Криптографија (Ц)

Задаци за рад по групама

Група VI

Задатак ове групе је да користећи неку постојећу библиотеку корисних програма, везаних за аритметику великих бројева, односно бројева који су представљени као низови цифара реализује групу неких познатих криптографских алгоритама. Овдје су бројеви представљени као стрингови. **Узимаћемо да је генерално ограничење за сваки стринг да је његова дужина највише 40.**

Задатак 1.

Написати програм за реализацију Pohlig-Hellman алгоритма. Уз овај програм потребно је посебно издвојити програм за рјешавање система конгуруенција помоћу кинеске теореме о остацима. Улазни подаци у програму су стрингови који представљају бројеве. Потребно је испититати да ли су улазни подаци одговарајући, као на примјер да ли је p прост број.

polig – hellman
Улаз: p, g, h **Излаз:** $x \in \mathbb{Z}_p$ тако да $g^x \equiv h \pmod{p}$.

Програм за рјешавање система конгруенција помоћу Кинеске теореме о остацима треба да буде у облику:

crt

Улаз: $(a_1, n_1), \ldots, (a_k, n_k)$
$(\mathbf{n_i}, \mathbf{n_j}) = \mathbf{1}$ за $i \neq j$
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: Улазни подаци и у прораму **crt** су стрингови који представљају бројеве.

Задатак 2.

Написати програм за реализацију Pollard Rho алгоритма за тражење ДЛОГ-а. Као и у претходном програму, потребно је испититати да ли су улазни подаци одговарајући, као на примјер да ли је p прост број.

poll_rho

Улаз: p, g, h
Излаз: $x \in \mathbb{Z}_p$ тако да
$g^x \equiv h \pmod{p}$.

Напомена: Сви програми се обједињују у оквиру јединственог корисничког интерфејса. Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику. 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.