

Stefan Sokołowski

KRYPTOGRAFIA

wykład 1

Inst. Informatyki Stosowanej, ANS

Elbląg, 2026/2027

Cele kryptografii (kryptografia = szyfrowanie)

Cele kryptografii (kryptografia = szyfrowanie)



wiadomość

A red arrow points from the sender's side to the receiver's side, with the word "wiadomość" (message) written in red above it.

Cele kryptografii (kryptografia = szyfrowanie)



Cele kryptografii (kryptografia = szyfrowanie)



Cele kryptografii (kryptografia = szyfrowanie)



Poufność: żeby osoby nieuprawnione nie miały dostępu do treści

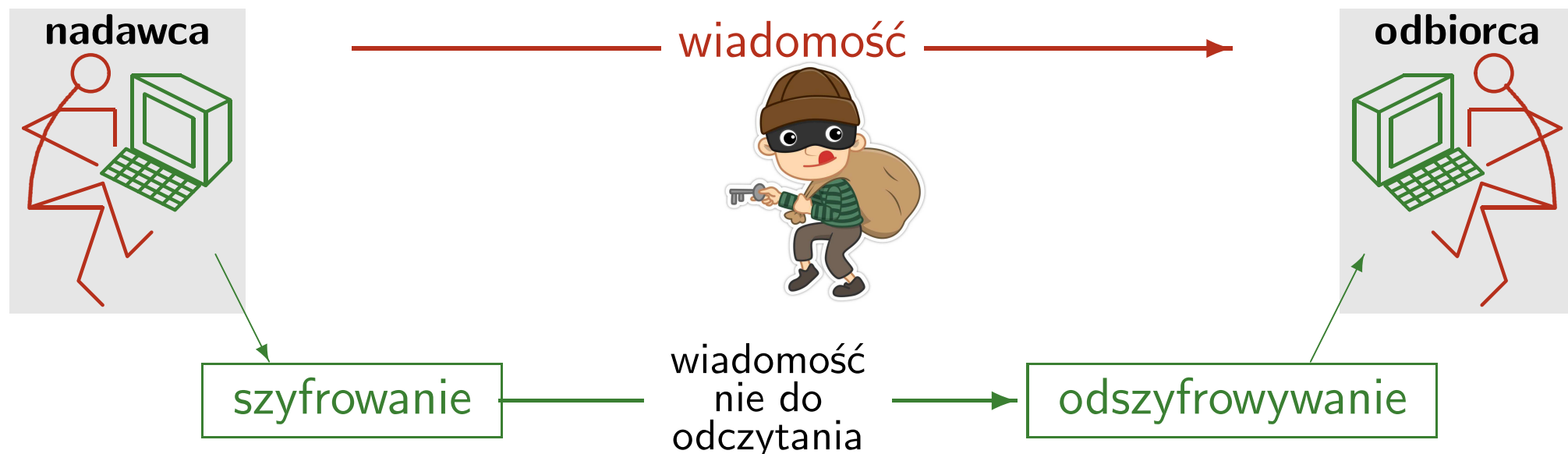
Cele kryptografii (kryptografia = szyfrowanie)



Poufność: żeby osoby nieuprawnione nie miały dostępu do treści



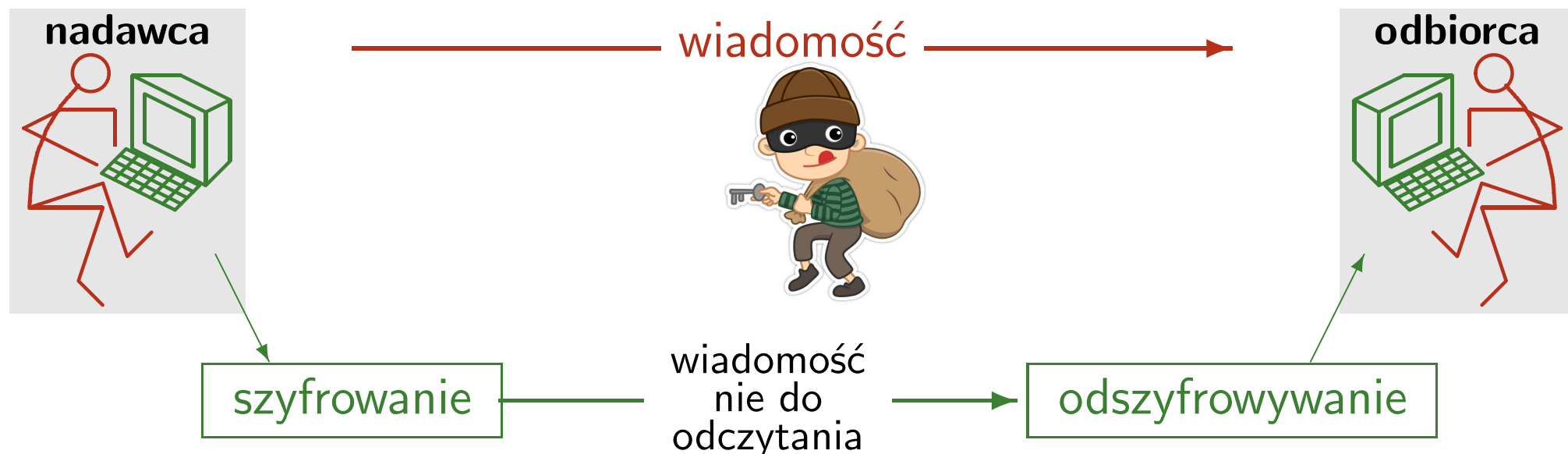
Cele kryptografii (kryptografia = szyfrowanie)



Poufność: żeby osoby nieuprawnione nie miały dostępu do treści



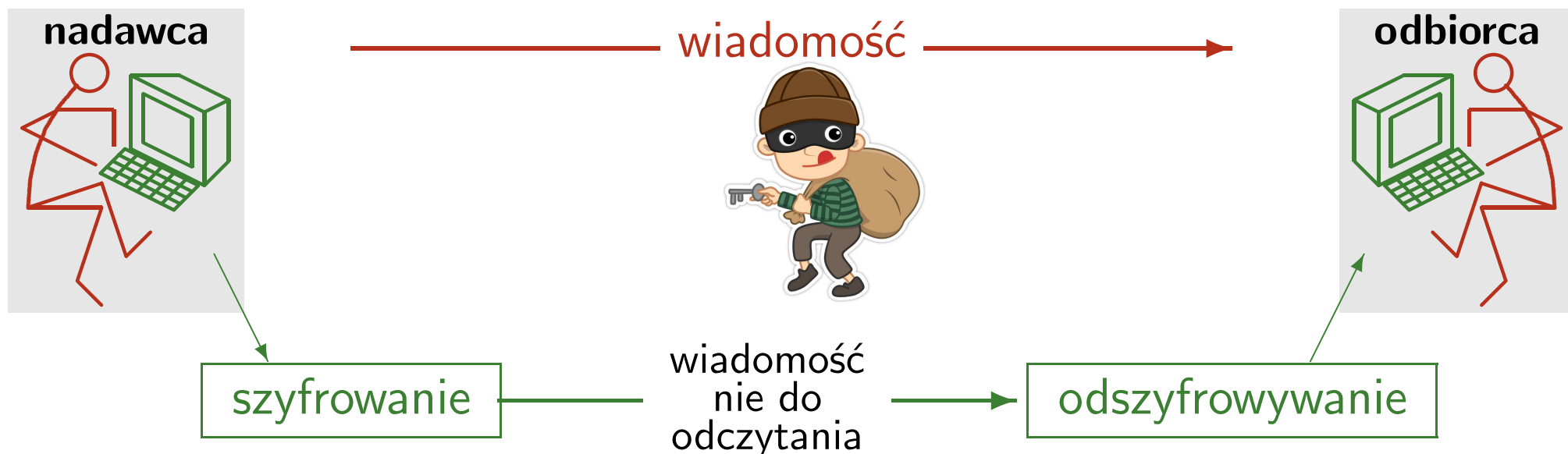
Cele kryptografii (kryptografia = szyfrowanie)



Poufność: żeby osoby nieuprawnione nie miały dostępu do treści



Cele kryptografii (kryptografia = szyfrowanie)



Poufność: żeby osoby nieuprawnione nie miały dostępu do treści



Uwierzytelnienie: żeby nie było wątpliwości, kto jest autorem

Klasyka: proste przestawienia

Klasyka: proste przestawienia

Szyfr dla dzieci

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓
s

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓
sz

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓
sza

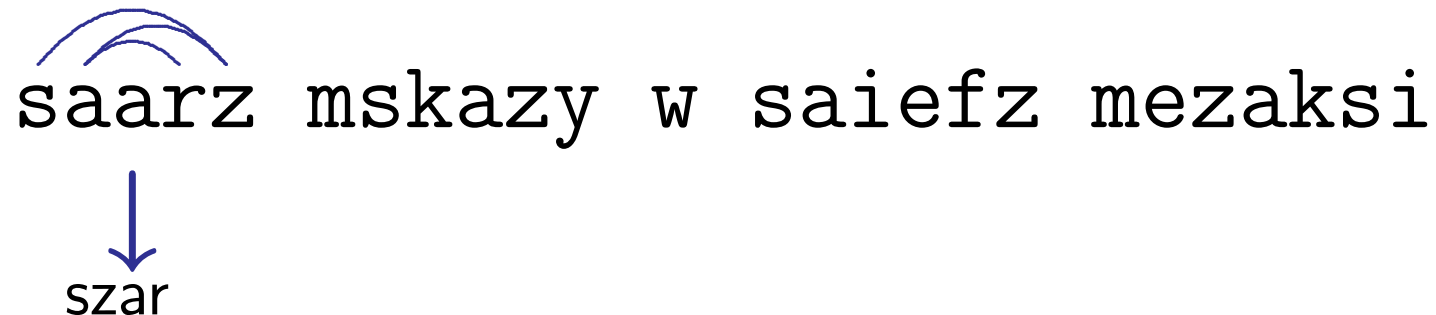
Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓

szar



Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓
szara

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓ ↓

szara m

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓
szara my

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓
szara mys

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓
szara mysz

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓
szara myszk

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓
szara myszka

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓ ↓
szara myszka w

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓ ↓ ↓
szara myszka w szafie

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi

↓ ↓ ↓ ↓ ↓

szara myszka w szafie mieszka

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓ ↓ ↓ ↓
szara myszka w szafie mieszka

- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓ ↓ ↓ ↓
szara myszka w szafie mieszka

- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...)

