1} = e.$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

PRZYKŁADY GRUP

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

PRZYKŁADY GRUP

(1) Zbiór liczb całkowitych z działaniem +.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

PRZYKŁADY GRUP

(1) Zbiór liczb całkowitych z działaniem +.

(2) Zbiór liczb rzeczywistych **bez zera** z działaniem mnożenia.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

PRZYKŁADY GRUP

(1) Zbiór liczb całkowitych z działaniem +.

(2) Zbiór liczb rzeczywistych **bez zera** z działaniem mnożenia.

(3) Zbiór liczb naturalnych z działaniem mnożenia **nie jest grupą**, bo 2 nie ma swojej odwrotności!

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

13 + 50 = 63

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

13 + 50 = 63 ----> 63 - 24 = 39

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

13 + 50 = 63 ----> 63 - 24 = 39 -----> 39 - 24 =15

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

$13 + 50 = 63 \dashrightarrow 63 - 24 = 39 \dashrightarrow 39 - 24 = 15$

W ten sposób dodaliśmy 13 oraz 30 **modulo 24:**

(Równoważnie: policzyliśmy resztę z dzielenia przez 24).

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DODAWANIE MODULO 24

Załóżmy, że jest 13:00. Jaka godzina będzie za 50 godzin?

$13 + 50 = 63$ ----> $63 - 24 = 39$ -----> $39 - 24 = 15$

W ten sposób dodaliśmy 13 oraz 30 **modulo 24:**

(Równoważnie: policzyliśmy resztę z dzielenia przez 24).

Zbiór „godzin" : {0, 1, 2, ..., 23}

wraz z działaniem dodawania modulo 24 jest grupą.

MNOŻENIE MODULO 24

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

MNOŻENIE MODULO 24

Podobnie można mnożyć liczby modulo 24:

$$10 * 30 \text{ modulo } 24 = 300 \text{ modulo } 24$$

$$= (300 - 24 - \ldots - 24) \text{ modulo } 24 = 12$$

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

MNOŻENIE MODULO 24

Podobnie można mnożyć liczby modulo 24:

$$10 * 30 \text{ modulo } 24 = 300 \text{ modulo } 24$$
$$= (300 - 24 - \ldots - 24) \text{ modulo } 24 = 12$$

Zbiór

z działaniem mnożenia modulo 24 jest grupą.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

MNOŻENIE MODULO 24

Podobnie można mnożyć liczby modulo 24:

$$10 * 30 \text{ modulo } 24 = 300 \text{ modulo } 24$$
$$= (300 - 24 - \ldots - 24) \text{ modulo } 24 = 12$$

Zbiór

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23\}$$

z działaniem mnożenia modulo 24 jest grupą.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

MNOŻENIE MODULO 24

Podobnie można mnożyć liczby modulo 24:

$$10 * 30 \text{ modulo } 24 = 300 \text{ modulo } 24$$
$$= (300 - 24 - \ldots - 24) \text{ modulo } 24 = 12$$

Zbiór

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,$$
$$14, 15, 16, 17, 18, 19, 20, 21, 22, 23\}$$

z działaniem mnożenia modulo 24 jest grupą.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

MNOŻENIE MODULO 24

Podobnie można mnożyć liczby modulo 24:

$$10 * 30 \text{ modulo } 24 = 300 \text{ modulo } 24$$
$$= (300 - 24 - \ldots - 24) \text{ modulo } 24 = 12$$

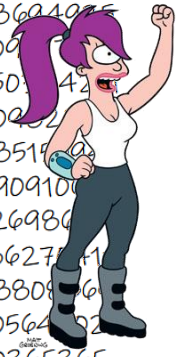
Zbiór

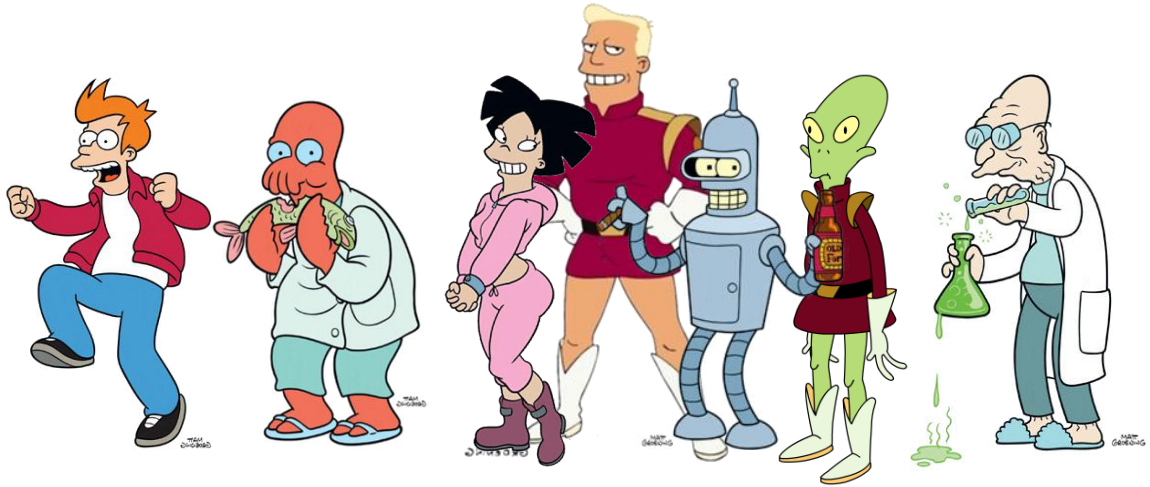
$$\{1, 5, 7, 11, 13, 17, 19, 23\}$$

z działaniem mnożenia modulo 24 jest grupą.

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

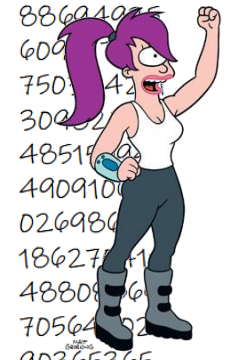
41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
903653[illegible]
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391



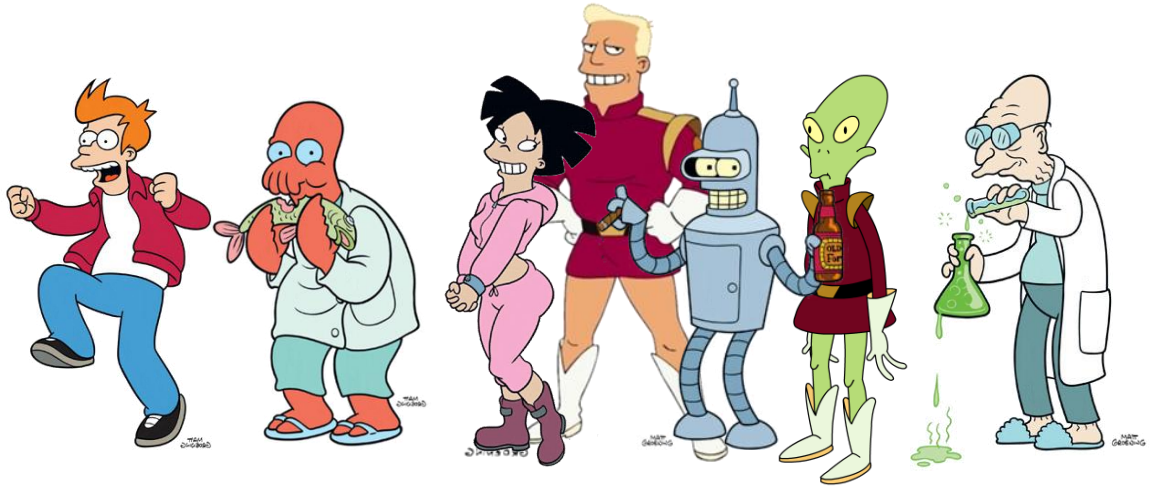


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
903365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

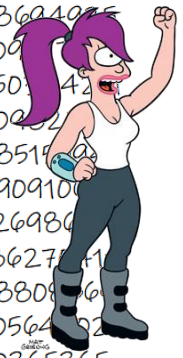


Fry, zaszyfruj wiadomość do mnie, podnosząc ją do potęgi e = 7 modulo 33!



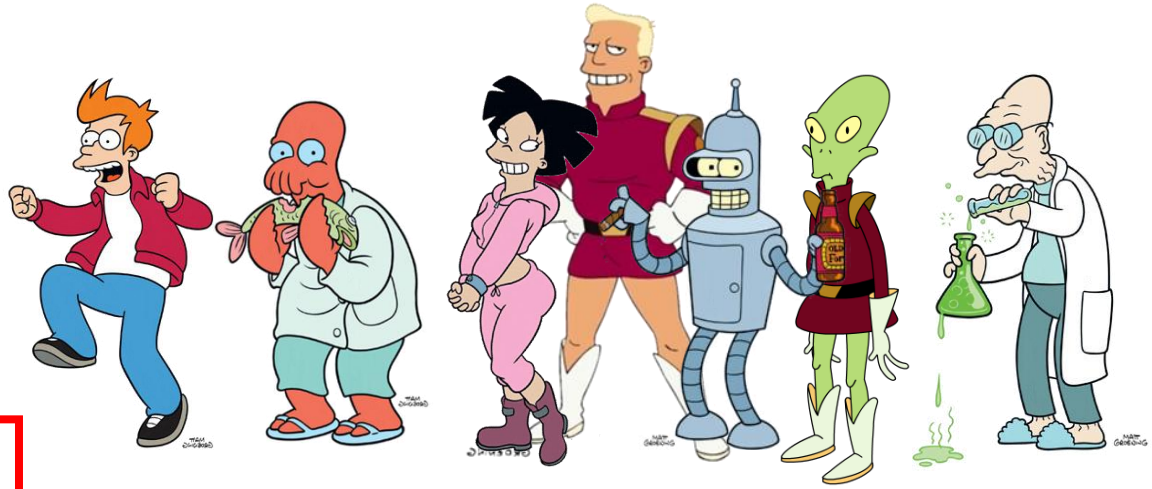
KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391



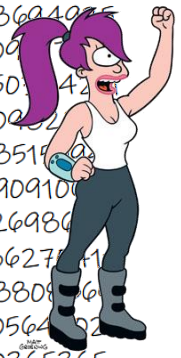
Fry, zaszyfruj wiadomość do mnie, podnosząc ją do potęgi e = 7 modulo 33!

