Криптографија

Задаци за рад по групама

Супституциони крипто-систем

Задатак ове групе је реализује супституциони алгоритам (енкрипцију и декрипцију), као и криптоаналитички алат за супституциони алгоритам. Програм је потребно урадити у виду десктоп и веб апликације.

Задатак 1.

Направити програм који ће кориснику омогућити

- Врши енкрипцију и декрипцију помоћу општег супституционог алгоритма.

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 знатно побољшати тиме што би се вршиле анализе учесталости слова, диграма, триграма, као и индекс коинциденције.

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. **PYTHON код за сваки од задатака.**
2. Прецизна упуства потенцијалним корисницима како се користе поједини програми, шта они раде и која су им ограничења.
3. Описати поступак рада групе и назначити сваки појединачни допринос чланова групе.
4. Написати предлог побољшања постојећих програма.
5. Указати на могуће недостатке у прецизности формулације постављених задатака.

Документацију доставити у склопу пројекта у електронској форми.

Програм је неопходно доставити у самосталној извршној верзији (standalone executable - без инсталирања посебних окружења, библиотека...) или као веб апликацију.