Klasyka: proste przestawienia

Szyfr dla dzieci:

saarz mskazy w saiefz mezaksi
↓ ↓ ↓ ↓ ↓
szara myszka w szafie mieszka

- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...), a potem dopisywane są litery z pozycji nieparzystych w odwrotnej kolejności.

Klasyka: proste przestawienia

Szyfr dla dzieci:

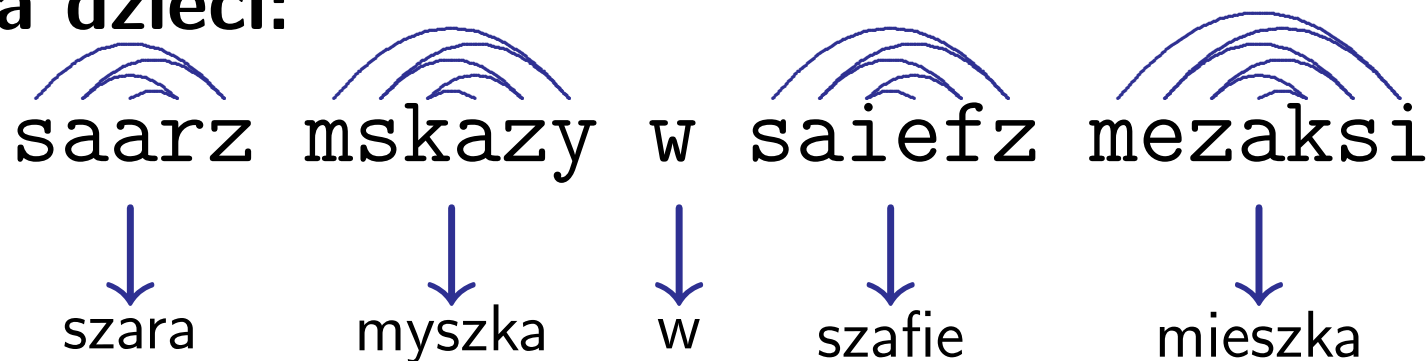
saarz mskazy w saiefz mezaksi
↓ ↓ ↓ ↓ ↓
szara myszka w szafie mieszka

- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...), a potem dopisywane są litery z pozycji nieparzystych w odwrotnej kolejności.

To samo, ale całe zdanie na raz

Klasyka: proste przestawienia

Szyfr dla dzieci:



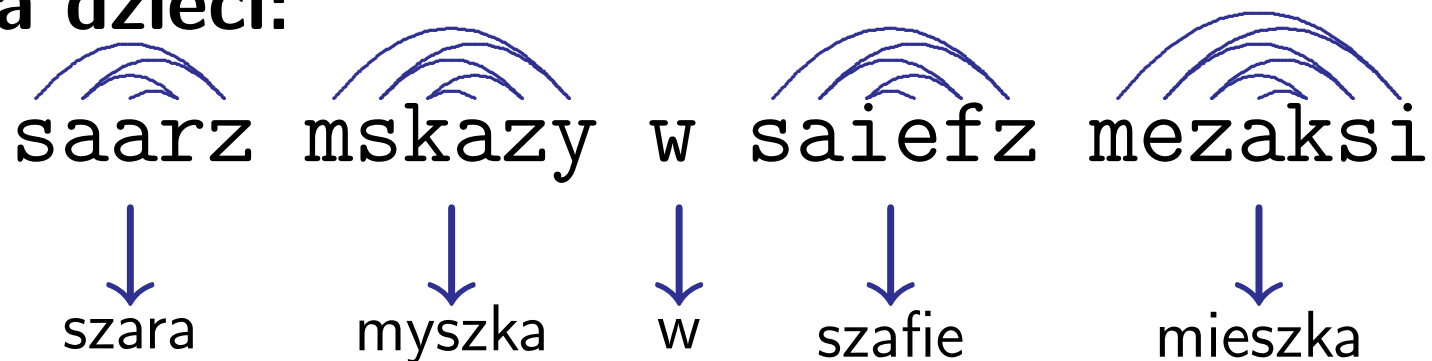
- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...), a potem dopisywane są litery z pozycji nieparzystych w odwrotnej kolejności.

To samo, ale całe zdanie na raz (kreseczki oznaczają spacje):

saamsk--zfemezaksi-iaswazy-rz

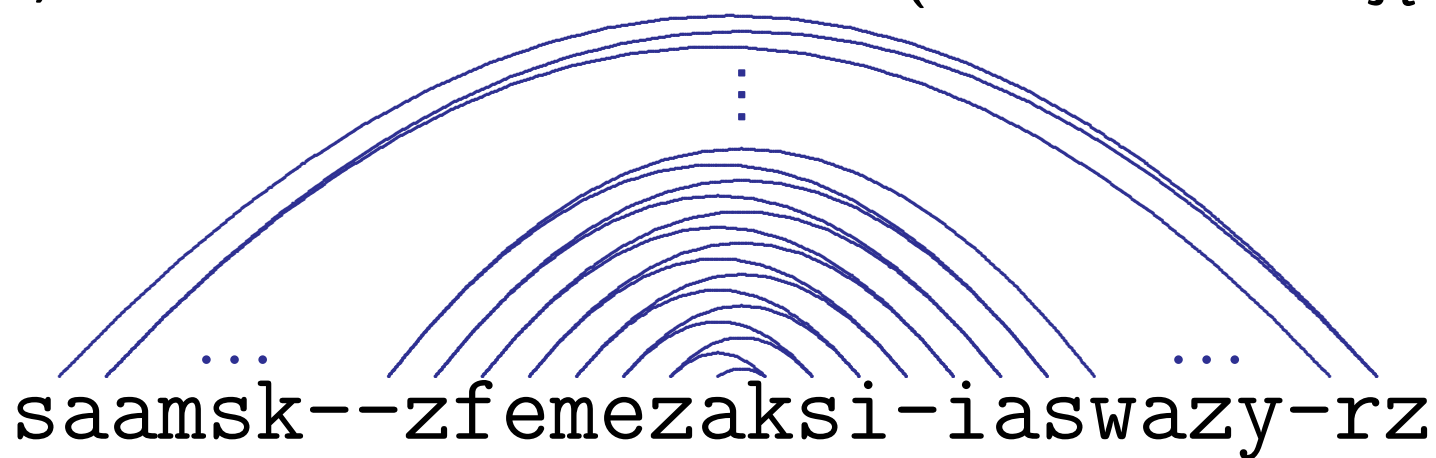
Klasyka: proste przestawienia

Szyfr dla dzieci:



- szyfrowane jest każde słowo z osobna, a interpunkcja (w tym spacje) jest zachowana;
- ciąg liter w słowie jest przestawiany w taki sposób, że najpierw wypisywane są litery z pozycji parzystych (0-wa, 2-ga, ...), a potem dopisywane są litery z pozycji nieparzystych w odwrotnej kolejności.

To samo, ale całe zdanie na raz (kreseczki oznaczają spacje):



Klasyka: szyfr Cezara

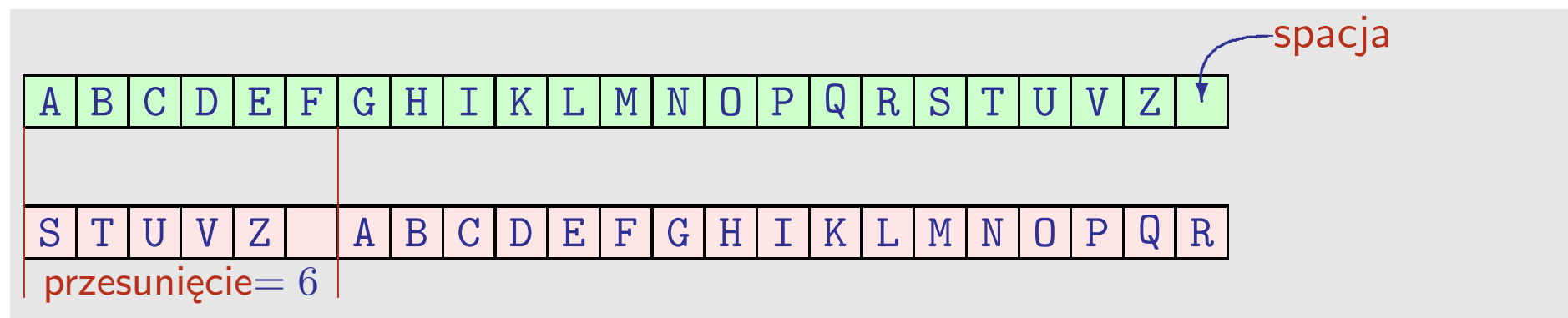
To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać.

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	Z	
S	T	U	V	Z		A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
przesunięcie= 6																						