Iloczyn dwóch liczb pierwszych



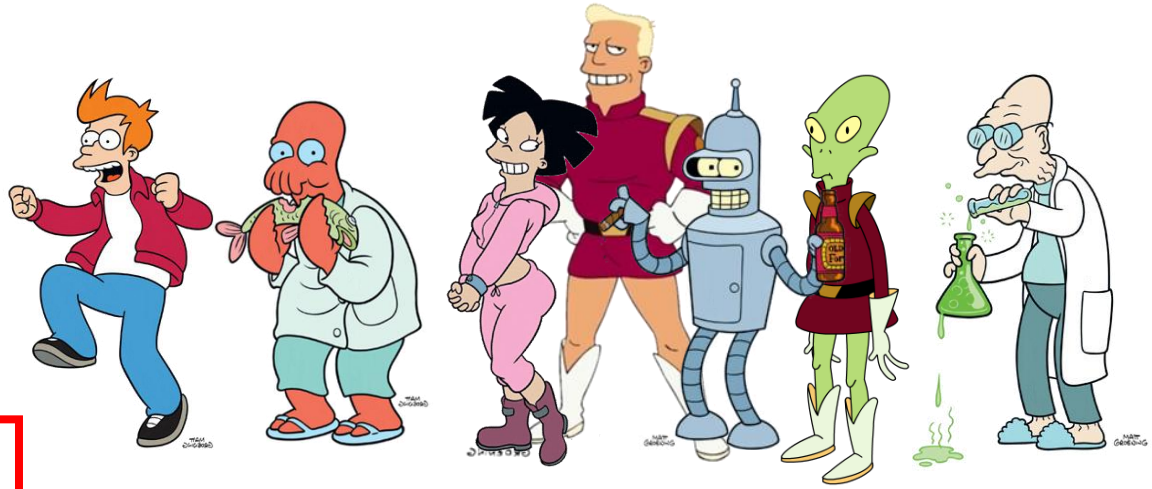
KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391



Fry, zaszyfruj wiadomość do mnie, podnosząc ją do potęgi e = 7 modulo 33!

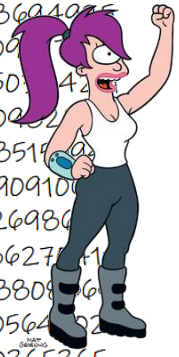
Dowolna (prawie) liczba

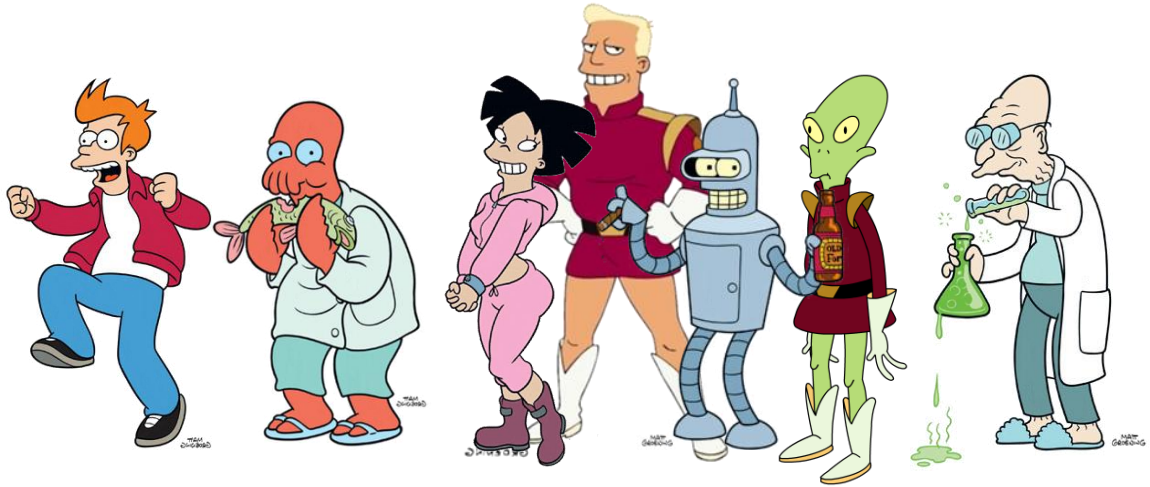


Iloczyn dwóch liczb pierwszych

KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
903653[illegible]
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

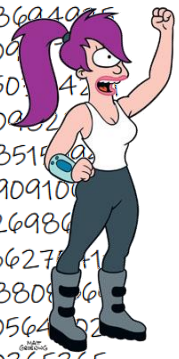


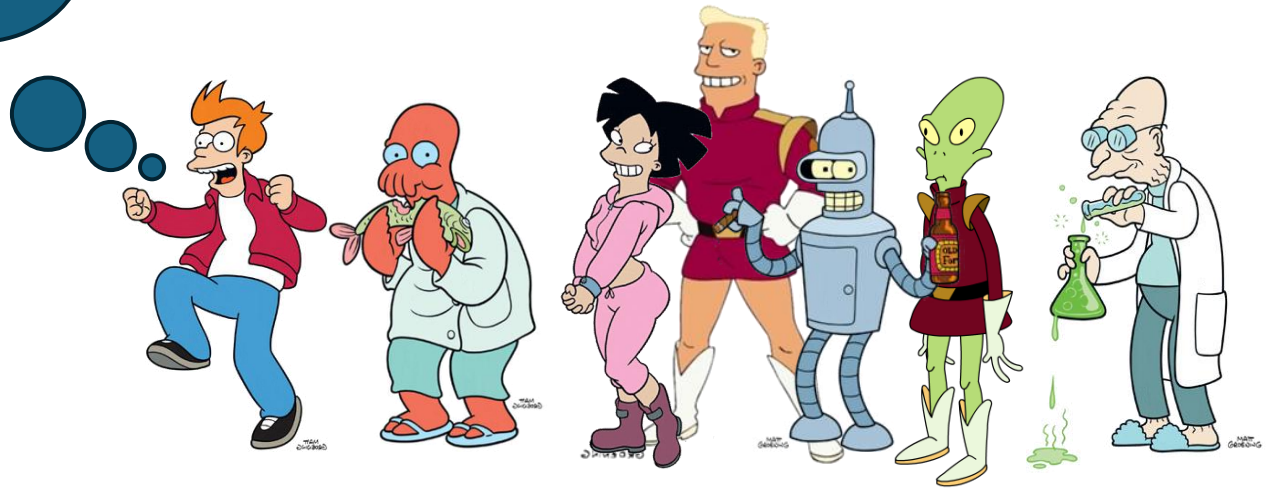


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

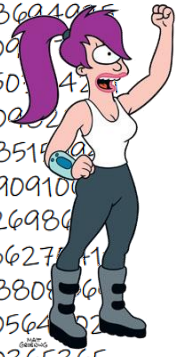
Moja wiadomość to 2. Zatem szyfrogram to:
$2^7 \bmod 33 = 29$

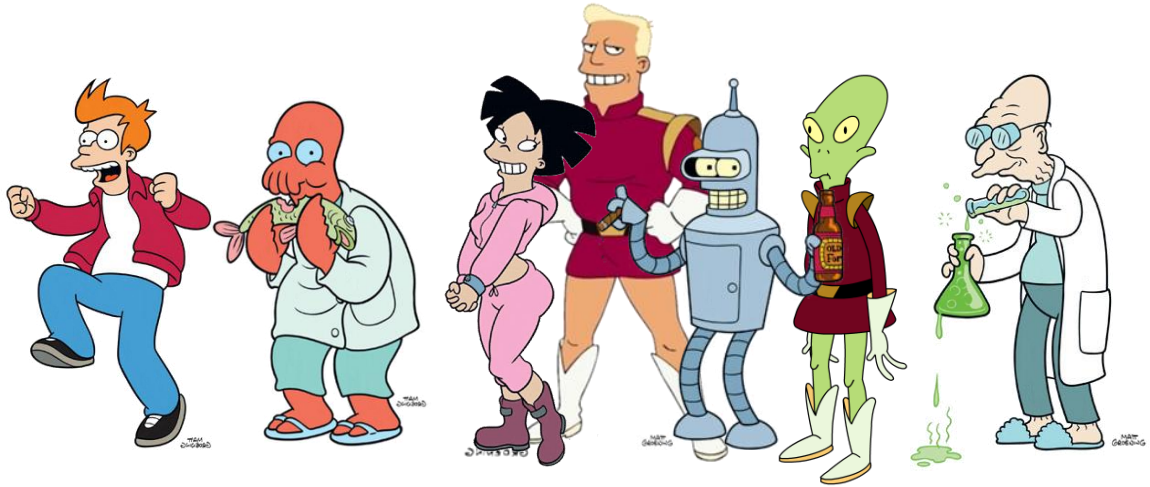




KLUCZ PUBLICZNY, KLUCZ PRYWATNY

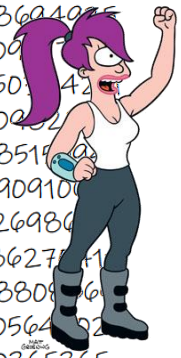
41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
903653[illegible]
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391



