Криптографија

Задаци за рад по групама

Група I

Задатак ове групе је реализује неке основне криптографске алгоритме симетричне криптографије, као и један технички алгоритам - тражење рјешења система конгруенција помоћу Кинеске теореме о остацима.

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.

Написати програм за рјешавање система конгруенција помоћу Кинеске теореме о остацима:

crt
Улаз: $(a_1, n_1), \ldots, (a_k, n_k)$ **Излаз:** $x \in \mathbb{Z}_N$ тако да $x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_k \pmod{n_k}$, $N = n_1 n_2 \cdots n_k$

Напомена: Програм треба да аутоматски провјерава да ли су испуњени услови $(\mathbf{n_i}, \mathbf{n_j}) = \mathbf{1}$ за $i \neq j$.

Напомена: 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.