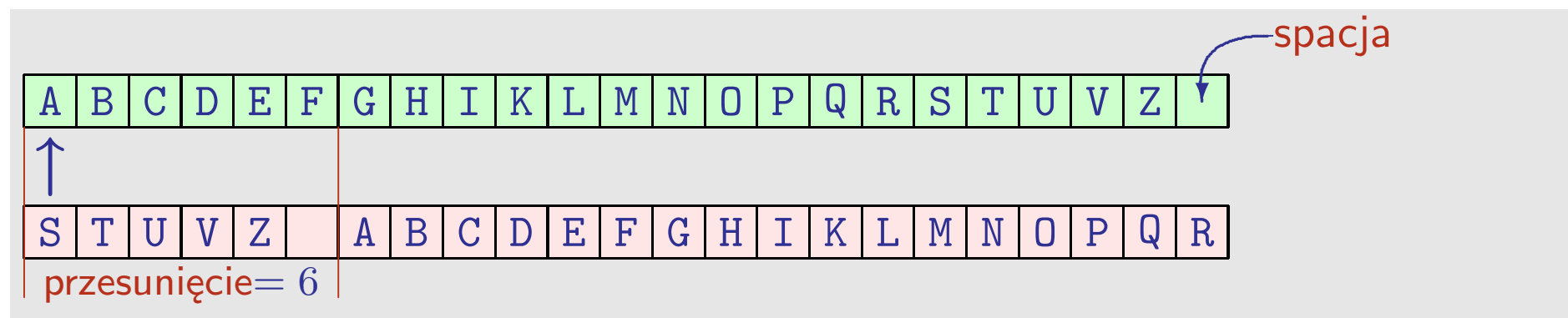
spacja

spacja

SEZSRCSUNSRZMN

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

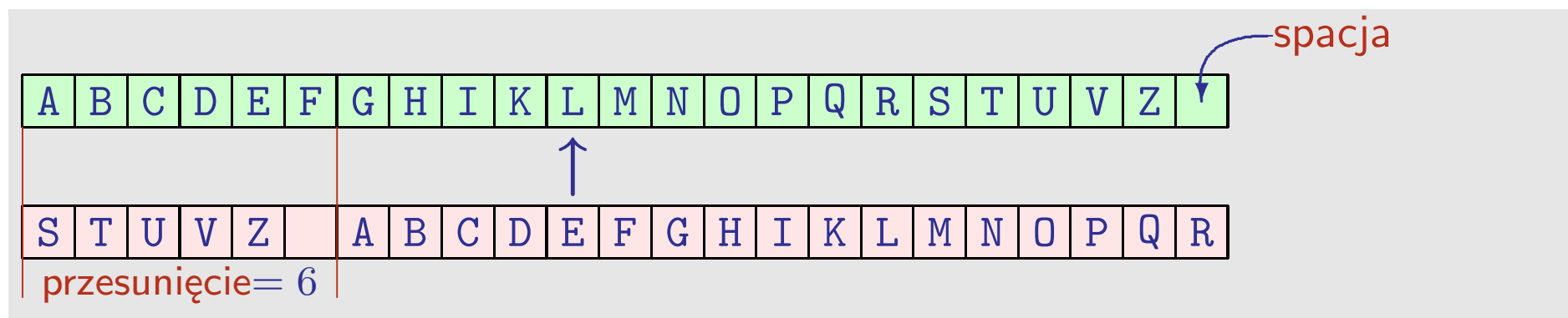


SEZSRCSUNSRZMN

↓
A

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

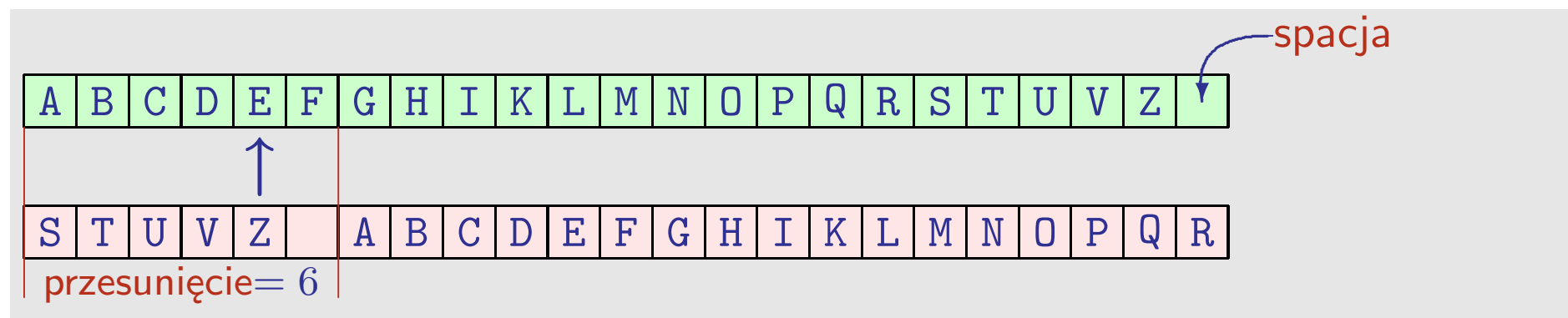


SEZSRC SUNSRZMN

↓
AL

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



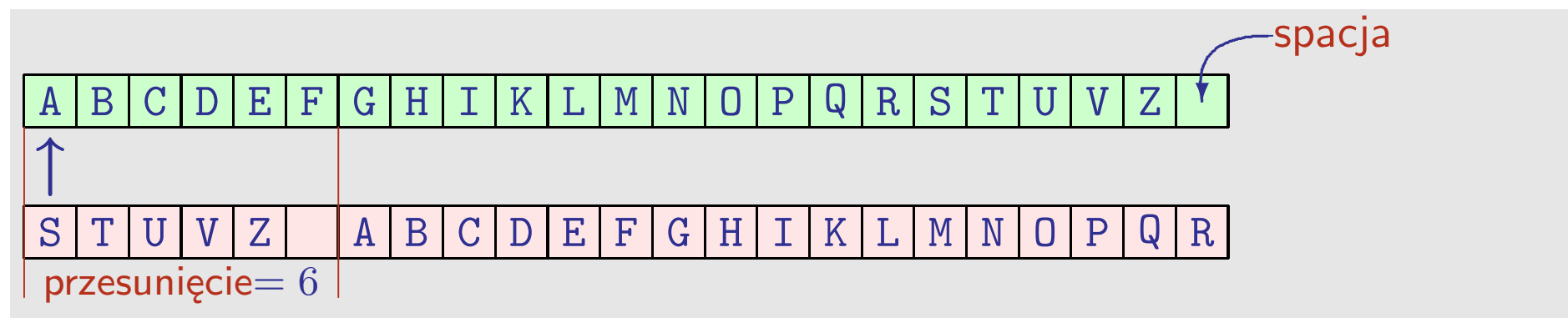
SEZSRCSUNSRZMN



ALE

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



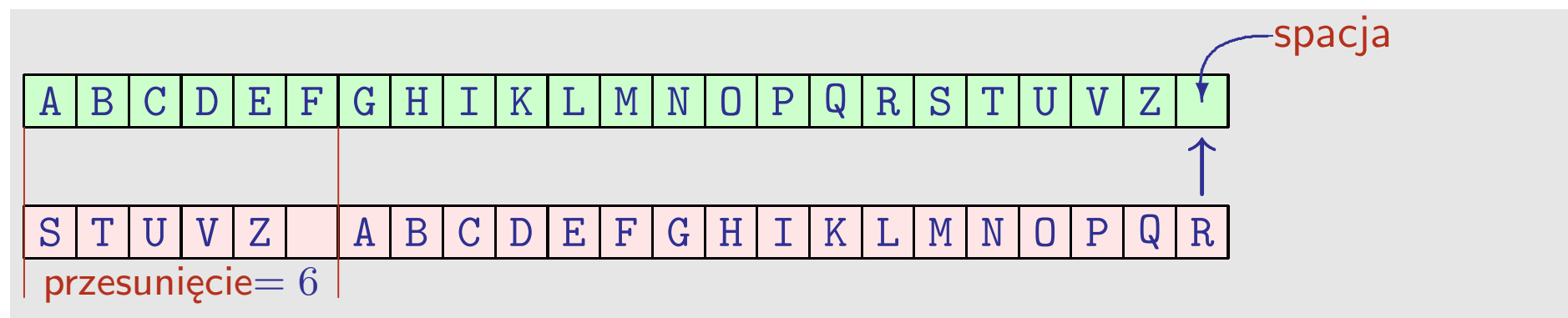
SEZSRCSUNSRZMN



ALEA

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



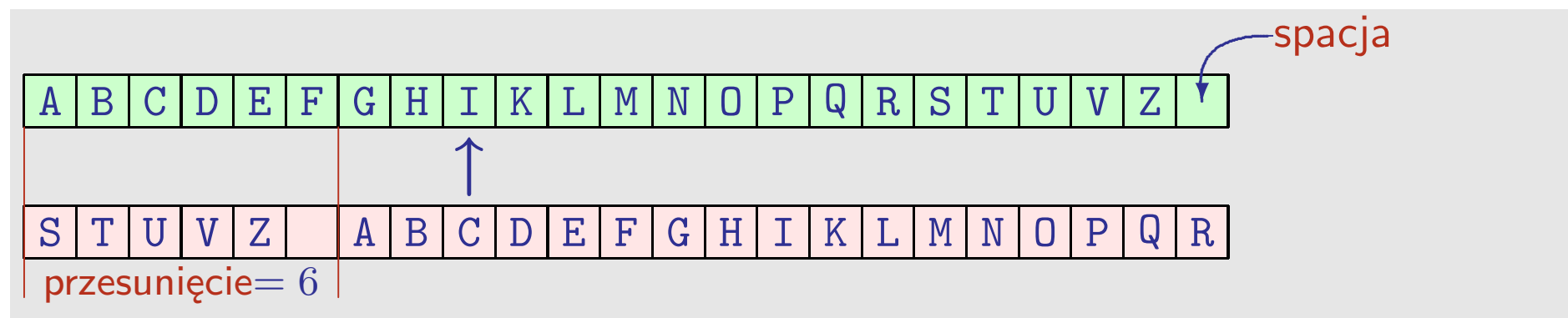
SEZSRC SUNSRZMN



ALEA

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

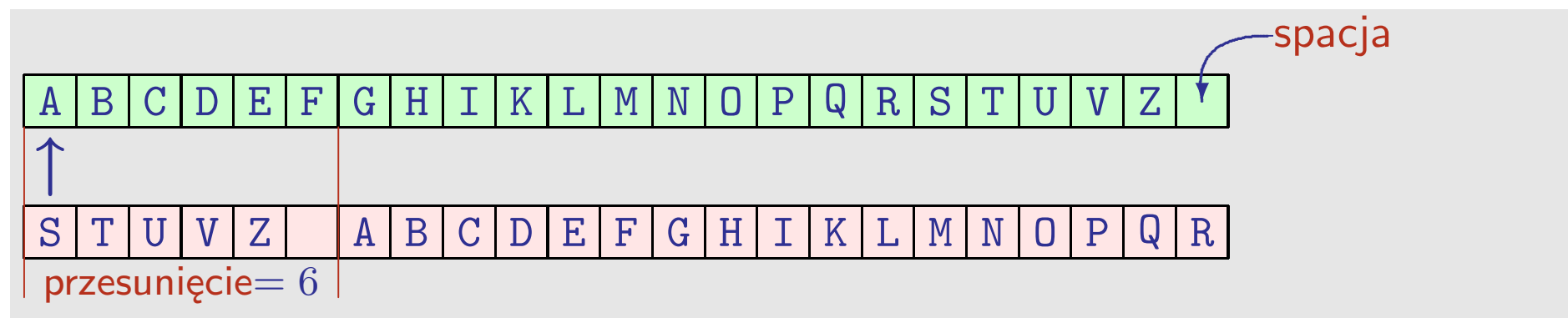


SEZSRC SUNSRZMN

↓
ALEA I