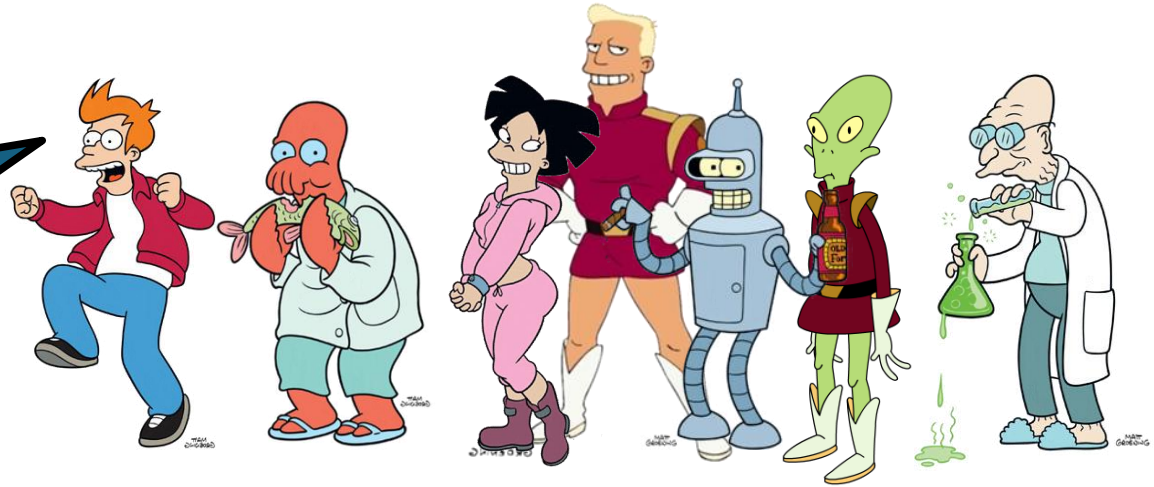


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

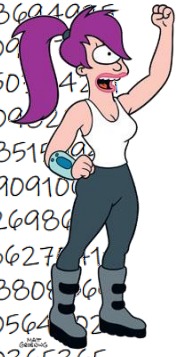


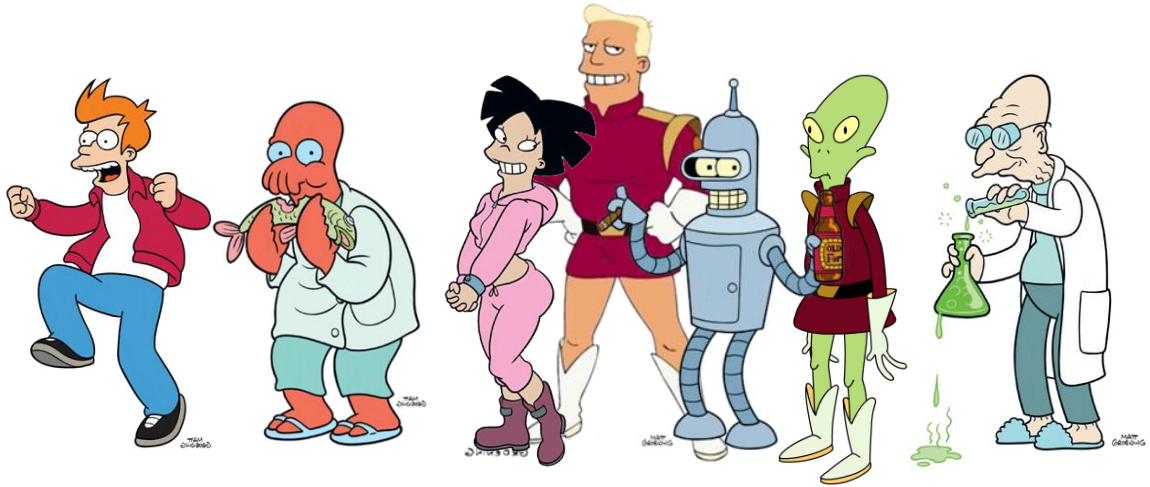
Moja zaszyfrowana wiadomość to:
29!



KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
903653[illegible]
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

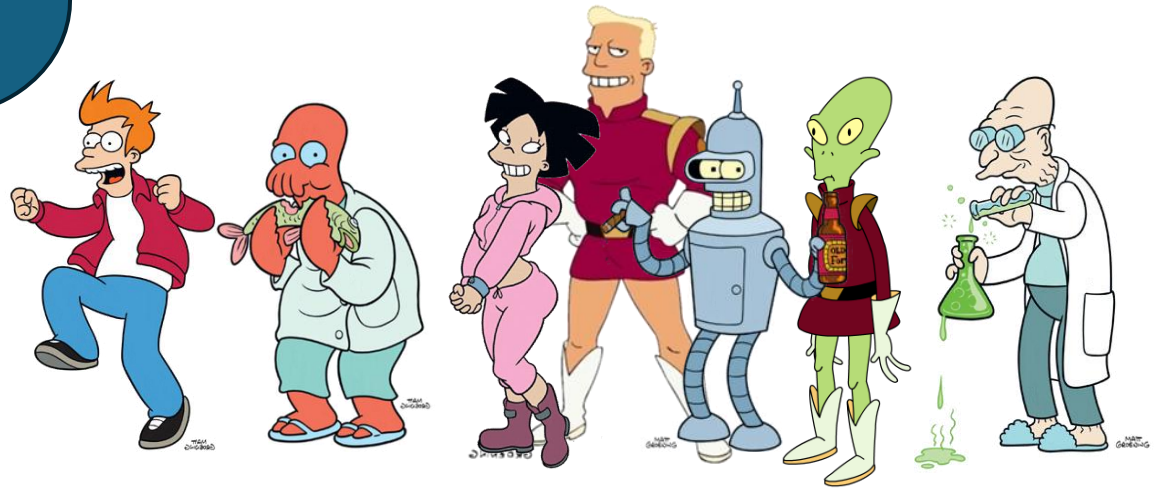




KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

Mój klucz prywatny to
d = 3.
Zatem wiadomość Fry'a
to:
$29^3 \bmod 33 = 2$.

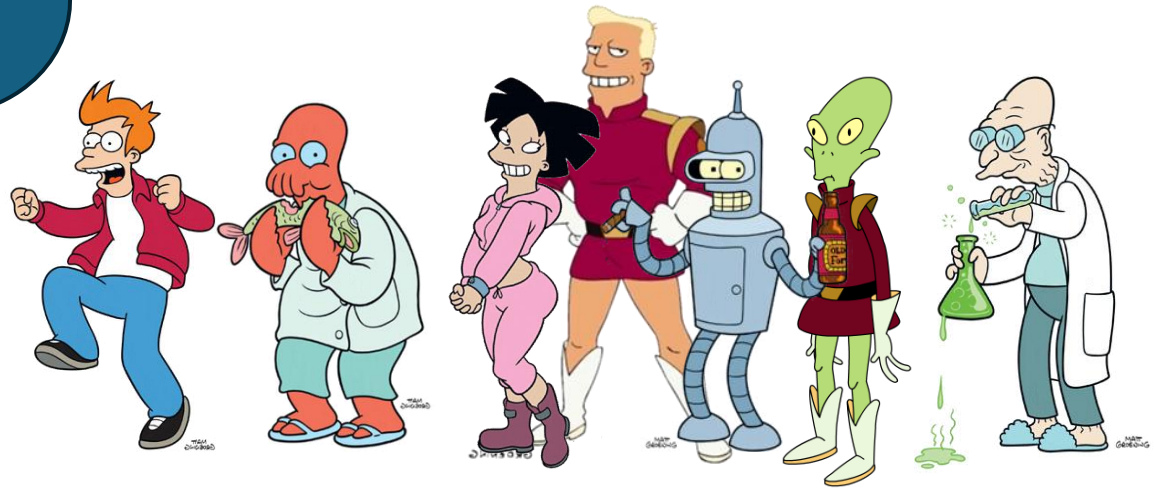


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
903065365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

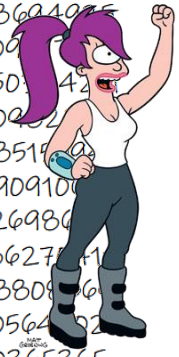
Mój klucz prywatny to d = 3.
Zatem wiadomość Fry'a to:
$29^3 \bmod 33 = 2$.

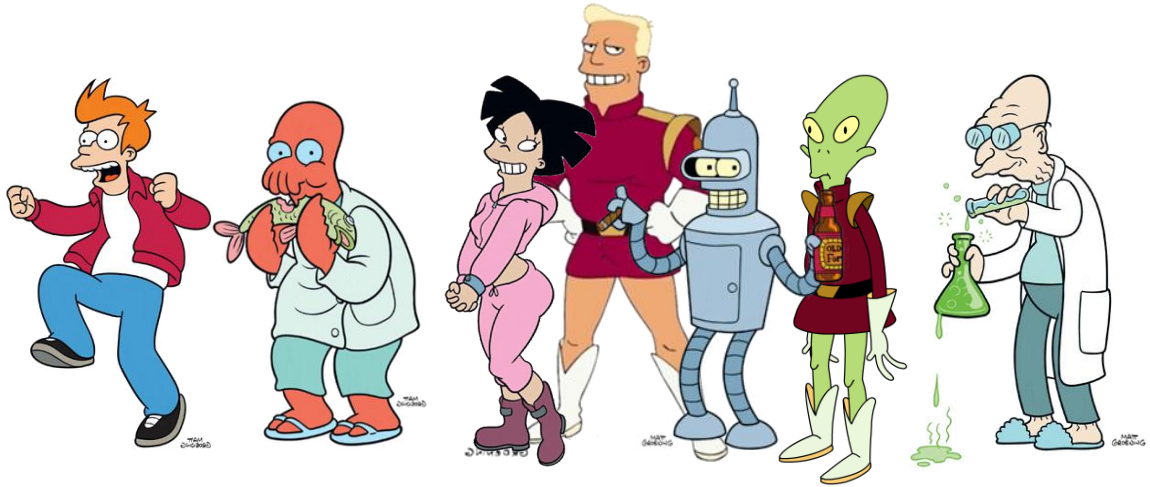
Leila może obliczyć d, znając p oraz q!



KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
[illegible]
[illegible]
[illegible]
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
903653[illegible]
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391



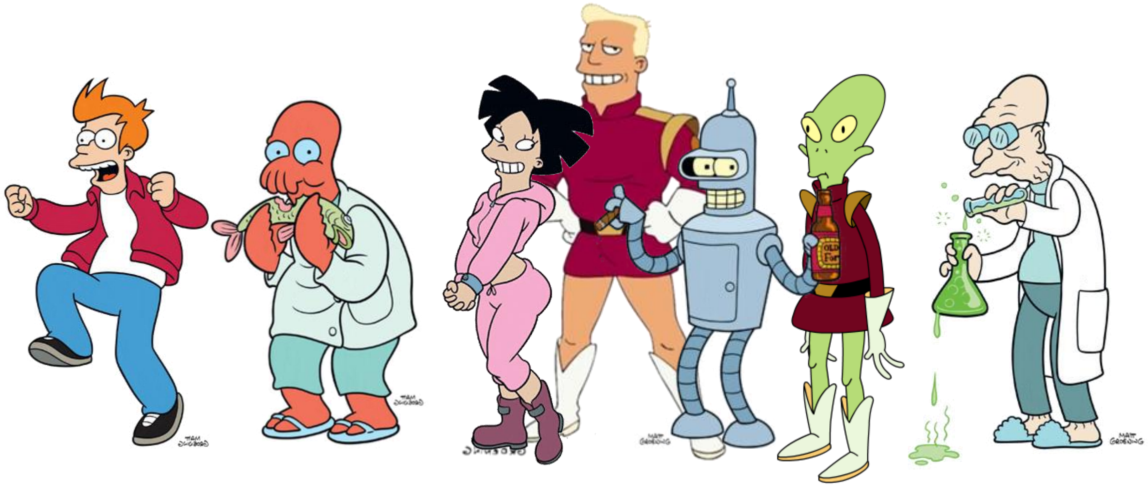


KLUCZ PUBLICZNY, KLUCZ PRYWATNY

41202343
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718

90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

Fry, zaszyfruj
wiadomość do mnie,
podnosząc ją do potęgi
e = 783217898931
modulo
41202343698665954385553136
53325759481798116998443279
82845455626433876445565248
42619809887042316184187926
14202471888694925609317763
75033421130982397485150944
90910691026986103186270411
48808669705649029036536588
67433731720813104105190864
25479328260139125762403394
63732693391!



