Bezpieczeństwo systemów komputerowych

Raport z laboratorium nr 1 – cz. 2.

Klasyczne systemy kryptograficzne

1. Monoalfabetyczny szyfr Cezara

Każda litera tekstu niezaszyfrowanego zastępowana jest inną, oddaloną od niej o stałą liczbę pozycji w alfabecie, przy czym kierunek zamiany musi być zachowany.

Dla przesunięcia o **5** tablica szyfru ma postać:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
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

Tablica zaszyfrowana:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
5	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**0**	**1**	**2**	**3**	**4**
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

2. Przesunięty szyfr przerzedzony

Szyfr oparty na przesunięciu liter alfabetu w prawo o **k** pozycji modulo zgodnie ze wzorem:

$$f(a) = (a * k) mod\ \boldsymbol{n}$$

a – szyfrowana litera, **k** – klucz, **n** – liczba liter w alfabecie

Dla przesunięcia o **9** tablica szyfru ma postać:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
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

Tablica zaszyfrowana:

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
0	**9**	**18**	**1**	**10**	**19**	**2**	**11**	**20**	**3**	**12**	**21**	**4**	**13**	**12**	**5**	**14**	**23**	**6**	**15**	**24**	**7**	**16**	**25**	**8**	**17**
a	j	s	b	k	t	c	l	u	d	m	v	e	n	w	f	o	x	g	p	y	h	q	z	i	r

3. Wieloalfabetyczny szyfr Vigenère'a

Działanie szyfru Vigenère'a opiera się na następującej tablicy:

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Szyfr oparty na wykorzystaniu klucza szyfrowania K = $k_1 \ldots k_n$ będącego sekwencją liter. Liczba przesunięć w **i**-tym alfabecie określana jest przez $k_i = (i = 1,\ldots,d)$. Szyfrowanie opiera się zatem na wykorzystaniu formuły:

$$f(a) = (a + k_i)\ mod\ \boldsymbol{n}$$

Tekst jawny	S	Z	Y	F	R
Klucz	N	I	C	N	I
Tekst zaszyfrowany	F	H	A	S	Z

4. Szyfr Homofoniczny

Każdej literze alfabetu przypisuje się liczbę homofonów zależną od częstości występowania litery w tekście.

Litera	Homofony					
S	17	19	34	41	60	83
T	08	22	53	65	90	
U	03	44	76	27	40	80
D	02	09	15	28	54	78
E	01	11	23	29		
N	33	91	20			

Tekst jawny	**S**	**T**	**U**	**D**	**E**	**N**	**T**
Tekst zaszyfrowany	17	08	03	02	01	33	22