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



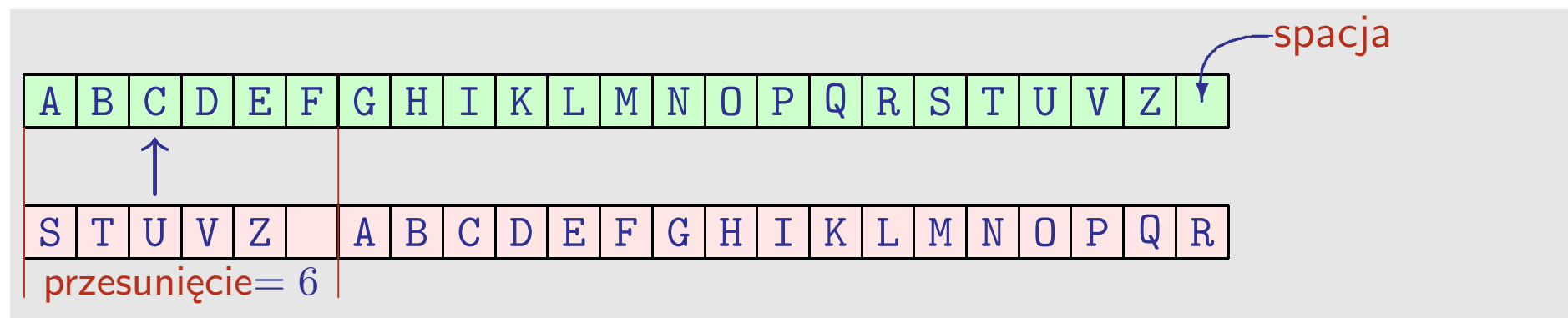
SEZSRC SUNSRZMN



ALEA IA

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

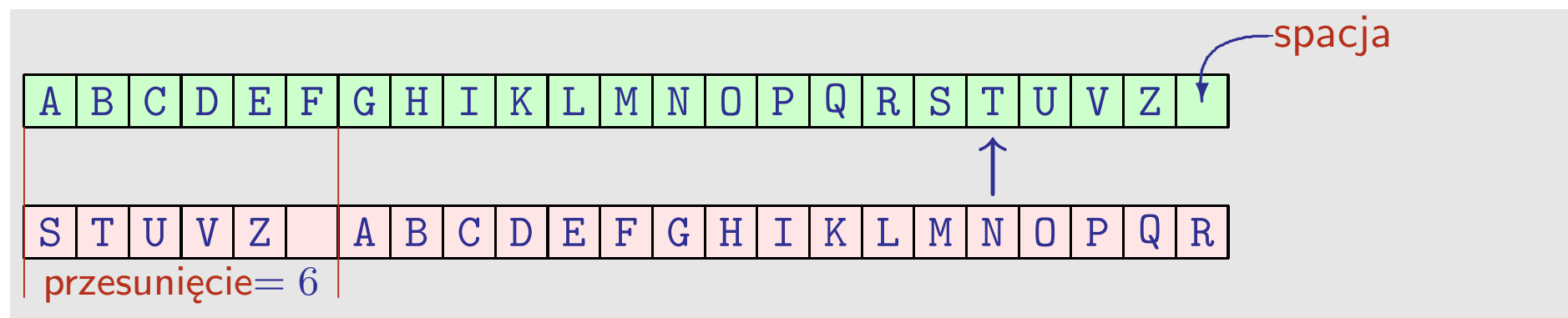


SEZSRC SUNSRZMN

ALEA IAC

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



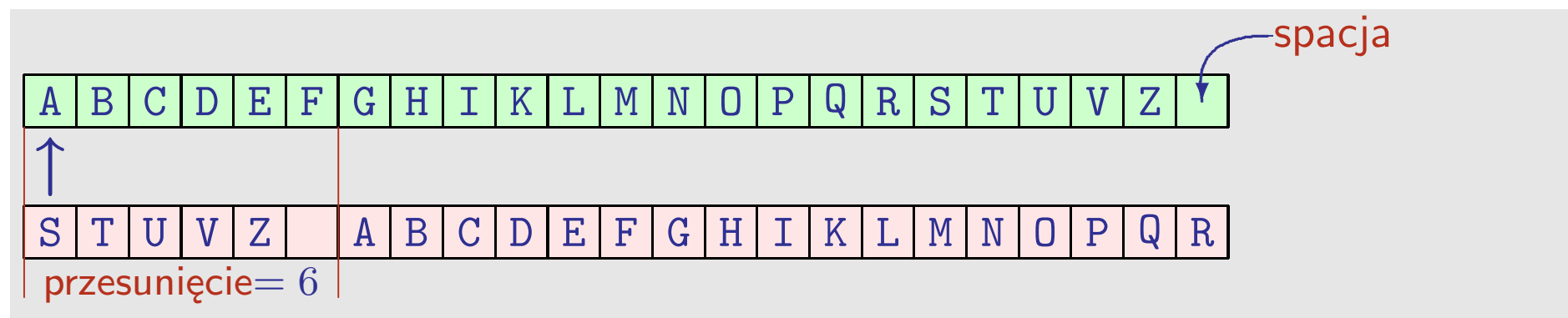
SEZSRCSUNSRZMN



ALEA IACT

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



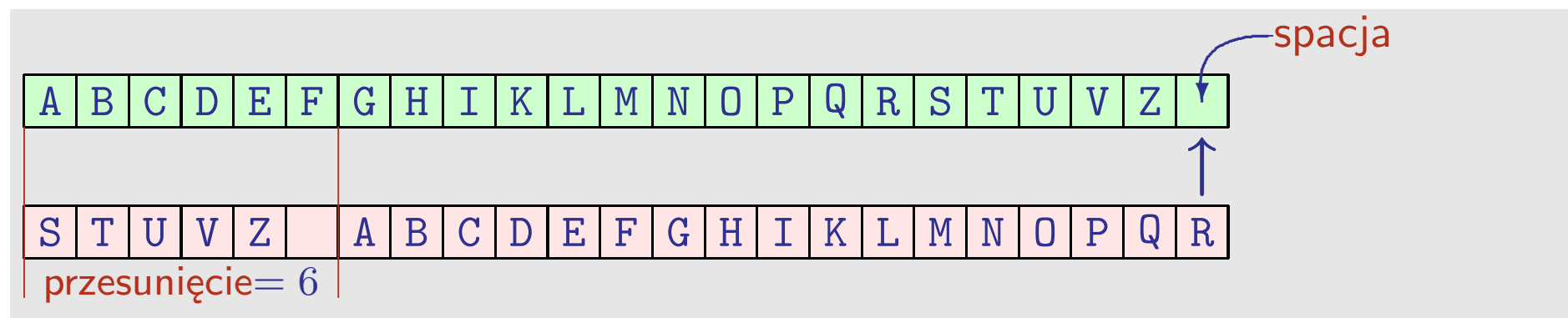
SEZSRCSUNSRZMN



ALEA IACTA

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



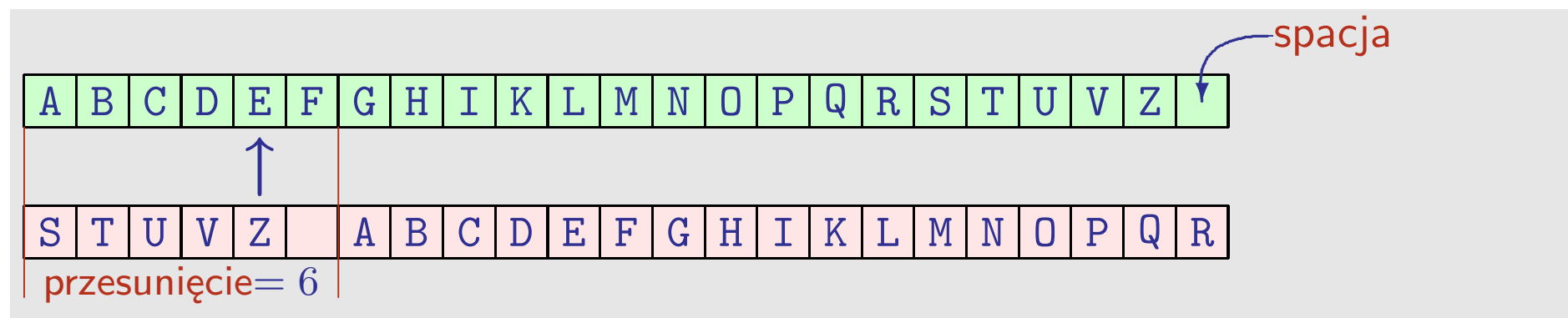
SEZSRCSUNSRZMN



ALEA IACTA

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

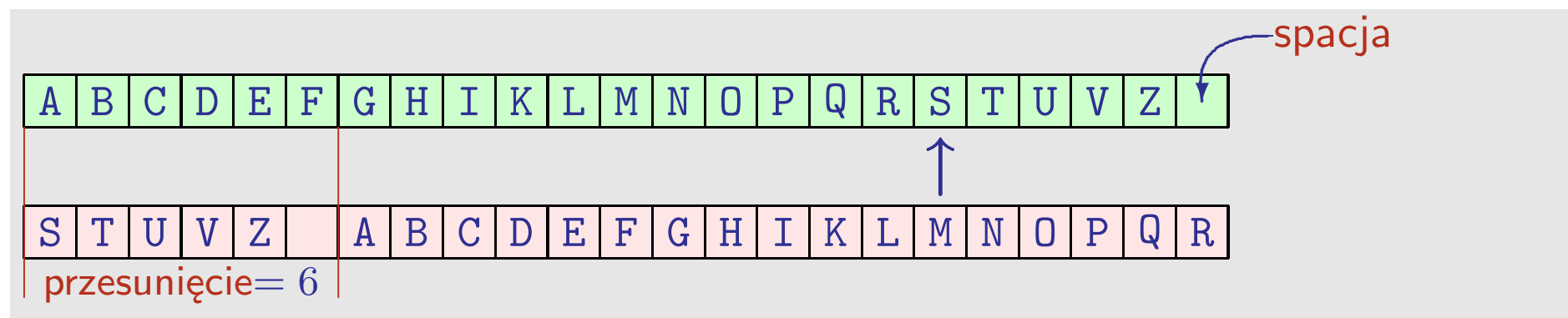


SEZSRCSUNSRZMN

↓
ALEA IACTA E

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:

