Криптографија

Задаци за рад по групама

Група I

Задатак ове групе је реализује неке основне криптографске алгоритме симетричне криптографије. Овдје су бројеви представљени као стрингови.

Задатак 1.

Написати програм **class_crypt** који преко одговарајућег корисничког интерфејса има следеће могућности:

- За задати кључ, врши енкрипцију односно декрипцију помоћу општег супституционог алгоритма.
- За задати кључ, врши енкрипцију односно декрипцију помоћу Виженеровог алгоритма.

Корисник, на почетку, бира језик између више понуђених и након тога дефинише кључ **K**, којим ће се вршити енкрипција текста. Кориснику се нуди опција да текст уноси директно или из неке датотеке на рачунару. Излаз је низ карактера који се приказују на екрану, а опционо уписују у неку текстуалну датотеку.

Задатак 2.

Направити програм **sub_anal** за криптнализу текста који је енкриптован основним супституционим алгоритмом. На основу анализе учесталости појединачних слова, диграма и триграма кориснику се даје предлог супституције неколико слова и даје му се на увид (на адектватан визуелан начин) како изгледају ефекти такве промјене. На примјер, након прве итерације имамо:

L	O	J	U	M		D	M	T	J	Z		W	M	J	G	G
t	-	e	-	-		-	-	-	e	-		-	-	e	-	-

Y	S	N	D	L		U	Y	L	E	O		S	K	D	V	C
-	-	-	-	t		-	-	t	-	-		-	-	-	-	-

У овом случају би било логично, да ако се ради о енглеском језику, да корисник закључи да слово **O** одговара слову **h** (јер је врло логично да реченица почиње чланом **the**). У неколико сличних итерација, у интеракцији са корисником, на крају се долази до комплетне табеле супституције.

Цјелокупан процес је могуће у потпуности аутоматизовати, без учешћа корисника. У том случају, потребно је интезивно користити статистике учесталости слова, диграма, триграма, као и индекс коинциденције. Такође, потребно је бити обазрив приликом дефинисања **излазног критеријума**.

sub_dec

Улаз: стринг
Излаз: пермутација алфабета, стринг

Напомена: Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику.
Задатке реализовати тако да постоји јединствени интерфејс, а корисник бира различите опције. За пројекат је потребно направити одговарајућу **документацију**. Документација подразумијева

1. Прецизна упуства потенцијалним корисницима како се користе поједини програми, шта они раде и која су им ограничења.

2. Описати поступак рада групе и назначити сваки појединачни допринос чланова групе.

3. Написати предлог побољшања постојећих програма.

4. Указати на могуће недостатке у прецизности формулације постављених задатака.

Документацију доставити у склопу пројекта у електронској форми.