albo

Tekst zaszyfrowany	34	22	40	54	11	91	65

albo

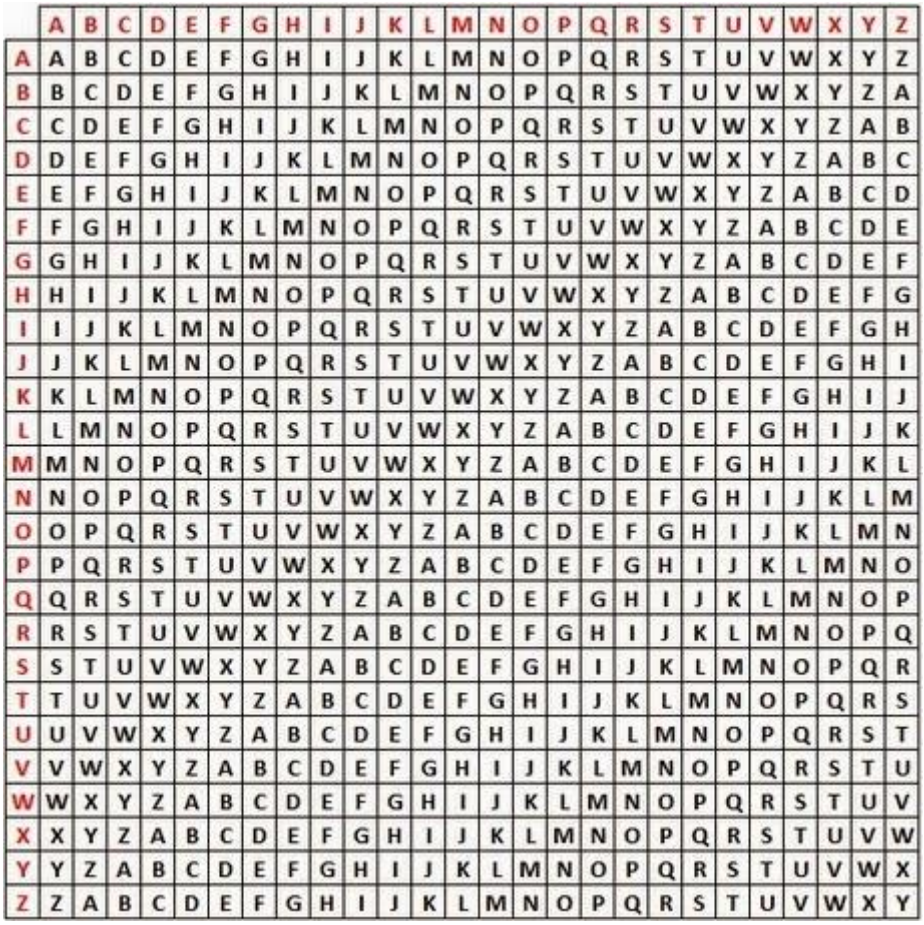
Tekst zaszyfrowany	19	90	27	15	23	20	08

5. Wieloalfabetyczny szyfr Beaufort’a

Podobnie jak szyfr Vigenère’a algorytm szyfrowania polega na zamienianiu kolejnych liter tekstu jawnego, na litery wskazane przez tablicę. Strony dysponują wspólnym sekretnym kluczem, którym może być jedno lub parę słów.

Działanie szyfru opisuje wzór:

$$f(a) = (k_i - a) mod\ \boldsymbol{n}$$



	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

Tekst jawny	**S**	**T**	**U**	**D**	**E**	**N**	**T**
Klucz	K	L	U	C	Z	K	L
Tekst zaszyfrowany	C	E	O	F	D	X	E

6. Transpozycyjny szyfr płotu

Do szyfrowania wykorzystuje się figurę geometryczną, najczęściej macierz dwuwymiarową. Tekst jawny może zostać wpisany wierszami, odczytany zaś kolumnami ze wskazaną kolejnością.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
P	O	L	I	T	E	C	H
N	I	K	A	P	O	L	I
T	E	C	H	N	I	K	-

Przy odczycie kolumn w kolejności 2-6-1-3-5-4-8-7 zaszyfrowany tekst ma postać:
OIEEOIPNTLKCTPNIAHHI-CKL

7. Szyfrowanie strumieniowe XOR

Jednym z szyfrów strumieniowych jest szyfrowanie znaków algorytmem **XOR**. Każdy znak szyfrowany jest za pomocą wybranego przez użytkownika klucza np.: `0111 0001`

Bin	Dec	Hex	Znak	Bin	Dec	Hex	Znak
0100 0000	64	40	@	0100 1110	78	4E	N
0100 0001	65	41	A	0100 1111	79	4F	O
0100 0010	66	42	B	0101 0000	80	50	P
0100 0011	67	43	C	0101 0001	81	51	Q
0100 0100	68	44	D	0101 0010	82	52	R
0100 0101	69	45	E	0101 0011	83	53	S
0100 0110	70	46	F	0101 0100	84	54	T
0100 0111	71	47	G	0101 0101	85	55	U
0100 1000	72	48	H	0101 0110	86	56	V
0100 1001	73	49	I	0101 0111	87	57	W
0100 1010	74	4A	J	0101 1000	88	58	X
0100 1011	75	4B	K	0101 1001	89	59	Y
0100 1100	76	4C	L	0101 1010	90	5A	Z
0100 1101	77	4D	M				

