1.1 Šifriranje s substitucijo znakov

To je postopek šifriranja pri katerem znake v čistopisu zamenjamo z enim (preprosta zamenjalna šifra) ali več znaki v šifropisu (poligrafska zamenjalna šifra). Pri tem lahko tekom celotnega postopka uporabljamo isto abecedo (monoalfabetski postopek) ali pa se abeceda med postopkom spreminja (polialfabetski postopek).

1.1.1 Cezarjeva šifra

To je preprosta, monoalfabetska zamenjalna šifra. Postopek je krožni zamik abecede za določeno število znakov. Ključ je število znakov zamika.

Naloga:

1. V pythonu izdelajte funkcijo *fnCezar(cistopis,kljuc)*, ki bo niz ASCII znakov šifrirala in dešifrirala po Cezarjevem postopku s poljubnim zamikom abecede.

Navodila:

- Za abecedo najprej uporabite samo male črke ASCII tabele.
- Postopek razširite na velike črke in številke, pri čemer se vsak sklop šifrira znotraj svoje abecede:
    a. male črke se krožno zamikajo po abecedi malih črk (a do z),
    b. velike črke se krožno zamikajo po abecedi velikih črk (A do Z),
    c. števila se krožno zamikajo po abecedi števil (0 do 9).
- Funkciji fnCezar dodajte še argument razdeljeno*: fnCezar(cistopis,kljuc,razdeljeno)*. V kolikor je vrednost argumenta razdeljeno enaka 0, izvedite *nerazdeljeno* šifriranje z uporabo ASCII znakov med kodami 32 in 126 (vključno). Postopka ne delimo na posamezne abecede – celoten uporabljen nabor ASCII je ena abeceda.

Naloga:

2. S pomočjo funkcije *fnCezar* dešifrirajte naslednje šifropise (določite premik abecede):
    a. szwo
    b. Hzgxkcdhi
    c. l#,9b-zz|9g~1.)(9$~9(z*)0~}z&9%)(~|9-0~.z94z9&~.)9KIOIG

Rešitev:

1.1.2 Vigenerejeva šifra

v splošnem predstavlja polialfabetsko različico Cezarjeve šifre. Ključ je niz znakov, pri čemer vsak izmed znakov ključa določa zamik (ključ za Cezarjevo šifro) istoležnega elementa v čistopisu. Za šifriranje in dešifriranje zgolj velikih tiskanih črk angleške abecede se je pogosto uporabljal Viegenerjev kvadrat oz. Viegenerjeva tabela, poznana tudi pod imenom *tabula recta*.

Naloga:

3. Z uporabo Vigenerjevega kvadrata (Slika 1) dešifrirajte šifropis: »LXFOPVEFRNHR«, ki je bil pridobljen s ključem »LEMON«.

Rešitev:

Naloga:

4. V pythonu izdelajte funkcijo *fnVigenere(cistopis,kljuc,smer)*, ki bo čistopis velikih črk angleške abecede šifrirala oz. dešifrirala po Viegenerejevi šifri. Če je vrednost vhodnega argumenta *smer* enaka 0, naj se izvede dešifriranje, če je vrednost 1, naj se opravi šifriranje.
5. Z uporabo funkcije *fnVigenere*:
    a. Dešifrirajte šifropis: »OHV IWYXIEIR QAICEI VG S FZTYBR GY ZNTEMHMDNX NZHAVBVGWU MZXK OM MLDNX N GWKDEJ BT AGOEIJCNXI CRRGSK XIGUSJL« s ključem »VARNOST«

Rešitev:

	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

Slika 1: Tabula recta

1.1.3 Zamenjalna šifra z naključno abecedo

Pri tem šifrirnem postopku vsak znak čistopisa zamenjamo z znakom neke naključne abecede. Ta je lahko sestavljena iz naključno razporejenih znakov abecede čistopisa ali pa iz poljubnih drugih znakov (Dancing Men).

Naloga:

6. V pythonu izdelajte funkcijo *fnSubstitucija(cistopis,smer)*, ki bo niz znakov šifrirala po substitucijski metodi z uporabo naključne abecede.

Navodila:

- Vhodni argument *smer* naj predstavlja smer postopka: 1 = šifriranje, 0 = dešifriranje.
- Postopek najprej izvedite samo za velike črke, naključno abecedo določite sami.
- Postopek razširite na male črke z istim razporedom naključne abecede kot pri velikih črkah.
- Dodajte podporo za ločila: presledek, pika in vejica (šifriranje ločil ne spremeni).

1.2 Šifriranje z enkratnim ključem

Naloga:

7. Iz podanega šifropisa in ključa dešifrirajte čistopis. Nalogo lahko rešite »peš« ali z uporabo pythona.

Šifropis: [52,62,72,123,125,135,142,152,177,178,185,200,204,210,216,315,321,322,358, 373,376,377,378,405,432,464,468,470,489,641,650,667,701]

Ključ: 1. poglavje knjige VIKS (https://www.dropbox.com/s/rogvl0cu5vflzoh/VIKS.pdf?dl=0).