



**POLITECHNIKA BIAŁOSTOCKA**  
**WYDZIAŁ INFORMATYKI**  
**Bezpieczeństwo sieci komputerowych**

**PRACOWNIA SPECJALISTYCZNA 2-3**  
**DR INŻ. MACIEJ BRZozowski**

**TEMAT: IMPLEMENTACJA PODSTAWOWYCH MODUŁÓW KRYPTOGRAFICZNYCH.**

**Przykład 1. Rail fence**

M = CRYPTOGRAPHY, n=3

C			T		A		
	R		P		O		R
		Y		G		P	Y
				H			

C = CTARPORPYGH

**Przykład 2a. Przetawienia macierzowe**

M = CRYPTOGRAPHYOSA, key=3-1-4-2

	1	2	3	4
C	R	Y	P	
T	O	G	R	
A	P	H	Y	
O	S	A		

C = YCPRGTROHAYPAOS<sup>1</sup>

**Przykład 2b.**

M=HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION<sup>2</sup>

Key=CONVENIENCE

C	O	N	V	E	N	I	E	N	C	E
1	10	7	11	3	8	6	4	9	2	5
H	E	R	E	I	S	A	S	E	C	R
E	T	M	E	S	S	A	G	E	E	N
C	I	P	H	E	R	E	D	B	Y	T
R	A	N	S	P	O	S	I	T	I	O
N										

C=HECRN CEYI ISEP SGDI RNT0 AAES RMPN SSRO EEBT ETIA EEHS<sup>3</sup>

<sup>1</sup>Proszę zwrócić uwagę na prawidłowe zaszyfrowanie i rozszyfrowanie niepełnego bloku!

<sup>2</sup>W powyższym rozwiązaniu znaki białe zostały usunięte w celu zwiększenia czytelności przykładu.

<sup>3</sup>W powyższym rozwiązaniu znaki białe zostały wstawione w celu zwiększenia czytelności przykładu. W implementacjach autorskich powyższe znaki białe mają niewystępować!

Przykład 2c.

C	O	N	V	E	N	I	E	N	C	E
1	10	7	11	3	8	6	4	9	2	5
H										
E	R	E	I	S	A	S	E	C	R	
E	T	M	E	S						
S	A	G	E	E	N	C	I			
P	H	E	R	E	D	B	Y	T	R	A
N	S	P	O	S	I	T				
I	O	N								

C=HEESPNI RR SSEES EIY A SCBT EMGEPN ANDI CT RTAHSO IEERO<sup>4</sup>

Przykład 3a. **Szyfrowanie cezara (Caesar cipher)**

szyfrowanie:  $c = (a + k) \bmod n$   
deszyfrowanie:  $a = [c + (n - k)] \bmod n$

gdzie:

- n - liczba znaków w alfabecie
- k - klucz
- c - znak do zaszyfrowania
- a - znak zaszyfrowany

Dla  $k=3$  oraz wiadomości jawnej  $M = \text{CRYPTOGRAPHY}$  otrzymujemy  $EK(M) = \text{FUBSWRJUDSKB}$

Przykład 3b. **Szyfrowanie cezara (Caesar cipher)**

szyfrowanie:  $c = (a * k_1 + k_0) \bmod n$   
deszyfrowanie:  $a = [c + (n - k_0)] k_1^{\varphi(n) - 1} \bmod n$

dla  $n=21$   $\varphi(n)=12$

$k_1, k_0$  muszą być pierwsze względem  $n$ .

---

<sup>4</sup>W powyższym rozwiązaniu znaki białe zostały wstawione w celu zwiększenia czytelności przykładu. W implementacjach autorskich powyższe znaki białe mają niewystępować! Proszę zwrócić uwagę na prawidłowe szyfrowanie oraz deszyfrowanie tekstu przy niepełnych blokach!

#### Przykład 4. Szyfrowanie Vigenere'a

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

Dla litery tekstu jawnego  $a$  i klucza  $k$ , zaszyfrowany tekst  $c$  jest literą w kolumnie  $a$  i wierszu  $k$ .  
Dla szyfrogramu  $c$ , plaintext  $a$  jest kolumną zawierającą  $c$  w wierszu  $k$ .

$M = \text{CRYPTOGRAPHY}$   
 $K = \text{BREAKBREAKBR}$   
 $EK(M) = \text{DICDPXVAZIP}$

#### Zadania (maksymalnie 7 punktów):

1. Zaimplementuj algorytm kodujący i dekodujący z wykorzystaniem szyfru prostego przestawiania „rail fence” dla  $k = n$ . Skorzystaj z przykładu 1 (1 punkt).
2. Zaimplementuj kryptosystem przedstawieniowy bazujący na przykładzie 2a dla  $d = 5$  oraz klucza  $key = 3-4-1-5-2$  (1 punkt).
3. Zaimplementuj kryptosystem przedstawieniowy bazujący na przykładzie 2b (1 punkt) oraz 2c (2 punkty) dla dowolnego klucza.
4. Zaimplementuj szyfr cezara bazując na przykładzie 3b (1 punkt).
5. Zaimplementuj kryptosystem bazujący na tablicy Vigenere’a (1 punkt).