Криптографија

Задаци за рад по групама

DES крипто-систем

Задатак ове групе је да направи програм за ДЕС енкрипцију и декрипцију.

Задатак 1.

Направити програм за енкрипцију и декрипцију путем DES криптосистема. Обратити пажњу на чињеницу да се овдје не затјева разбијање DES-а већ програм за декрипцију кад је задат кључ.

des_enc
Улаз: K (кључ), стринг; **Излаз:** стринг

des_dec
Улаз: K (кључ), стринг; **Излаз:** 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. **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.