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
7503342
309823
48515
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

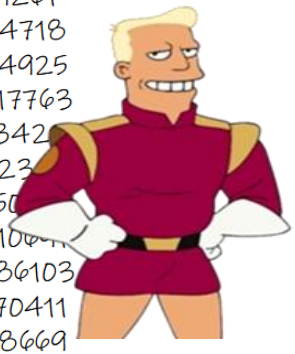
KLUCZ ROZDZIELONY

Chcemy, by mogli uruchomić rakietę tylko po wspólnej decyzji!

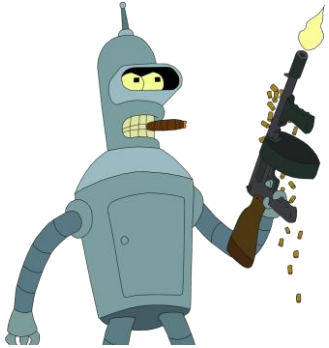
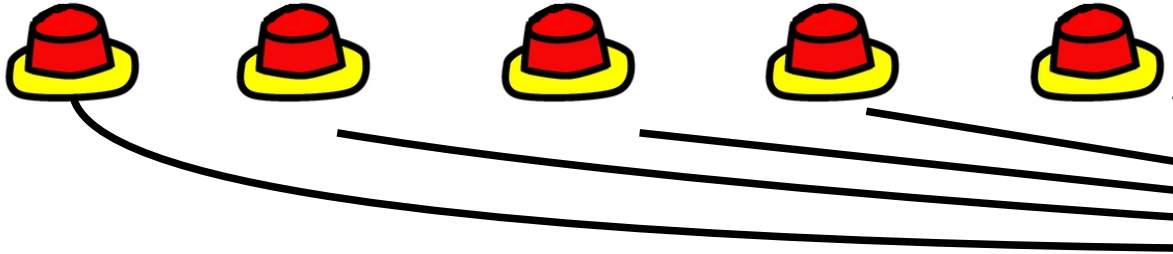
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
7503342
309823
48515
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY

74 92 04 73 92





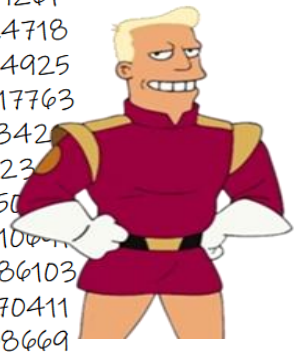




41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
652484260
14809887
04231618
41879261
42024718
88694925
609317763
7503342
309823
485150
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

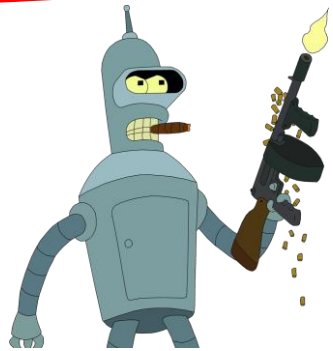
KLUCZ ROZDZIELONY

tajny kod

74 92 04 73 92



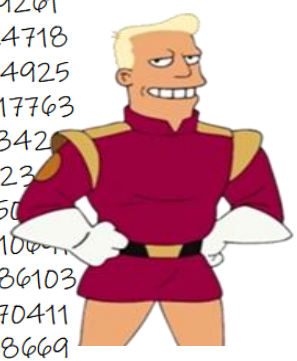




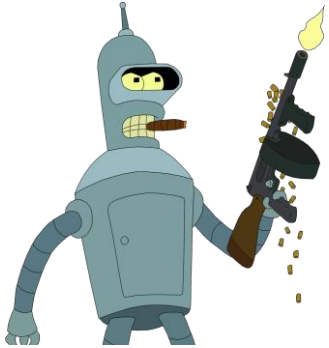
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
652484426
148098887
04231618
41879261
42024718
88694925
609317763
7503342
309823
48515
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY

74 92 04 73 ??





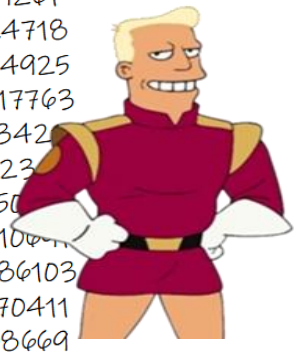


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
652484260
14809887
04231618
41879261
42024718
88694925
609317763
7503342
309823
485150
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

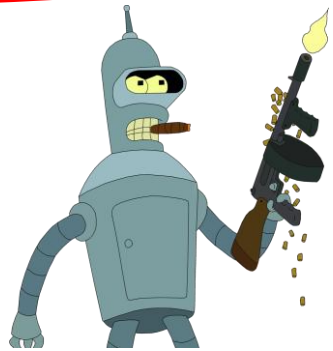
KLUCZ ROZDZIELONY

Znają 80% kodu!

74 92 04 73 ??







41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
7503342
309823
48515
490910
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

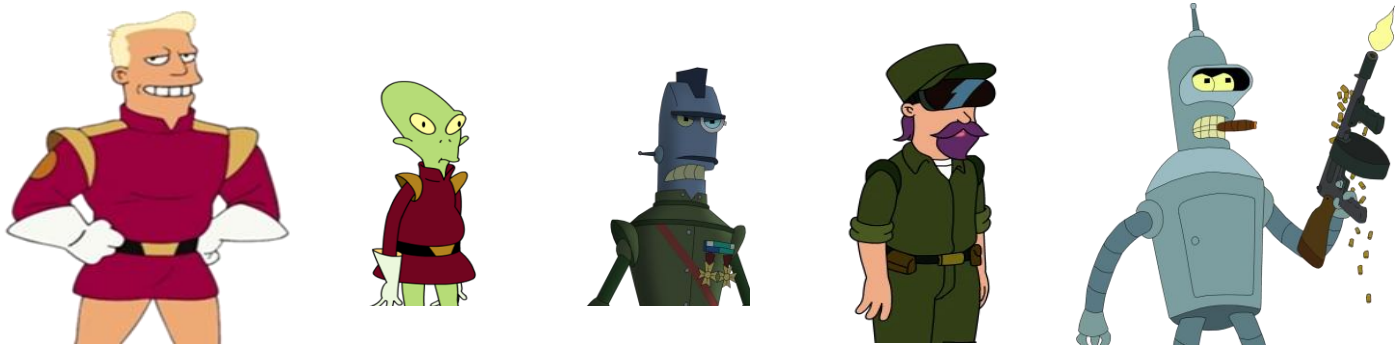
KLUCZ ROZDZIELONY

74+92+04+73+92 = 335

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

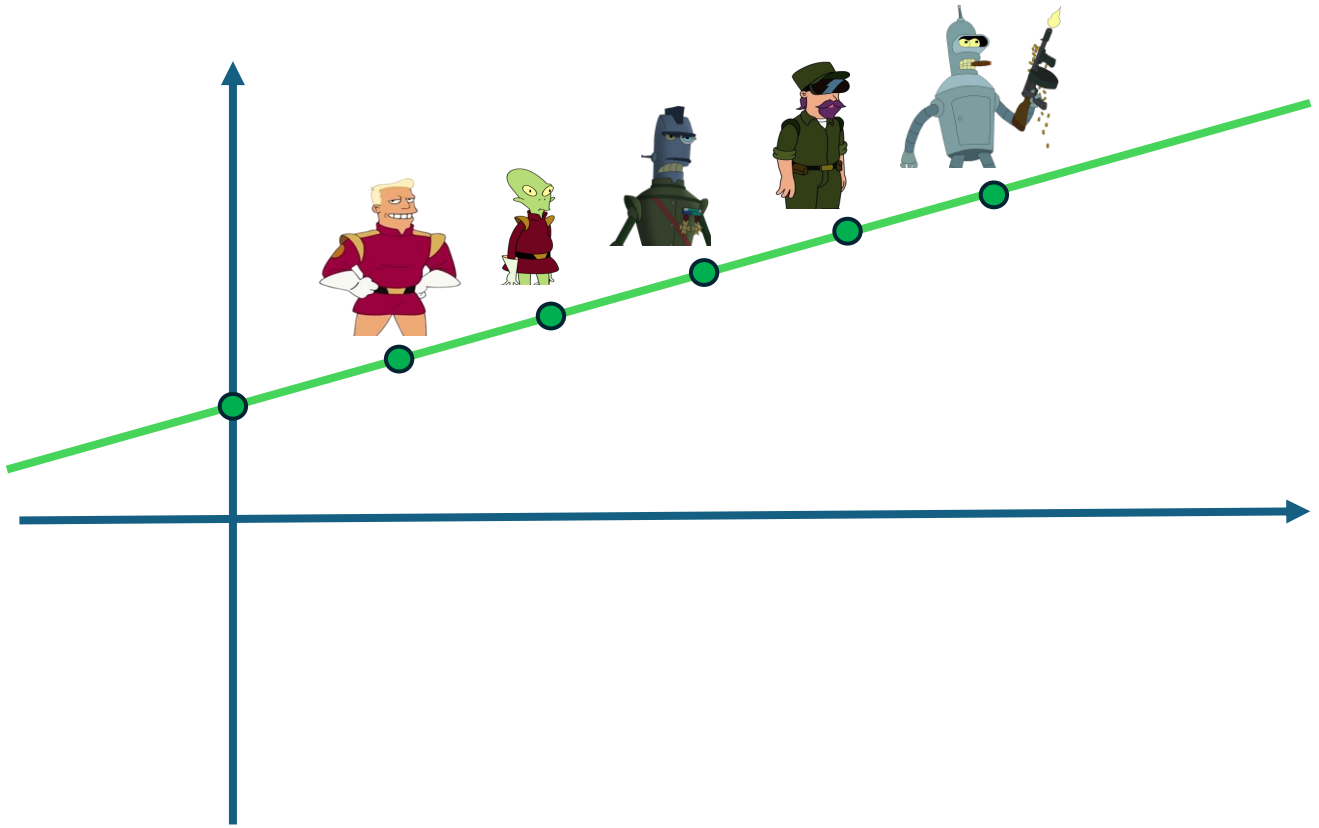
KLUCZ ROZDZIELONY

Co, jeżeli chcemy by dowolnych dwóch generałów mogło uruchomić rakietę?



