Радни лист – B05
Вежбе из моно-алфабетског шифрирања

Вежба 1: Користећи доњу табелу кореспонденције шифрирај поруку: « bonne chance pour casser ce code (*срећно у откривању шифре, п.п.*)»

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

Вежба 2: Користећи исту табелу кореспонденције дешифруј поруку « D JB EBUB »

Вежба 3а: Колико времена је потребно да неко тестира све могуће кључеве моно-алфабетског шифрирања, ако је познато да их има $4x10^{26}$ (4 и још 26 нула), и дешифрује поруку? Претпостављамо да је за тестирање једног кључа потребно 5 секунди (генерисање релане поруке и провера њеног смисла).

Вежба 3б: Ако би сви људи на планети радили заједно на решавању овог проблема, колико би им времена требало?

Вежба 3в: Колико би времена за исти задатак било потребно најмоћнијем суперкомпјутеру (Tianhe-2, кинеске армије), који може да тестира 10^{15} кључева у секунди?

Вежба 4: Одабери кључну-реч или кључну реченицу и попуни шифрирану азбуку у доњој табели. Пажња, немој исто слово да користиш више пута!
Користи ову нову табелу кориспонденције за шифрирање кратке поруке. Пошаљи ту поруку свом суседу (наравно, и кључ) и провери да ли је добро дешифровао твоју поруку.

Азбука	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
Шифрирана азбука																										