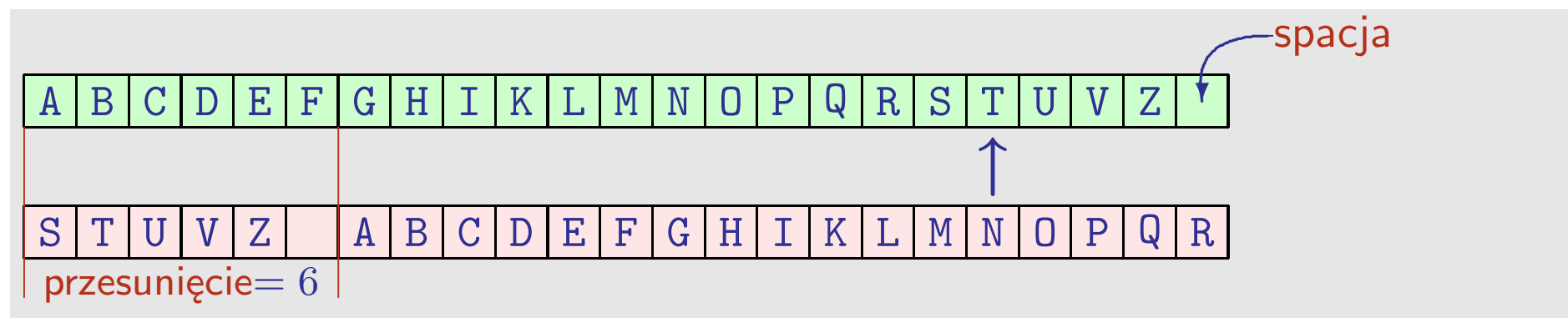


SEZSRCSUNSRZMN

ALEA IACTA ES

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



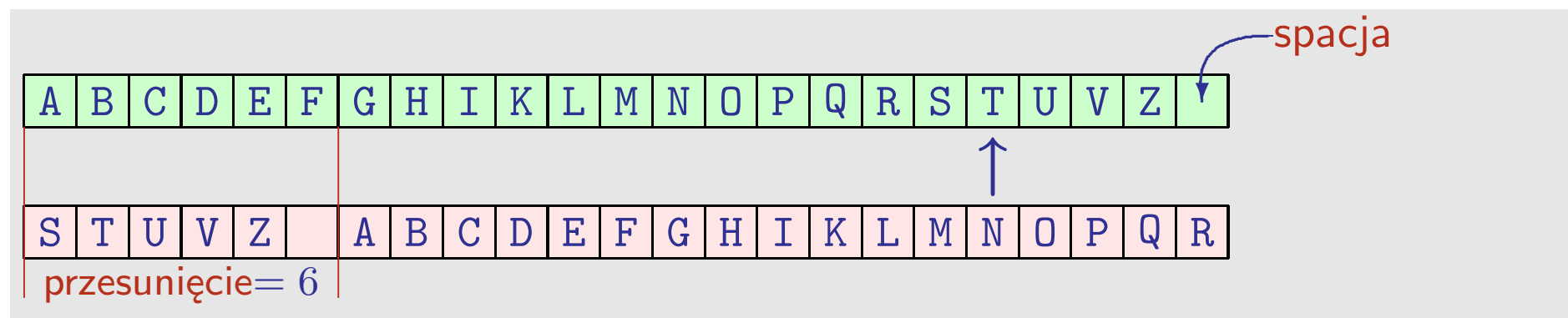
SEZSRCSUNSRZMN



ALEA IACTA EST

Klasyka: szyfr Cezara

To jest szyfr z kluczem, który trzeba znać, żeby szyfrować i odszyfrowywać. Kluczem w szyfrze Cezara jest liczba określająca **przesunięcie** w alfabecie:



SEZSRCSUNSRZMN

ALEA IACTA EST
 ↓
 = kości zostały rzucone

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.

Szyfrogram otrzymamy, odczytując go kolumnami.

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.

Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (?? znaków)

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.

Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.

Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMO

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIM

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIMOCĆAAU

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIMOCĆAAU, ,ŁS.

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIMOCĆAAU, ,ŁS. W T.

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIMOCĆAAU, ,ŁS. W T.MYWZ .

Proste przestawienia

„Szyfr dla dzieci” jest przykładem prościutkiego szyfru *przestawieniowego* (przestawiamy litery w słowie lub zdaniu).

Przykład: (inny przykład szyfru przestawieniowego)

Tekst jawny wpisujemy do kwadratowej tablicy wierszami.
Szyfrogram otrzymamy, odczytując go kolumnami.

tekst jawny (48 znaków):

KTO, MOGĄC WYBRAĆ, WYBRAŁ ZAMIAST DOMU...

tablica 7×7 miejsc:

K	T	O	,		M	O
G	Ą	C		W	Y	B
R	A	Ć	,		W	Y
B	R	A	Ł		Z	A
M	I	A	S	T		D
O	M	U	.	.	.	

szyfrogram:

KGRBMOTĄARIMOCĆAAU, ,ŁS. W T.MYWZ .OBYAD

Proste przestawienia

Szyfry przestawieniowe są słabe

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną,
- wypełnia się ją literami tekstu jawnego wg jakiejś zasady

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną,
- wypełnia się ją literami tekstu jawnego wg jakiejś zasady,
- poddaje się ją jakiemuś przekształceniu (np. obrotowi, lub odbiciu)

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną,
- wypełnia się ją literami tekstu jawnego wg jakiejś zasady,
- poddaje się ją jakiemuś przekształceniu (np. obrotowi, lub odbiciu),
- odczytuje się szyfrogram wg tej samej zasady z przekształconej figury.

Proste przestawienia

Szyfry przestawieniowe są słabe (= na ogół łatwe do złamania).

Można je trochę komplikować przez ustalanie bardziej skomplikowanych schematów przestawiania liter. Na ogół

- rysuje się jakąś figurę geometryczną,
- wypełnia się ją literami tekstu jawnego wg jakiejś zasady,
- poddaje się ją jakiemuś przekształceniu (np. obrotowi, lub odbiciu),
- odczytuje się szyfrogram wg tej samej zasady z przekształconej figury.

Współcześnie metody przestawieniowe stosuje się jako uzupełnienie innych metod szyfrowania.

Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Przykład: (inny przykład szyfru podstawieniowego)

Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Przykład: (inny przykład szyfru podstawieniowego)

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

Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Przykład: (inny przykład szyfru podstawieniowego)

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

W E S H A L L O V E R C O M E S O M E D A Y

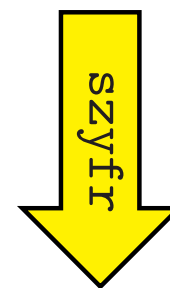
Proste podstawienia

„Szyfr Cezara” jest przykładem prościutkiego szyfru *podstawieniowego* (zastępujemy każdą literę inną literą lub znakiem).

Przykład: (inny przykład szyfru podstawieniowego)

A →	😊	O →	😡
B →	😁	P →	🐼
C →	😂	Q →	🐈
D →	😇	R →	🐕
E →	😍	S →	🦁
F →	😜	T →	🐪
G →	😎	U →	🐘
H →	😬	V →	🦇
I →	🤠	W →	🦔
J →	🎉	X →	🦘
K →	😎	Y →	🦆
L →	🧐	Z →	🐧
M →	😷	sp →	👩
N →	😡		

W E S H A L L O V E R C O M E S O M E D A Y



Proste podstawienia

Szyfry podstawieniowe również są słabe.

Proste podstawienia

Szyfry podstawieniowe również są słabe.

Do ich łamania stosuje się na ogół *analizę statystyczną*

Proste podstawienia

Szyfry podstawieniowe również są słabe.

Do ich łamania stosuje się na ogół *analizę statystyczną*:

- należy znać częstotliwość występowania liter w tekstach w danym języku

Proste podstawienia

Szyfry podstawieniowe również są słabe.

Do ich łamania stosuje się na ogół *analizę statystyczną*:

- należy znać częstotliwość występowania liter w tekstach w danym języku; np. w polskich tekstach:

A 8.965%	Ą 1.021%	B 1.482%	C 3.988%	Ć 0.448%	D 3.293%	E 7.921
Ę 1.131%	F 0.312%	G 1.377%	H 1.072%	I 8.286%	J 2.343%	K 3.411
L 2.136%	Ł 1.746%	M 2.911%	N 5.600%	Ń 0.185%	O 7.590%	Ó 0.823
P 3.101%	Q 0.003%	R 4.571%	S 4.263%	Ś 0.683%	T 3.966%	U 2.347
V 0.034%	W 4.549%	X 0.019%	Y 3.857%	Z 5.620%	Ż 0.061%	Ź 0.885

Proste podstawienia

Szyfry podstawieniowe również są słabe.

Do ich łamania stosuje się na ogół *analizę statystyczną*:

- należy znać częstotliwość występowania liter w tekstach w danym języku; np. w polskich tekstach:

A 8.965%	Ą 1.021%	B 1.482%	C 3.988%	Ć 0.448%	D 3.293%	E 7.921
Ę 1.131%	F 0.312%	G 1.377%	H 1.072%	I 8.286%	J 2.343%	K 3.411
L 2.136%	Ł 1.746%	M 2.911%	N 5.600%	Ń 0.185%	O 7.590%	Ó 0.823
P 3.101%	Q 0.003%	R 4.571%	S 4.263%	Ś 0.683%	T 3.966%	U 2.347
V 0.034%	W 4.549%	X 0.019%	Y 3.857%	Z 5.620%	Ż 0.061%	Ź 0.885

- sprawdzić częstotliwość występowania znaków w szyfrogramie

Proste podstawienia

Szyfry podstawieniowe również są słabe.

Do ich łamania stosuje się na ogół *analizę statystyczną*:

- należy znać częstotliwość występowania liter w tekstach w danym języku; np. w polskich tekstach:

A 8.965%	Ą 1.021%	B 1.482%	C 3.988%	Ć 0.448%	D 3.293%	E 7.921
Ę 1.131%	F 0.312%	G 1.377%	H 1.072%	I 8.286%	J 2.343%	K 3.411
L 2.136%	Ł 1.746%	M 2.911%	N 5.600%	Ń 0.185%	O 7.590%	Ó 0.823
P 3.101%	Q 0.003%	R 4.571%	S 4.263%	Ś 0.683%	T 3.966%	U 2.347
V 0.034%	W 4.549%	X 0.019%	Y 3.857%	Z 5.620%	Ż 0.061%	Ź 0.885

- sprawdzić częstotliwość występowania znaków w szyfrogramie,
- dopasować jedno do drugiego.

