Криптографија (Д)

Други колоквијум, 27.5.2016.

Максималан број бодова на испиту је 100. Укупно вријеме рада је **90** минута. **Нечитко исписани одговори и некомплетна рјешења се неће бодовати**. Срећно!

Задатак 1. (20 поена)

Алиса и Боб су успоставили параметре $p = 17$, $g = 3$ за Дифи-Хелман протокол којим желе да размијене заједнички кључ. Ако су на крају протокола добили 4 као заједнички кључ, а Алисин тајни експонент је $a = 3$, који је Бобов тајни експонент? Образложити и описати ток протокола.

Задатак 2. (30 поена)

Алиса је на свом веб-сајту објавила јавне параметре ЕлГамала $p = 17$, $g = 5$ и $g^a = 2$. Тајни податак који Алиса чува је $a = 6$.

а. Боб хоће да енкриптује $m = 4$, бирајући $k = 3$. Шта ће Боб послати Алиси?

б. Претпоставимо да је Боб за неку поруку s послао енкрипцију у виду уређеног пара $(13, 9)$. Ева је успјела да дође до поруке s. Објаснити како.

Упуство за б: Потребно је одредити k из првог елемента уређеног пара.

Задатак 3. (30 поена)

Алиса је на свом веб-сајту објавила јавне параметре $N = 77$ и $e = 11$. Боб треба да пошаље поруку $m = 4$ користећи РСА енкрипцију. Објаснити шта Боб ради, извршити рачунања, а потом објаснити како ће Алиса извршити декрипцију. Приказати сваки рачунски корак.

Питања (20 поена)

- Шта је то Дифи-Хелманов проблем?
- Шта је то проблем дискретног логаритма?
- Ако би посједовали алгоритам за ефикасну факторизацију природних бројева, онда РСА не би био сигуран крипто-систем. Објасни.
- Описати бар један метод за факторизацију природних бројева.