Wszechświat liczb
2. Układ całkowity
Kodowanie i szyfrowanie symetryczne
skrypt warsztatowy

spisał: Michał Korch

6 maja 2017

Na rozgrzewkę!

Każdy z Was pewnie bawił się w szyfrowanie prostych wiadomości, głównie dla zabawy. Takie proste szyfry można przy odrobinie wysiłku odszyfrować nawet nie znając zasad, wedle których zostały zaszyfrowane. Dlatego może lepiej o nich mówić, że to kodowanie. Niemniej niekiedy robią się z tego niezłe łamigłówki. Spróbujcie rozszyfrować napis na załączonej kartce.

W razie czego pewne wskazówki możecie uzyskać u prowadzącego!

Użyto tu alfabetu bez polskich znaków, za to z q, v i x.

Szyfrowanie graficzne

W materiałach znajdziecie dwa paski papieru z narysowanymi tajemniczymi zaciemnionymi kwadratami. Każdy z kawałków papieru jest połową pewnego sekretu. Mając tylko jeden z nich nie da się wymyślić, co jest tu zaszyfrowane. Mając jednak oba kawałki papieru, można to zrobić z relatywną łatwością. Co jest tam napisane?

Zanalizujcie, jak działa ta metoda szyfrowania. Zauważcie, że każdy piksel oryginalnego obrazka odpowiada czterem pikselom na poszczególnym szyfrogramie. Opiszcie, w jaki sposób zaszyfrować dany obrazek.

Narysujcie obrazek, na kratkowanej kartce o dużych polach zaczerniając piksele. Zaszyfrujcie je w postaci dwóch kartek (załączam więcej kartek na wszelki wypadek).

Szyfr Cezara

Najprostszym szyfrem podstawieniowym jest szyfr Cezara. Polega on na tym, że każdą literę zmieniamy na literę stojącą o k pozycji dalej w alfabecie. Dla ustalenia uwagi, będziemy używać polskiego alfabetu:

AĄBCĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻ

Czyli np. dla $k = 3$ każda litera A zostanie zaszyfrowana jako C, zaś G jako J. Natomiast Z zostanie wtedy zaszyfrowane jako A, Ż jako B. Szyfr Cezara nie jest jednak trudny do złamania, nawet jeśli nie znamy liczby k. Rozszyfruj poniższy napis:

ŹPŁŻHUWAZHZ GĄŁHĘŁ

Szyfr Vigenère'a

Szyfr Vigenère'a jest poprawioną wersją szyfry Cezara. Aby skorzystać z tego szyfru wygodnie mieć następującą tablicę:

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

Rolę liczby k odgrywa tutaj tajny klucz w postaci jakiegoś słowa lub tekstu. Dla przykładu weźmy klucz TAJNE. Chcąc zaszyfrować jakiś tekst, np: SZYFR VIGENEREA, trzeba znaleźć litery w kolumnie odpowiadającej kolejnym literom klucza (w razie czego go zapętlając) i wierszu odpowiadającym odpowiednim literom szyfrowanej wiadomości. W tym wypadku wyjdzie:

LZHSV OIPRRXRNN

Niech teraz każdy z Was zaszyfruje swoje imię korzystając z szyfru Vigenère'a z kluczem UNIWERSYTET.

Wasz szyfr

Podzielcie się teraz na dwie grupy. Niech każda z grup wymyśli jakąś ciekawą metodę szyfrowania wiadomości. Zaszyfrujcie tą metodą wybrany napis w tajemnicy przed drugą grupą i wymieńcie się szyfrogramami i spróbujcie złamać swoje szyfry.

Możecie udzielać sobie wskazówek prowadzących do rozwiązania.