Podstawienia z kluczem

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N	14
A 1	O	15
B 2	P	16
C 3	Q	17
D 4	R	18
E 5	S	19
F 6	T	20
G 7	U	21
H 8	V	22
I 9	W	23
J 10	X	24
K 11	Y	25
L 12	Z	26
M 13		

tekst jawny:	
nry liter:	
klucz:	B U K I E T Y W I E J S K I E J A K . .
nry liter:	
sumy mod 27:	
szyfrogram:	

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

	0	N	14
A	1	O	15
B	2	P	16
C	3	Q	17
D	4	R	18
E	5	S	19
F	6	T	20
G	7	U	21
H	8	V	22
I	9	W	23
J	10	X	24
K	11	Y	25
L	12	Z	26
M	13		

tekst jawny:	
nry liter:	
klucz:	B U K I E T Y W I E J S K I E J A K . .
nry liter:	2 22 11 9 5 20 25 0 23 9 5 10 19 11 9 5 0 10 1 11 .
sumy mod 27:	
szyfrogram:	

Przykład: (klucz: „Kwiaty polskie” Tuwima)

tekst jawny:	K O C H A M C I E S K R Y C I E
nry liter:	
klucz:	B U K I E T Y W I E J S K I E J A K . .
nry liter:	2 22 11 9 5 20 25 0 23 9 5 10 19 11 9 5 0 10 1 11 .
sumy mod 27:	
szyfrogram:	

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N	14
A 1	O	15
B 2	P	16
C 3	Q	17
D 4	R	18
E 5	S	19
F 6	T	20
G 7	U	21
H 8	V	22
I 9	W	23
J 10	X	24
K 11	Y	25
L 12	Z	26
M 13		

tekst jawny:	K O C H A M C I E S K R Y C I E
nry liter:	11 15 3 8 1 13 0 3 9 5 0 19 11 18 25 3 9 5
klucz:	B U K I E T Y W I E J S K I E J A K . .
nry liter:	2 22 11 9 5 20 25 0 23 9 5 10 19 11 9 5 0 10 1 11 .
sumy mod 27:	
szyfrogram:	

Przykład: (klucz: „Kwiaty polskie” Tuwima)

tekst jawny:	K O C H A M C I E S K R Y C I E
nry liter:	11 15 3 8 1 13 0 3 9 5 0 19 11 18 25 3 9 5
klucz:	B U K I E T Y W I E J S K I E J A K . .
nry liter:	2 22 11 9 5 20 25 0 23 9 5 10 19 11 9 5 0 10 1 11 .
sumy mod 27:	13 10 14 17 6 6 25 3 5 14 5 2 3 2 7 8 9 15
szyfrogram:	

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

	0	N	14
A	1	O	15
B	2	P	16
C	3	Q	17
D	4	R	18
E	5	S	19
F	6	T	20
G	7	U	21
H	8	V	22
I	9	W	23
J	10	X	24
K	11	Y	25
L	12	Z	26
M	13		

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5
klucz:	B	U	K	I	E	T	Y	W	I	E	J	S	K	I	E	J	A	K
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N	14
A 1	O	15
B 2	P	16
C 3	Q	17
D 4	R	18
E 5	S	19
F 6	T	20
G 7	U	21
H 8	V	22
I 9	W	23
J 10	X	24
K 11	Y	25
L 12	Z	26
M 13		

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N 14
A 1	O 15
B 2	P 16
C 3	Q 17
D 4	R 18
E 5	S 19
F 6	T 20
G 7	U 21
H 8	V 22
I 9	W 23
J 10	X 24
K 11	Y 25
L 12	Z 26
M 13	

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N	14
A 1	O	15
B 2	P	16
C 3	Q	17
D 4	R	18
E 5	S	19
F 6	T	20
G 7	U	21
H 8	V	22
I 9	W	23
J 10	X	24
K 11	Y	25
L 12	Z	26
M 13		

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

C → C

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N 14
A 1	O 15
B 2	P 16
C 3	Q 17
D 4	R 18
E 5	S 19
F 6	T 20
G 7	U 21
H 8	V 22
I 9	W 23
J 10	X 24
K 11	Y 25
L 12	Z 26
M 13	

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

C → C

C → H

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N 14
A 1	O 15
B 2	P 16
C 3	Q 17
D 4	R 18
E 5	S 19
F 6	T 20
G 7	U 21
H 8	V 22
I 9	W 23
J 10	X 24
K 11	Y 25
L 12	Z 26
M 13	

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

C → C

C → H

Nikt oprócz nadawcy i odbiorcy nie powinien znać klucza.

Podstawienia z kluczem

— za każdą literę podstawiać inną, ale nie zawsze tą samą, tylko wg *klucza*, którym może być dowolny dłuższy tekst.

Przykład: (klucz: „Kwiaty polskie” Tuwima)

ALFABET

0	N	14
A 1	O	15
B 2	P	16
C 3	Q	17
D 4	R	18
E 5	S	19
F 6	T	20
G 7	U	21
H 8	V	22
I 9	W	23
J 10	X	24
K 11	Y	25
L 12	Z	26
M 13		

tekst jawny:	K	O	C	H	A	M		C	I	E		S	K	R	Y	C	I	E			
nry liter:	11	15	3	8	1	13	0	3	9	5	0	19	11	18	25	3	9	5			
klucz:	B	U	K	I	E	T	Y		W	I	E	J	S	K	I	E		J	A	K	..
nry liter:	2	22	11	9	5	20	25	0	23	9	5	10	19	11	9	5	0	10	1	11	.
sumy mod 27:	13	10	14	17	6	6	25	3	5	14	5	2	3	2	7	8	9	15			
szyfrogram:	M	J	N	Q	F	F	Y	C	E	N	E	B	C	B	G	H	I	O			

Te same litery są kodowane różnie zależnie od klucza; np.

C → N

C → C

C → H

To jest lekko zmieniony
szyfr Vigenère'a z 1553
„le chiffre indéchiffrable”

Nikt oprócz nadawcy i odbiorcy nie powinien znać klucza.

Szyfrowanie systemem arcyksięcia Albrechta

Szyfrowanie systemem arcyksięcia Albrechta

Jaroslav Hašek „Przygody dobrego wojaka Szwejka” t. III, rozdz. I

— Mówiłem już o nowym sposobie szyfrowania depesz w polu, a jeśli panowie nie wiedzieli, dlaczego polecono wam właśnie jedną z nowel Ludwika Ganghofer'a, *Die Sünden der Väter*, stronica 161, to dodam, że to jest klucz do tej nowej metody, obowiązującej na podstawie nowego rozporządzenia sztabu korpusu, do którego zostaliśmy przydzieleni.

Jeśli na przykład dostaniemy rozkaz: „*Auf der Kote 228, Maschinengewehrfeuer linksrichten*” — to otrzymujemy, moi panowie, taką depeszę:

„*Sache... mit... uns... das... wir... aufsehen... in... die...*

wirklich... denke... Idee... ganz... herrscht... Stimme... letzten”.

Bierze *Die Sünden der Väter*, otwiera książkę na stronicy 161 i szuka na górze na przeciwległej stronicy, 160, słowa „Sache”. Proszę panów, po raz pierwszy słowo „Sache” znajdujemy na stronicy 160, jako kolejne słowo 52, więc na przeciwległej stronicy 161 odszukujemy 52 literę na górze, Zauważmy, że jest to litera „a”. Dalszym słowem depeszy jest

Szyfrowanie systemem arcyksięcia Albrechta

Jaroslav Hašek „Przygody dobrego wojaka Szwejka” t. III, rozdz. I

— Mówiłem już o nowym sposobie szyfrowania depesz w polu, a jeśli panowie nie wiedzieli, dlaczego polecono wam właśnie jedną z nowel Ludwika Ganghofer'a, *Die Sünden der Väter*, stronica 161, to dodam, że to jest klucz do tej nowej metody, obowiązującej na podstawie nowego rozporządzenia sztabu korpusu, do którego zostaliśmy przydzieleni.

Jeśli na przykład dostaniemy rozkaz: „*Auf der Kote 228, Maschinengewehrfeuer linksrichten*” — to otrzymujemy, moi panowie, taką depeszę:

„*Sache... mit... uns... das... wir... aufsehen... in... die...*

wirklich... denke... Idee... ganz... herrscht... Stimme... letzten”.

Bierze *Die Sünden der Väter*, otwiera książkę na stronicy 161 i szuka na górze na przeciwległej stronicy, 160, słowa „Sache”. Proszę panów, po raz pierwszy słowo „Sache” znajdujemy na stronicy 160, jako kolejne słowo 52, więc na przeciwległej stronicy 161 odszukujemy 52 literę na górze, Zauważmy, że jest to litera „a”. Dalszym słowem depeszy jest

„Grzechy ojców”

Szyfrowanie systemem arcyksięcia Albrechta

Jaroslav Hašek „Przygody dobrego wojaka Szwejka” t. III, rozdz. I

— Mówiłem już o nowym sposobie szyfrowania depesz w polu, a jeśli panowie nie wiedzieli, dlaczego polecono wam właśnie jedną z nowel Ludwika Ganghofer’a, *Die Sünden der Väter*, stronica 161, to dodam, że to jest klucz do tej nowej metody, obowiązującej na podstawie nowego rozporządzenia sztabu korpusu, do którego zostaliśmy przydzieleni.

Jeśli na przykład dostaniemy rozkaz: „*Auf der Kote 228, Maschinengewehrfeuer linksrichten*” — to otrzymujemy, moi panowie, taką depeszę:

„*Sache... mit... uns... das... wir... aufsehen... in... die...*

wirklich... denke... Idee... ganz... herrscht... Stimme... letzten”.