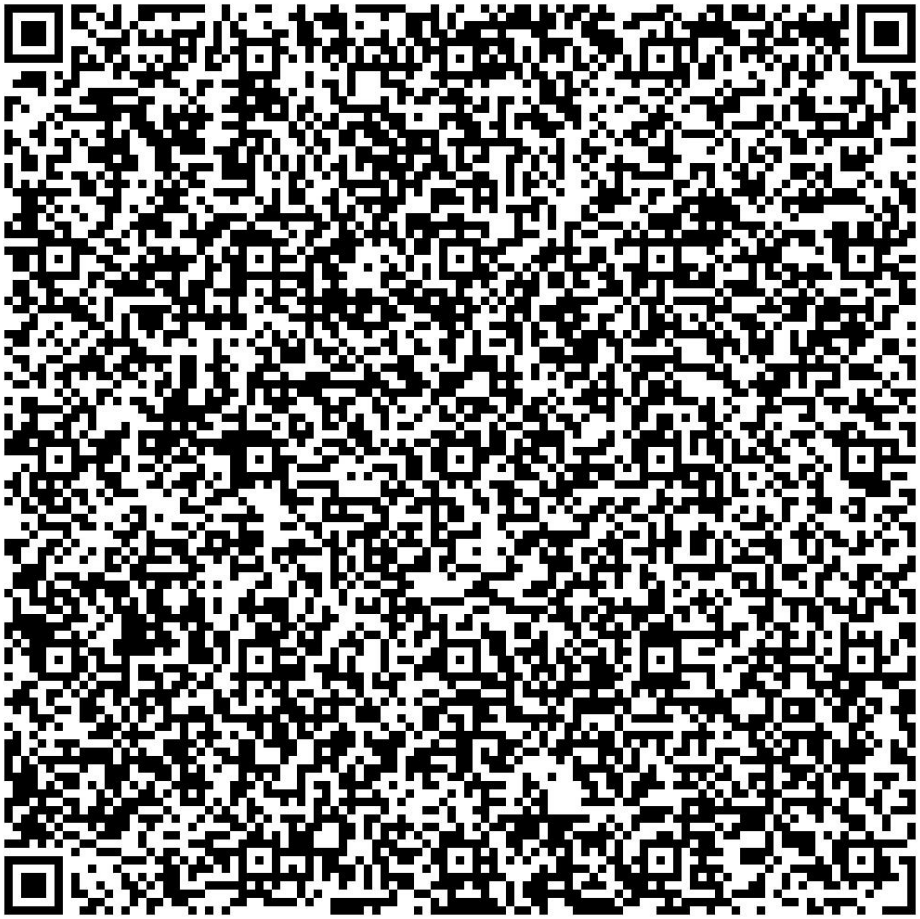
8. Szyfr Cmentarny

9. Kod QR

Do szyfrowania danych mogą służyć kody QR. Pozwalają one na zapisanie dużej ilości danych. Maksymalna ilość danych możliwa do zapisania w jednym kodzie jest zmienna.

Zadania do samodzielnego wykonania

1. Wykorzystując poznane algorytmy szyfrowania wykonaj operacje zaszyfrowania swojego **imienia** i **nazwiska** za pomocą:
    a. Figury macierzy 3x3, 3x4, 3x5 itp. w zależności od długości szyfrowanego tekstu
    b. Monoalfabetycznego szyfru Cezara o długości klucza podanego przez prowadzącego
    c. Szyfru homofoniczny
    d. Szyfru Cmentarnego
    e. Szyfru Beaufort'a , klucz **epidemia**
    f. Szyfru Vinegere'a, klucz **epidemia**
    g. Szyfru XOR o kluczu `0100 1100`
    h. Zaproponuj swój własny szyfr.
2. Jeśli masz możliwość, spróbuj odszyfrować poniższy kod QR:



3. Wykorzystując generator kodów QR online zaszyfruj dowolny tekst.