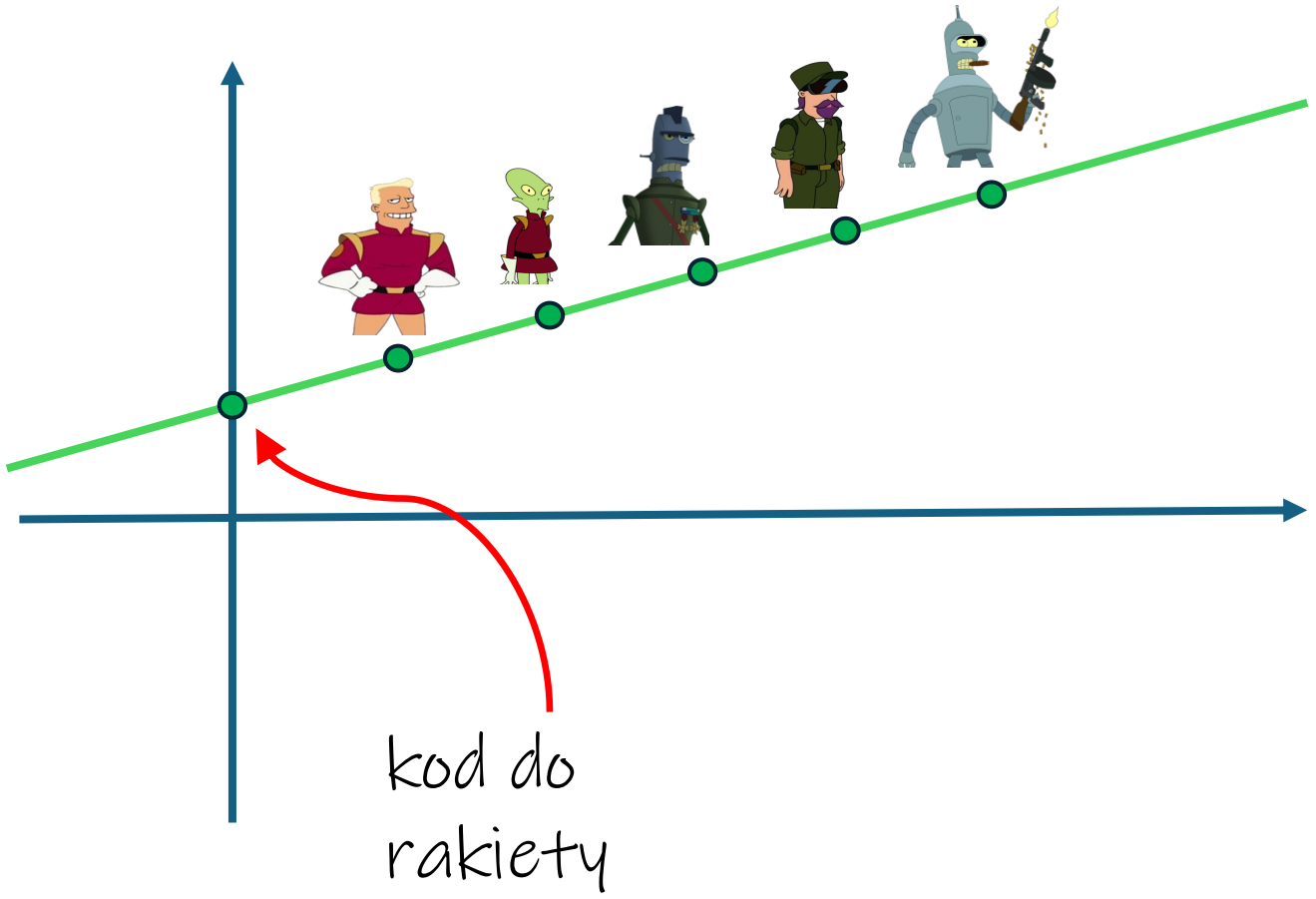
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY



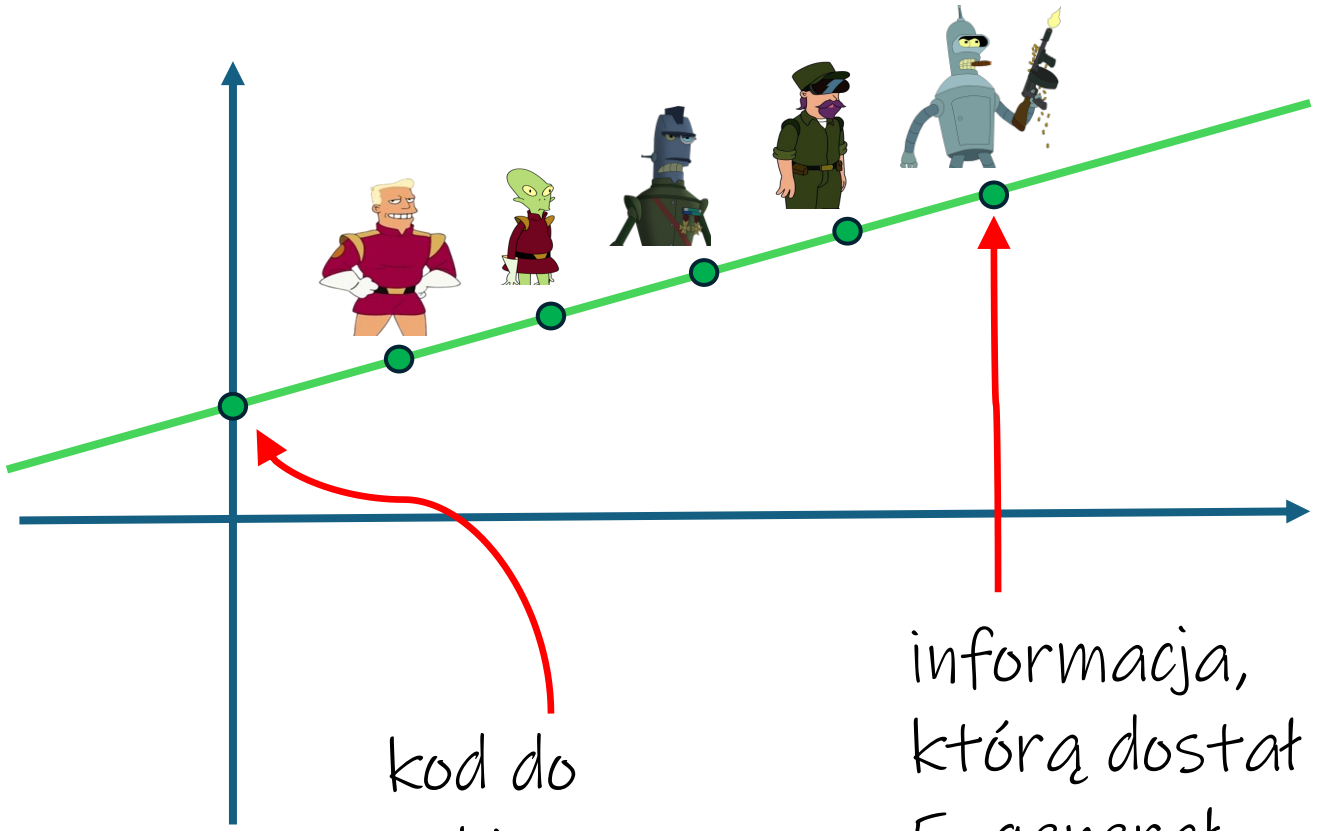
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