Bierze *Die Sünden der Väter*, otwiera książkę na stronicy 161 i szuka na górze na przeciwległej stronicy, 160, słowa „Sache”. Proszę panów, po raz pierwszy słowo „Sache” znajdujemy na stronicy 160, jako kolejne słowo 52, więc na przeciwległej stronicy 161 odszukujemy 52 literę na górze, Zauważmy, że jest to litera „a”. Dalszym słowem depeszy jest

„Grzechy ojców”

„Na wzgórzu 228
ogień karabinów
maszynowych
kierować w lewo”

Szyfrowanie systemem arcyksięcia Albrechta

Jaroslav Hašek „Przygody dobrego wojaka Szwejka” t. III, rozdz. I

— Mówiłem już o nowym sposobie szyfrowania depesz w polu, a jeśli panowie nie wiedzieli, dlaczego polecono wam właśnie jedną z nowel Ludwika Ganghofer'a, *Die Sünden der Väter*, stronica 161, to dodam, że to jest klucz do tej nowej metody, obowiązującej na podstawie nowego rozporządzenia sztabu korpusu, do którego zostaliśmy przydzieleni.

Jeśli na przykład dostaniemy rozkaz: „*Auf der Kote 228, Maschinengewehrfeuer linksrichten*” — to otrzymujemy, moi panowie, taką depeszę:

„*Sache... mit... uns... das... wir... aufsehen... in... die...*

wirklich... denke... Idee... ganz... herrscht... Stimme... letzten”.

Bierze *Die Sünden der Väter*, otwiera książkę na stronicy 161 i szuka na górze na przeciwległej stronicy, 160, słowa „Sache”. Proszę panów, po raz pierwszy słowo „Sache” znajdujemy na stronicy 160, jako kolejne słowo 52, więc na przeciwległej stronicy 161 odszukujemy 52 literę na górze, Zauważmy, że jest to litera „a”. Dalszym słowem depeszy jest

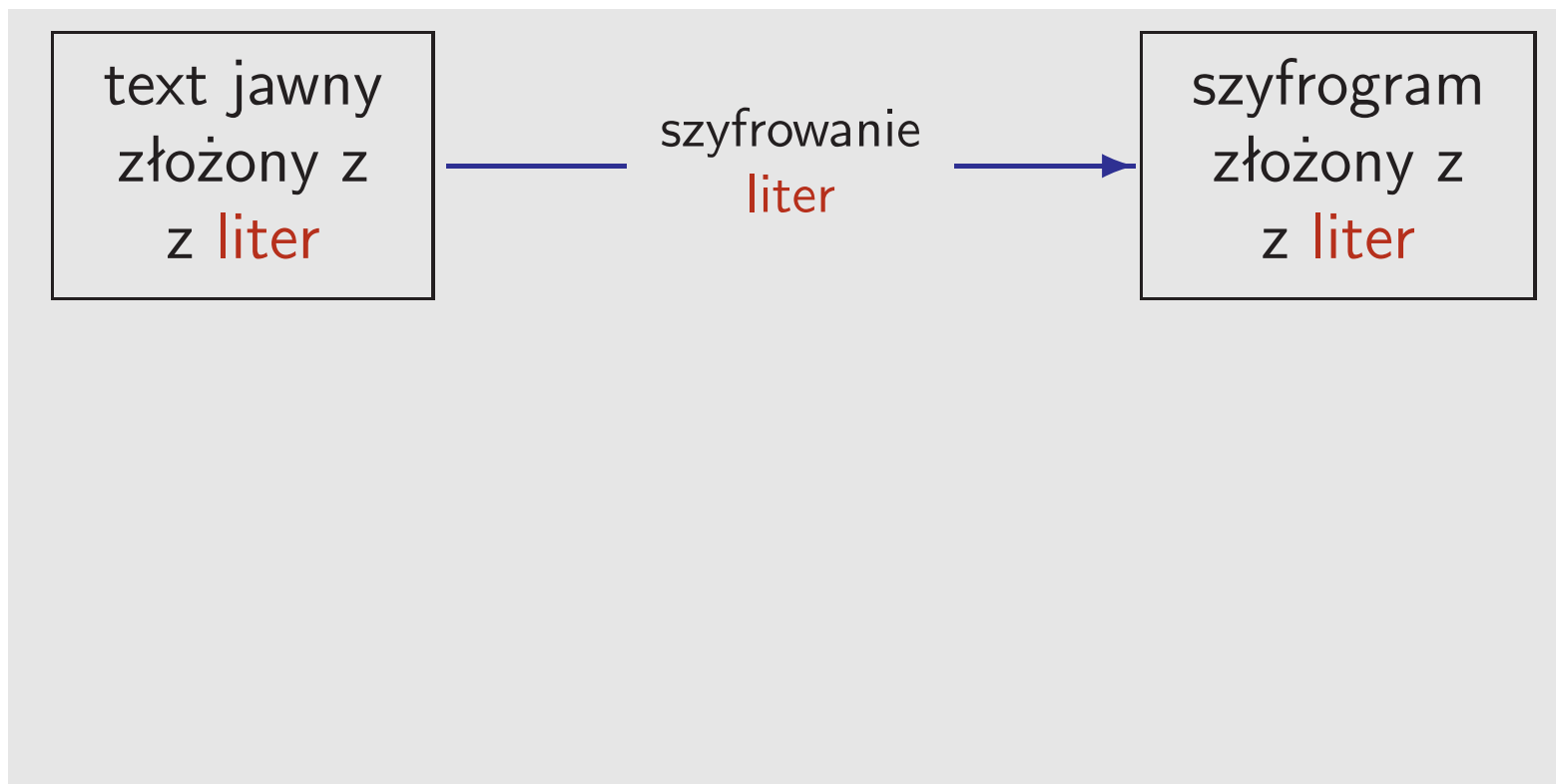
„Grzechy ojców”

„Na wzgórzu 228
ogień karabinów
maszynowych
kierować w lewo”

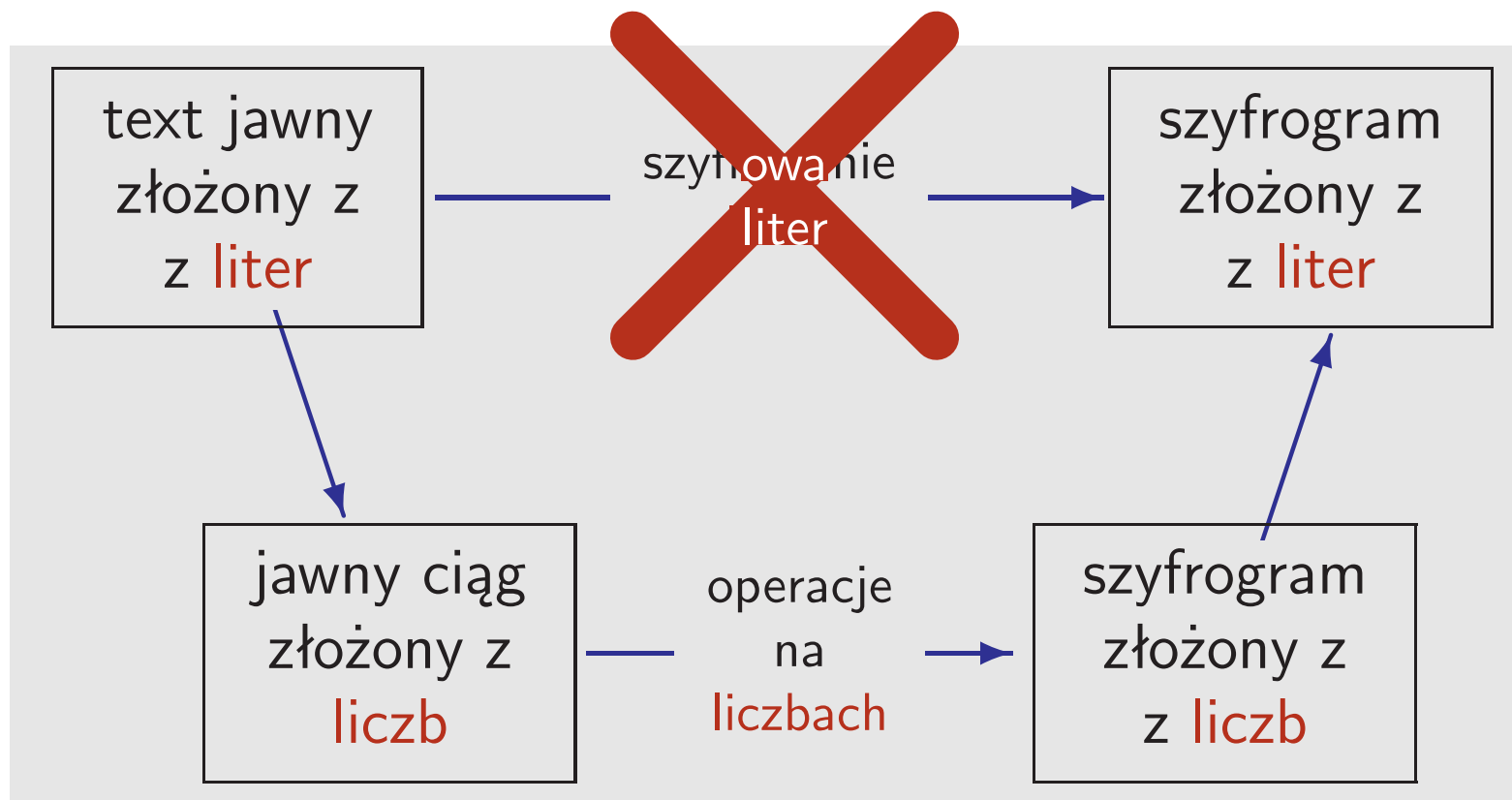
To jest szyfr **podstawieniowy** — słowa za litery
wg klucza, którym jest fragment powieści

