Exercise
Algorithmic Cryptography
Sheet 4

Exercise 4.1 (4 points)
Construct a protocol without any key-exchange (according to slide (2:3) of the lecture) based on
(a) factorization (RSA).
(b) discrete logarithm (ElGamal).

Exercise 4.2 (4 points)
Let \( p \) be a prime number, \( g \) be a generator of the cyclic group \( \mathbb{Z}_p^* \), \( x \in \{2, \ldots, p-2\} \), and \( y = g^x \mod p \).
Prove: The least significant bit of \( x \) can be computed efficiently using only \( y, g, \) and \( p \).

Exercise 4.3 (4 points)
Let an ElGamal system be given by the private key \((p, g, x)\) and the public key \((p, g, y = g^x \mod p)\). Furthermore, let \( k \in \{2, \ldots, p-2\} \) with \( \gcd(k, p-1) = 1 \). The message \( m \) was encrypted to \((a, b) = (g^k \mod p, m \cdot y^k \mod p)\).
Prove: It can be determined efficiently, whether \( m \) is a quadratic residue or not, using only \( y, g, p, a, \) and \( b \).

Exercise 4.4 (4 points)
Let \( p \) be a prime number and \( g \) be a generator of the cyclic group \( \mathbb{Z}_p^* \). Consider the following two problems:

ELGAMAL PROBLEM
Input: \( p, g, y, a, b \) with \( y = g^a \mod p \) and \((a, b) = (g^k \mod p, \bar{m} \cdot y^k \mod p)\).
Problem: Compute \( \bar{m} \).

DIFFIE-HELLMAN PROBLEM
Input: \( p, g, c, d \) with \( c = g^c \mod p \) and \( d = g^d \mod p \).
Problem: Compute \( g^{cd} \).

Prove:
(a) If the DIFFIE-HELLMAN PROBLEM can be solved efficiently, then also the ELGAMAL PROBLEM.
(b) If the ELGAMAL PROBLEM can be solved efficiently, then also the DIFFIE-HELLMAN PROBLEM.

Deadline: Thursday, November 21, 2013, 10:15 a.m.,
in the lecture or in the letterbox in front of i1.
Please fill in your name and your student number and mark the exercises that you can present. Then staple this page in front of your solution sheet.

<table>
<thead>
<tr>
<th>Name</th>
<th>Student Number</th>
<th>E 4.1</th>
<th>E 4.2</th>
<th>E 4.3</th>
<th>E 4.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>