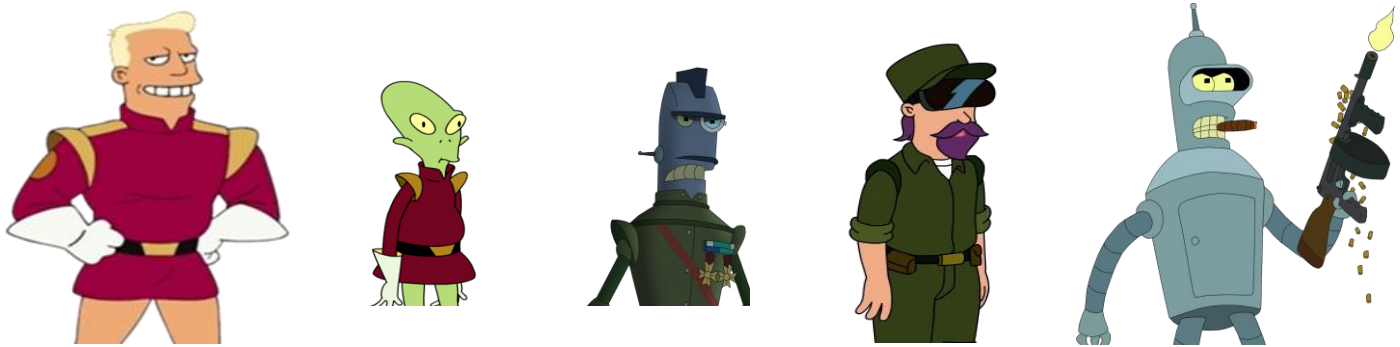
KLUCZ ROZDZIELONY



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

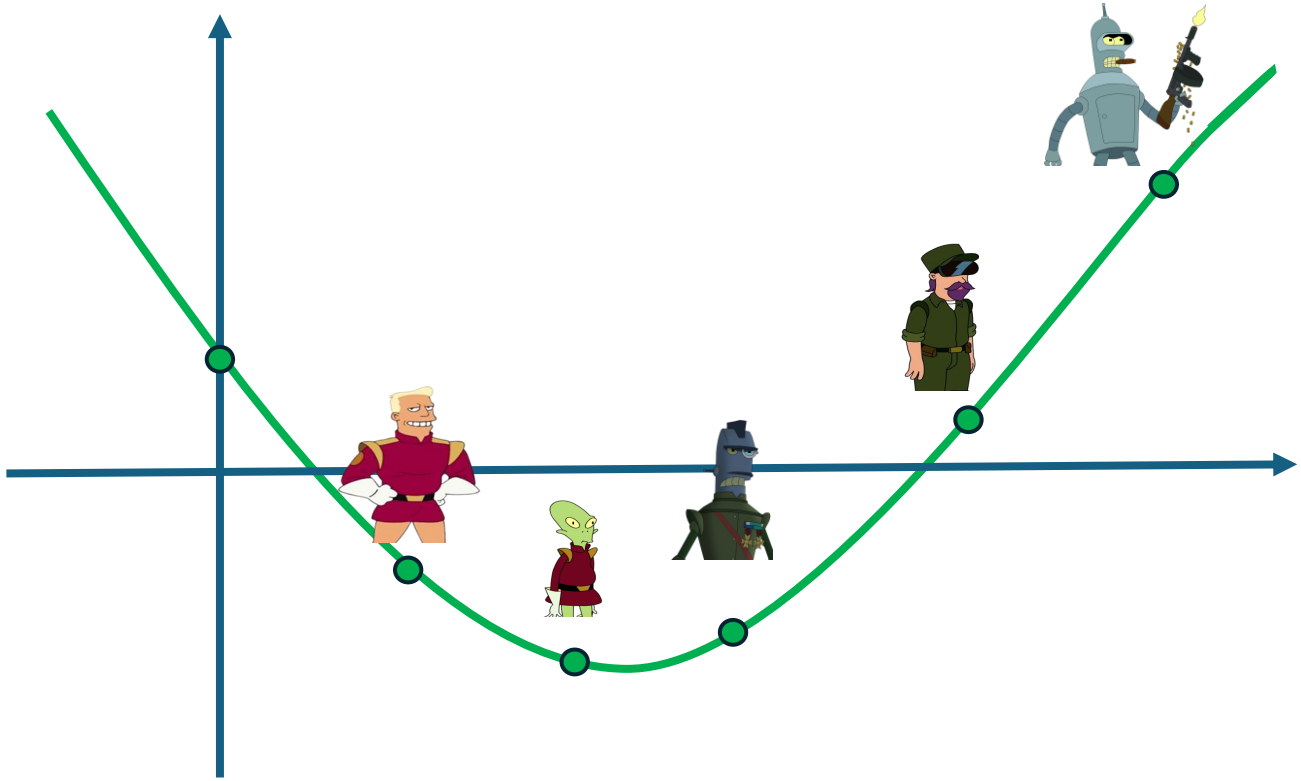
KLUCZ ROZDZIELONY

A dowolnych trzech generałów?



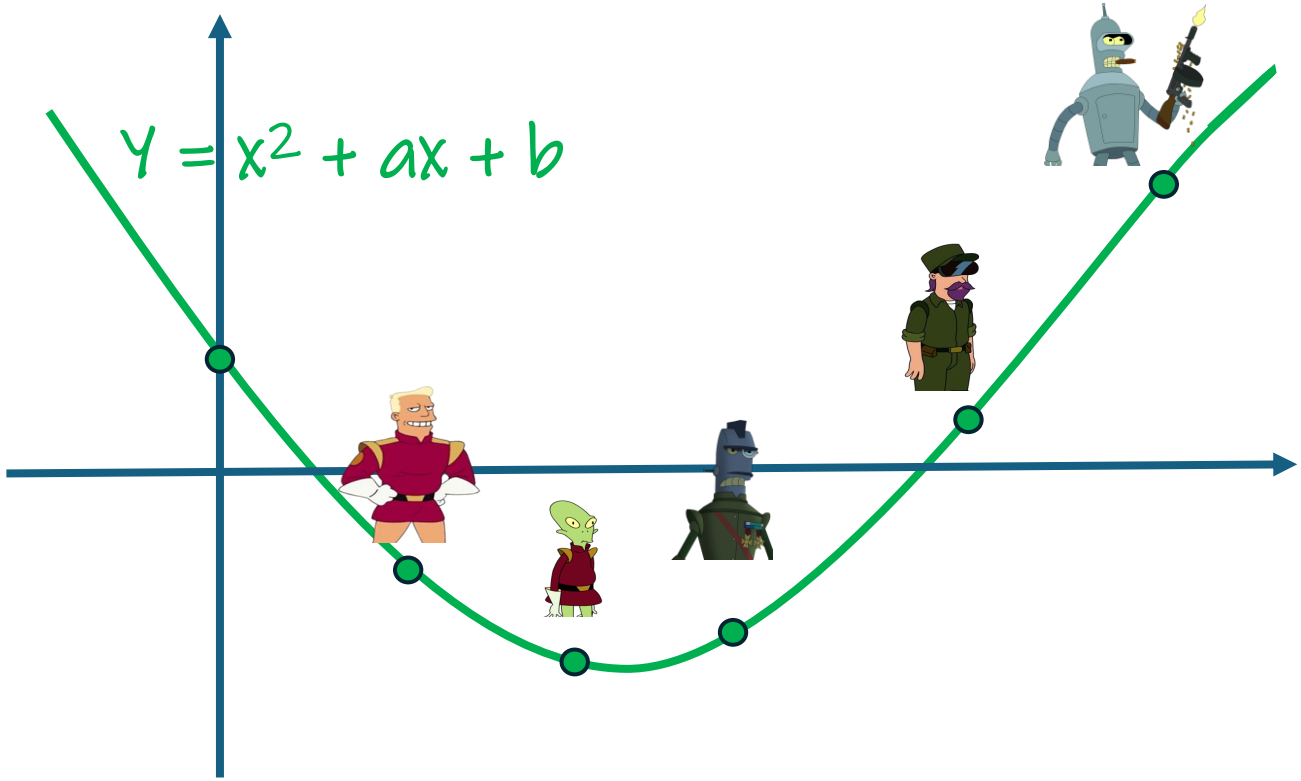
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY



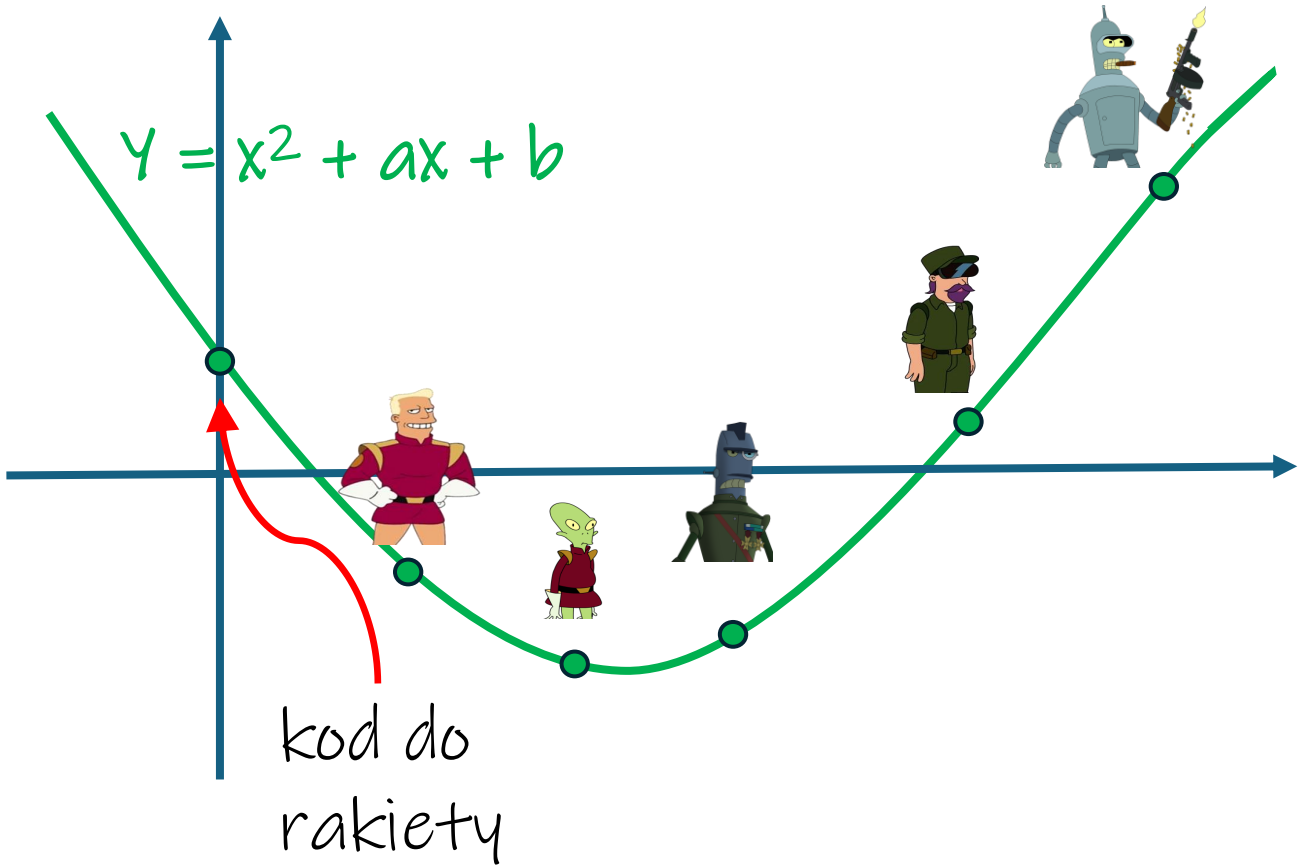
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY



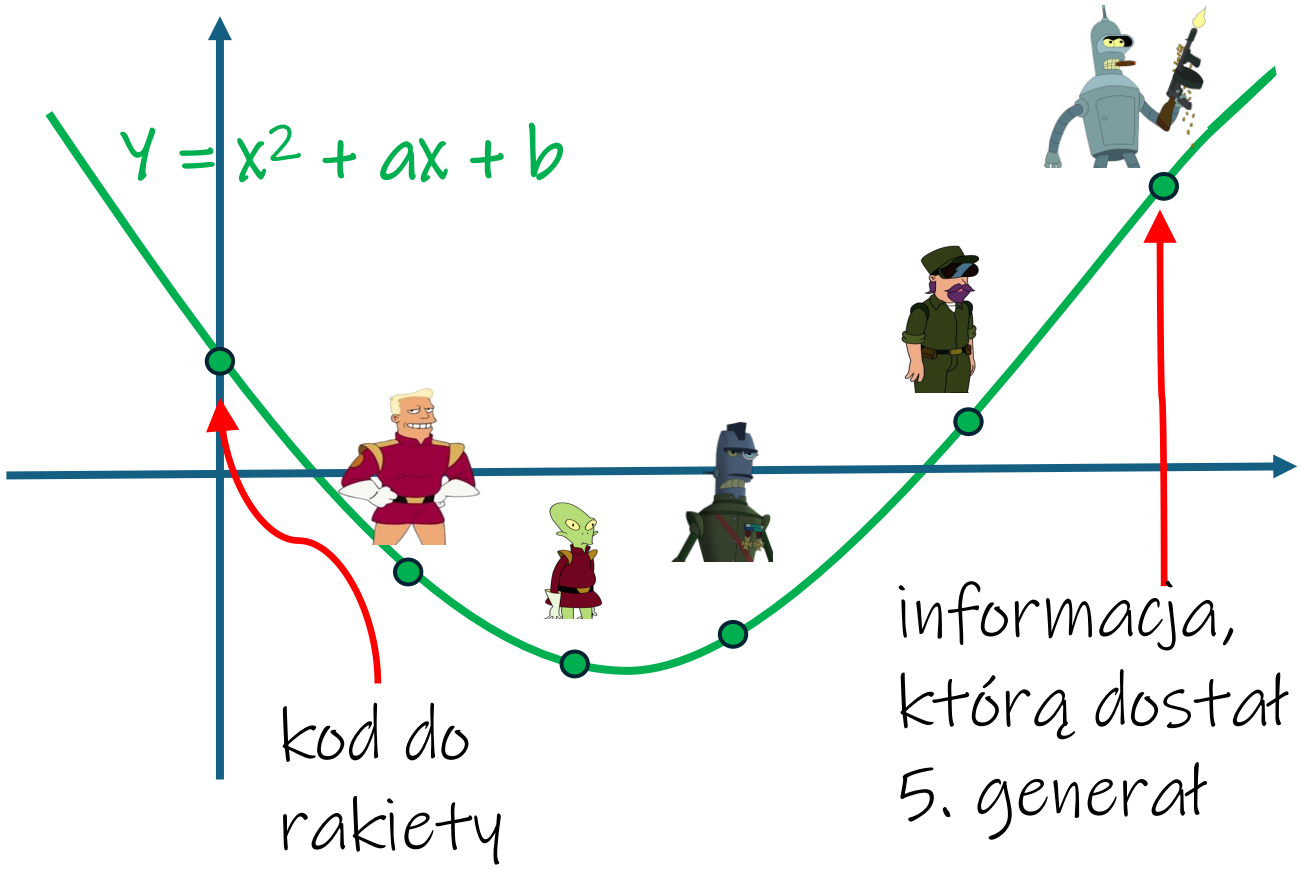
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KLUCZ ROZDZIELONY