Matematyka i informatyka w szyfrowaniu

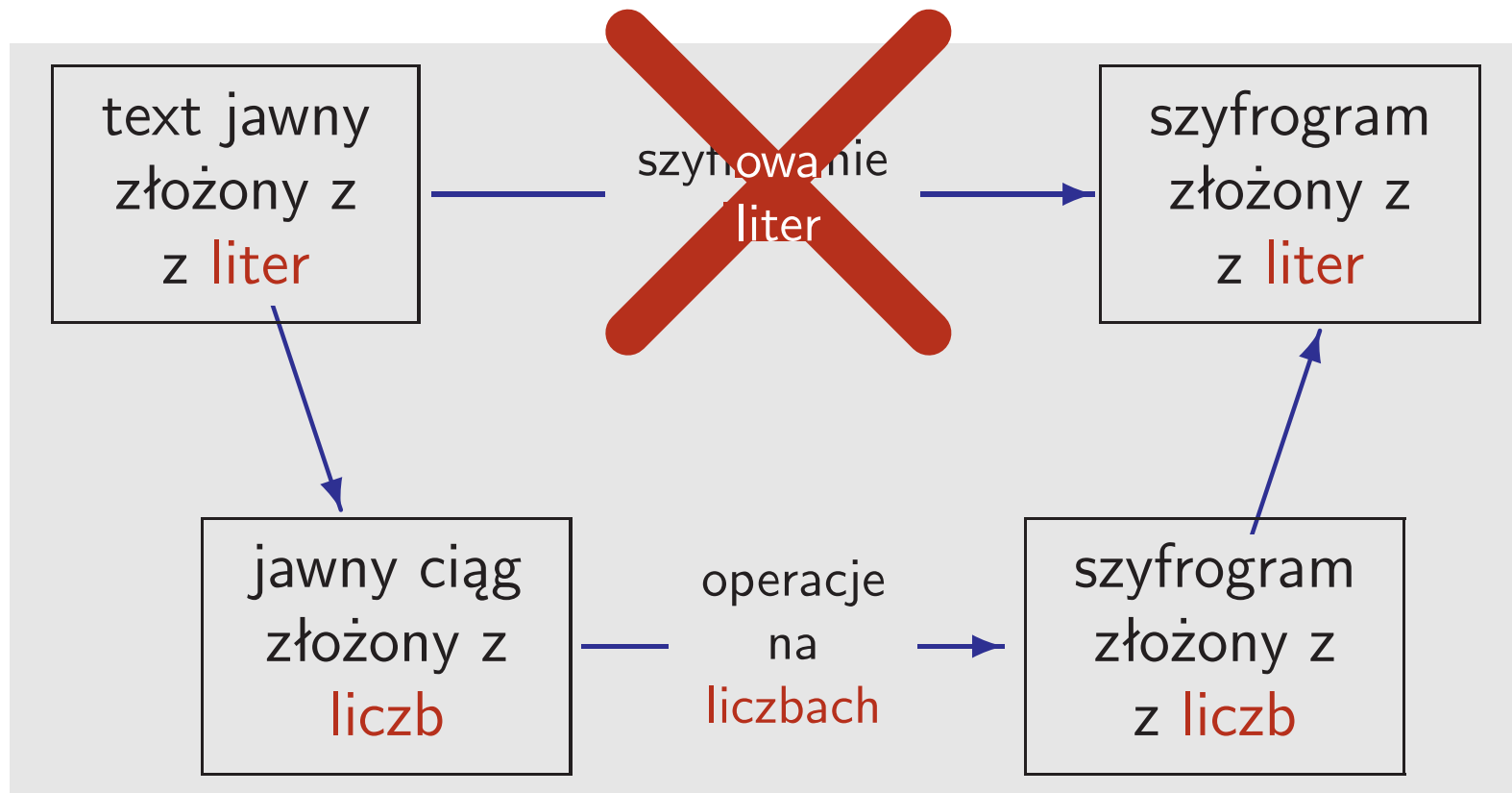
Matematyka i informatyka w szyfrowaniu



Matematyka i informatyka w szyfrowaniu

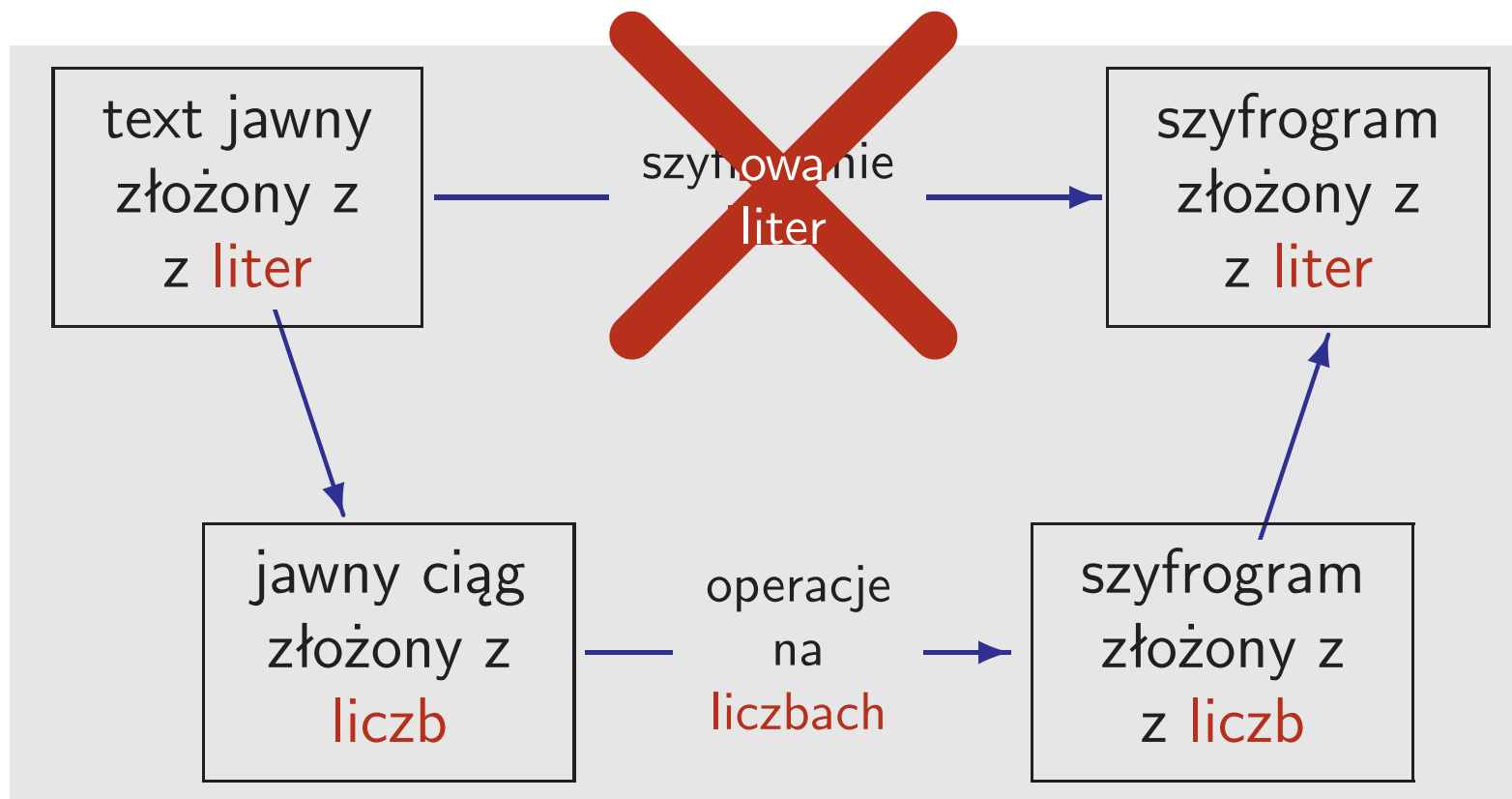


Matematyka i informatyka w szyfrowaniu



Zasady przekształcania liczb są łatwiejsze do zaprogramowania niż zasady przekształcania tekstów.

Matematyka i informatyka w szyfrowaniu



Zasady przekształcania liczb są łatwiejsze do zaprogramowania niż zasady przekształcania tekstów.

O przekształcaniu liczb łatwiej jest rozumować niż o przekształcaniu tekstów.

Matematyka i informatyka w szyfrowaniu

char — 8 bitów }
int — 32 bity }

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
int — 32 bity }

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

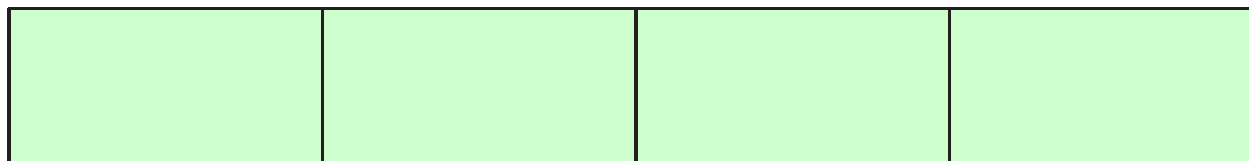
```
liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
```

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```
liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
```

Zapisujemy litery **ROK3** :



Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	same zera	same zera	same zera
--------------	--------------	--------------	--------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```
liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
```

Zapisujemy litery **ROK3** :

same zera	same zera	same zera	same zera
--------------	--------------	--------------	--------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	same zera	same zera	kod ascii R 82
--------------	--------------	--------------	--------------------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	same zera	kod ascii R 82	same zera
--------------	--------------	--------------------------	--------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	same zera	kod ascii R 82	kod ascii O 79
--------------	--------------	--------------------------	--------------------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	kod ascii R 82	kod ascii O 79	same zera
--------------	--------------------------	--------------------------	--------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

same zera	kod ascii R 82	kod ascii O 79	kod ascii K 75
--------------	--------------------------	--------------------------	--------------------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

kod ascii R 82	kod ascii O 79	kod ascii K 75	same zera
--------------------------	--------------------------	--------------------------	--------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

kod ascii R 82	kod ascii O 79	kod ascii K 75	kod ascii 3 51
--------------------------	--------------------------	--------------------------	--------------------------

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

kod ascii R	kod ascii O	kod ascii K	kod ascii 3
82	79	75	51

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```
liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
```

Zapisujemy litery **ROK3** :

kod ascii R	kod ascii O	kod ascii K	kod ascii 3
82	79	75	51

Wynik:

$$((82 \cdot 256 + 79) \cdot 256 + 75) \cdot 256 + 51$$

Matematyka i informatyka w szyfrowaniu

char — 8 bitów } — jak *umieścić* 4 litery w liczbie całkowitej?
 int — 32 bity } — jak *wydobyć* 4 litery z liczby całkowitej?

```

liczba = 0;
for(i=0; i<4; i++) {
    liczba = liczba*256; // przesunięcie w lewo o 8 bitów
    liczba = liczba+(char)litera[i];
    // wstawienie kolejnej litery
    // w wolne 8 bitów na prawym końcu liczby
}
  
```

Zapisujemy litery **ROK3** :

kod ascii R	kod ascii O	kod ascii K	kod ascii 3
82	79	75	51

Wynik:

$$((82 \cdot 256 + 79) \cdot 256 + 75) \cdot 256 + 33 = 1\,380\,928\,307$$