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

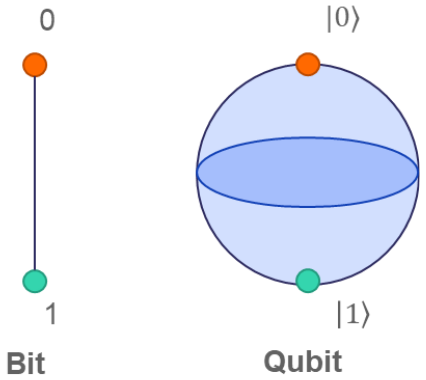
KLUCZ ROZDZIELONY

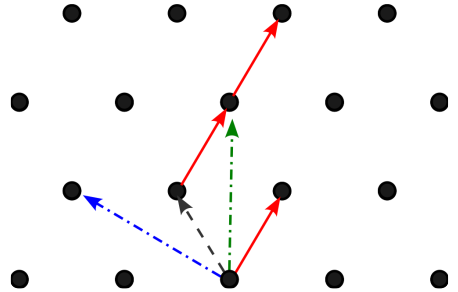


41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

AUKCJE

W 2008 r. opisany mechanizm posłużył w aukcjach odwrotnych przy skupie buraków od rolników w Danii.





PRZYSZŁOŚĆ

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE

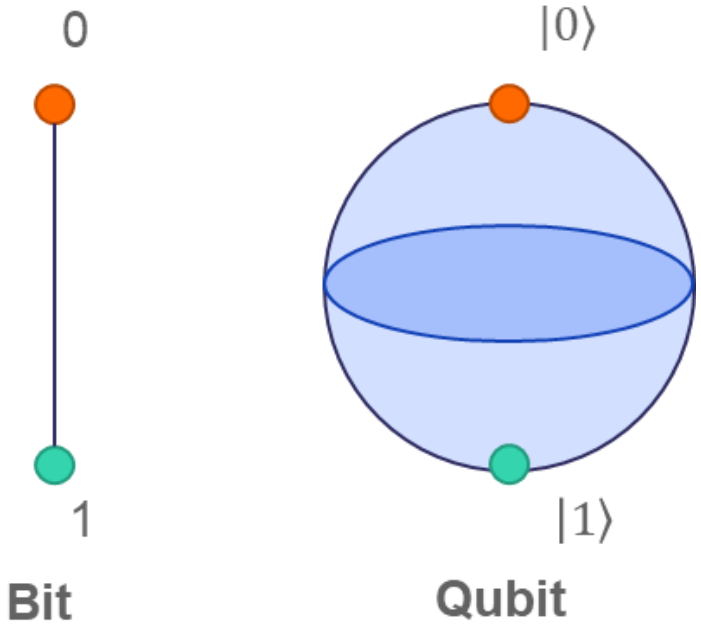
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE

- Komputery kwantowe działają w oparciu o prawa mechaniki kwantowej, wykorzystując zjawiska takie jak superpozycja i splątanie.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE

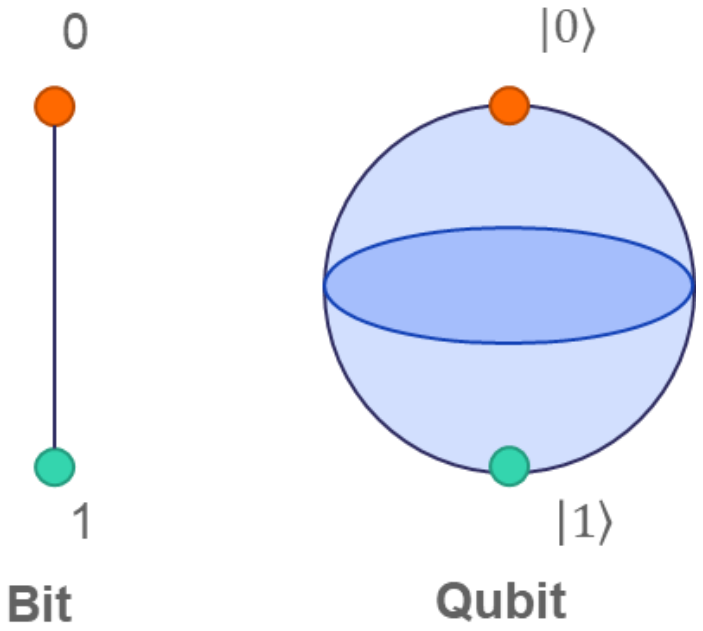


- Komputery kwantowe działają w oparciu o prawa mechaniki kwantowej, wykorzystując zjawiska takie jak superpozycja i splątanie.

- Podstawową jednostką informacji w komputerze kwantowym jest kubit, który w przeciwieństwie do klasycznego bitu może znajdować się jednocześnie w stanie 0 i 1.

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE



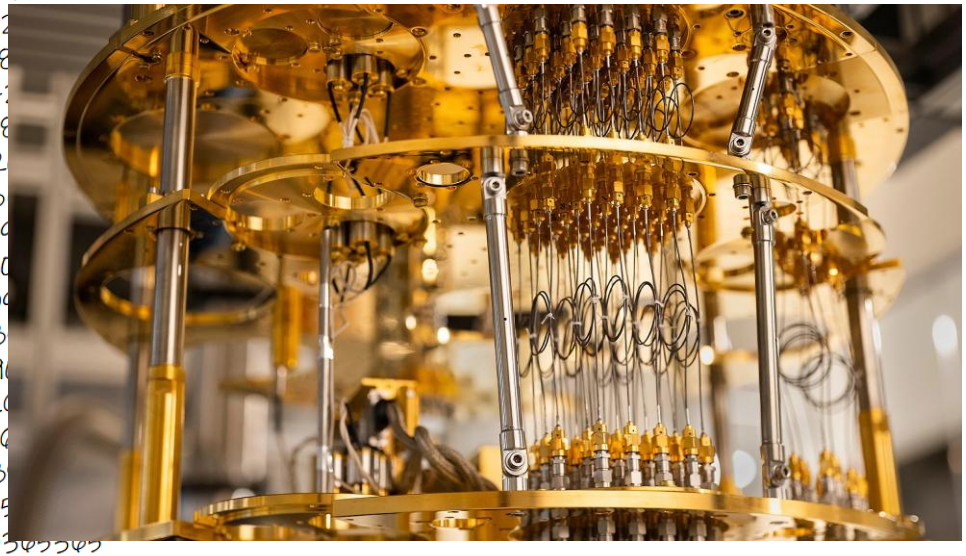
- Komputery kwantowe działają w oparciu o prawa mechaniki kwantowej, wykorzystując zjawiska takie jak superpozycja i splątanie.

- Podstawową jednostką informacji w komputerze kwantowym jest kubit, który w przeciwieństwie do klasycznego bitu może znajdować się jednocześnie w stanie 0 i 1.

- Dzięki superpozycji komputer kwantowy może przetwarzać wiele stanów jednocześnie, co daje mu przewagę obliczeniową nad zwykłym komputerem – **te komputery umieją szybko rozkładać liczby na czynniki pierwsze!**

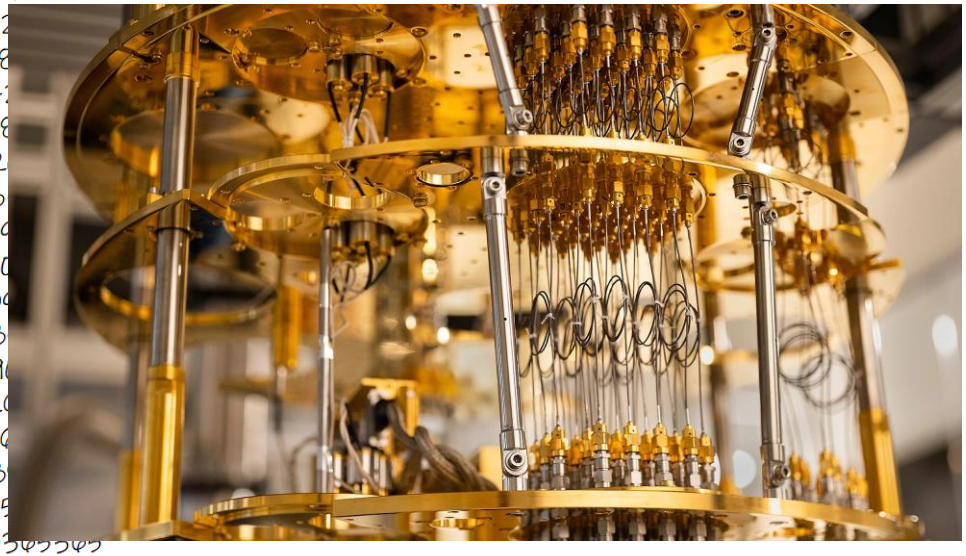
41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65
198
04
418
42
88
60
750
30
48
49
02
180
48
70
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE



41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

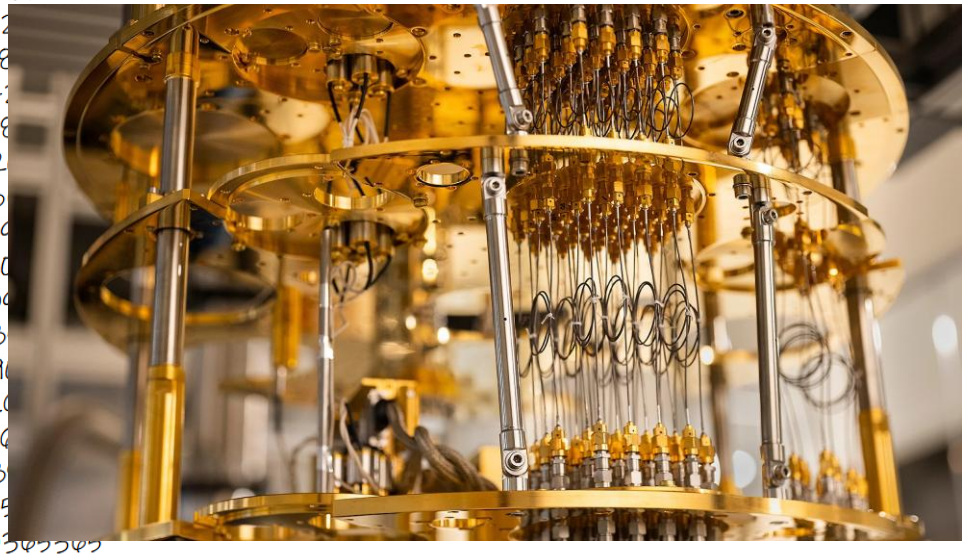
KOMPUTERY KWANTOWE



- 19 lutego 2025 r. Microsoft zaprezentował układ kwantowy oparty na nowej architekturze. Ma ona pozwolić na stworzenie komputerów kwantowych zdolnych do rozwiązywania problemów na skalę przemysłową w ciągu kilku lat, a nie dekad (na razie 8 kubitów – w przyszłości milion!)

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE

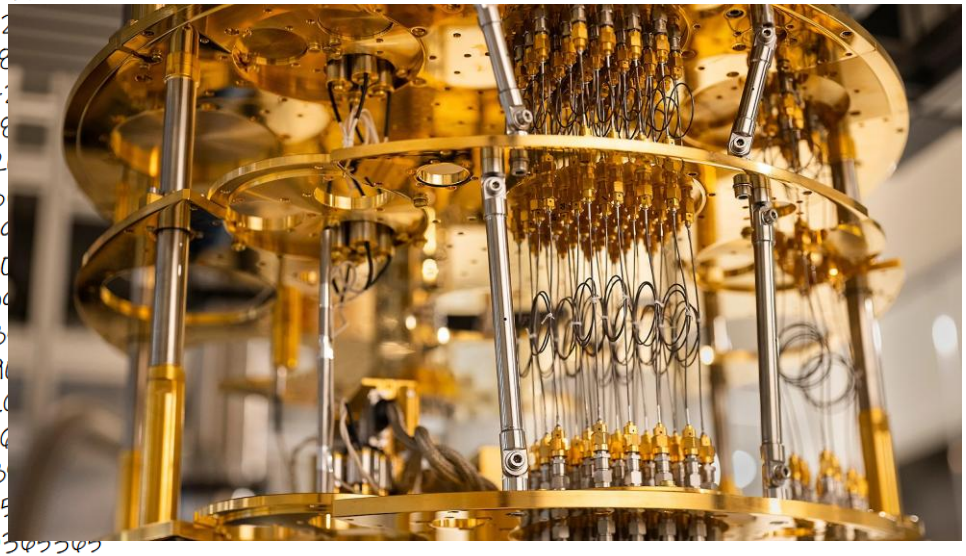


- 19 lutego 2025 r. Microsoft zaprezentował układ kwantowy oparty na nowej architekturze. Ma ona pozwolić na stworzenie komputerów kwantowych zdolnych do rozwiązywania problemów na skalę przemysłową w ciągu kilku lat, a nie dekad (na razie 8 kubitów – w przyszłości milion!)

- największa liczba sfaktoryzowana wyłącznie przez komputer kwantowy to (wg mojej wiedzy)...

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE

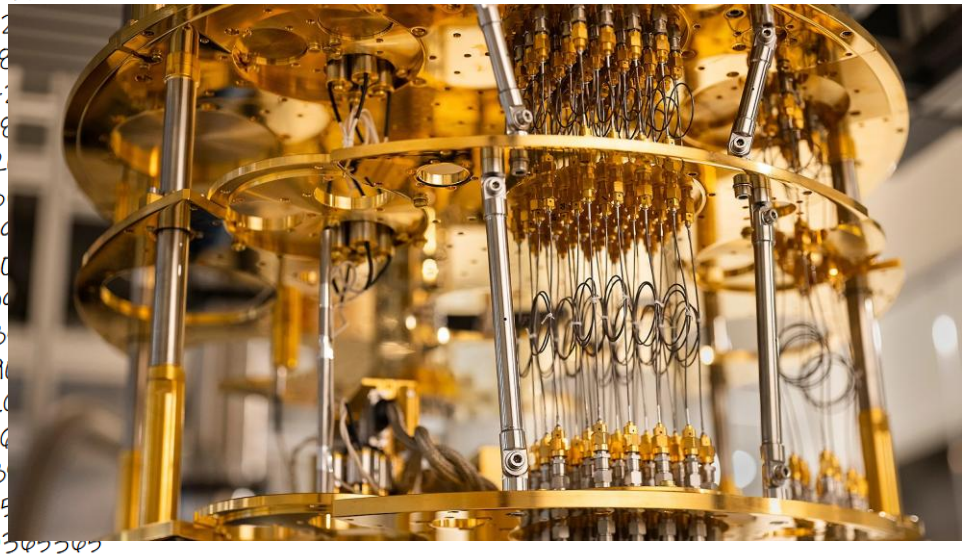


- 19 lutego 2025 r. Microsoft zaprezentował układ kwantowy oparty na nowej architekturze. Ma ona pozwolić na stworzenie komputerów kwantowych zdolnych do rozwiązywania problemów na skalę przemysłową w ciągu kilku lat, a nie dekad (na razie 8 kubitów – w przyszłości milion!)

- największa liczba sfaktoryzowana wyłącznie przez komputer kwantowy to (wg mojej wiedzy)... 21!

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

KOMPUTERY KWANTOWE



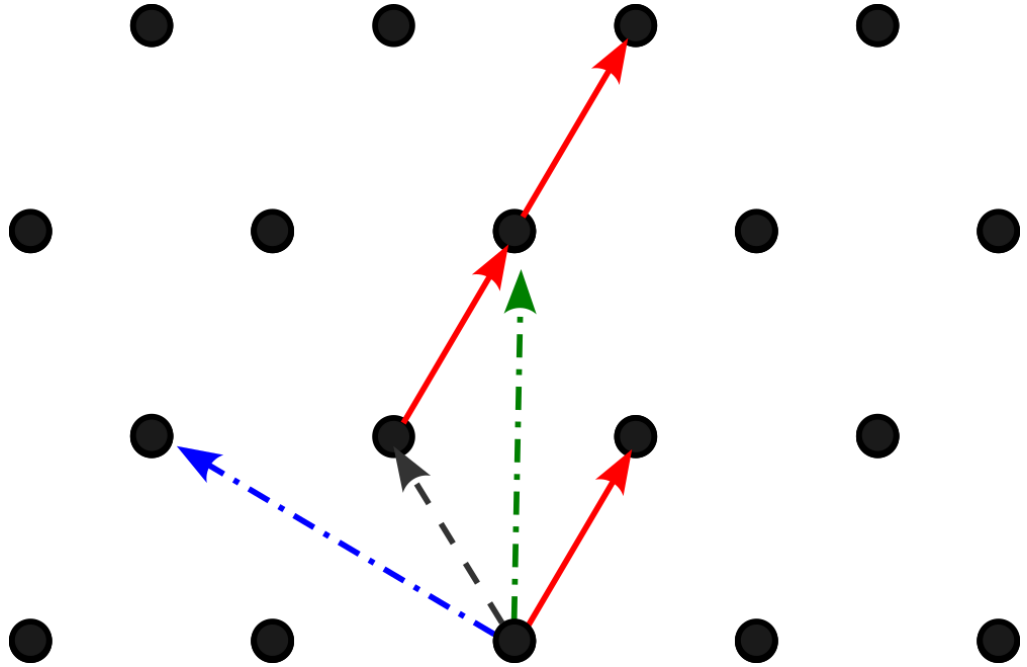
- 19 lutego 2025 r. Microsoft zaprezentował układ kwantowy oparty na nowej architekturze. Ma ona pozwolić na stworzenie komputerów kwantowych zdolnych do rozwiązywania problemów na skalę przemysłową w ciągu kilku lat, a nie dekad (na razie 8 kubitów – w przyszłości milion!)

- największa liczba sfaktoryzowana wyłącznie przez komputer kwantowy to (wg mojej wiedzy)... 21!

- Największa liczba sfaktoryzowana przez komputer kwantowy z pomocą klasycznego: 1,099,551,473,989.

41202343
69866595
43855531
36533[illegible]
594817[illegible]81
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

POSTKWANTOWE TRUDNE PROBLEMY



Jak znaleźć najkrótszy wektor w danej kracie?

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ODPOWIEDZIALNOŚĆ

G. H. Hardy (1940 r.):

„Prawdziwa matematyka nie ma wpływu na wojnę. Nikt jeszcze nie odkrył żadnego wojennego celu, któremu miałaby służyć teoria liczb lub teoria względności, i wydaje się mało prawdopodobne, by komuś to się udało."

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

ODPOWIEDZIALNOŚĆ

G. H. Hardy (1940 r.):

„Prawdziwa matematyka nie ma wpływu na wojnę. Nikt jeszcze nie odkrył żadnego wojennego celu, któremu miałaby służyć teoria liczb lub teoria względności, i wydaje się mało prawdopodobne, by komuś to się udało."

41202343
69866595
43855531
36533257
594817981
16998443
27982845
45562643
38764455
65248426
19809887
04231618
41879261
42024718
88694925
609317763
750334211
30982397
48515094
490910691
026986103
186270411
48808669
70564902
90365365
88674337
317208131
041051908
64254793
282601391
25762403
39463732
69391

DZIEKUJĘ ZA UWAGĘ !