

# Cryptography

## Problem set 8 - 14-15 V 2015

**Definition [Fiat-Shamir (simplified) indentication protocol]** Peggy proves to Victor that she knows a square root  $s$  of  $v$  mod  $n$ :

1. (Commitment) Peggy chooses a random number  $r \in \{1, \dots, n-1\}$  and computes  $x = r^2 \bmod n$ . She sends the result  $x$  to the verifier Victor.
2. (Challenge) Victor chooses a random number  $e \in \{0, 1\}$  and sends it to Peggy.
3. (Response) Peggy sends  $y = rs^e \bmod n$  to Victor.
4. (Verification) Victor accepts if and only if  $y^2 = xv^e \bmod n$ .

- 
1. Prove that if  $p$  is a prime then the number of generators of  $\mathbb{Z}_p^*$  is equal to  $\phi(p-1)$ .
  2. Prove the following lemma. Let  $p$  be a prime. Then  $x \in \mathbb{Z}_p^*$  is a primitive root if and only if  $x^{(p-1)/q} \not\equiv 1 \pmod p$  for every prime  $q$  which divides  $p-1$ .

How can one use this property to generate keys of *e.g.*, ElGamal cryptosystem?

3. Prove Euler's criterion: Let  $p$  be a prime  $> 2$ , and let  $x \in \mathbb{Z}$ . Then

$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod p.$$

4. (2 points) Use Euler's criterion for proving correctness and expected running time of the algorithm for computing square roots modulo prime (the one you implemented for the problem Lab6.1).
5. For the Fiat-Shamir (simplified) scheme, let  $n = 143$ ,  $v = 82$ ,  $x = 53$  and  $e = 1$ . Determine a valid response that proves the knowledge of a square root of  $v$  mod  $n$ . What is the response when  $e = 0$ ?
6. Let  $n = pq$ , where  $p$  and  $q$  are distinct primes and  $x_1, x_2 \in \mathbb{Z}_n^*$ . Assume that at least one of  $x_1$  and  $x_2$  is in  $\mathbb{QR}_n$ . Peggy wants to prove to Vic that she knows a square root of  $x_i$  for at least one  $i \in \{1, 2\}$  without revealing  $i$ . Modify *Fiat-Shamir simplified identification* protocol (the one presented during the lecture) to get an interactive zero-knowledge proof of knowledge.
7. Let  $p$  be a prime number,  $g$  a primitive root mod  $p$ ,  $a \in \{0, 1, \dots, p-2\}$ , and  $A = g^a \bmod p$ . Describe a zero-knowledge proof for the knowledge of the discrete logarithm  $a$  of  $A$  mod  $p$  to the base  $g$ . Prove its: completeness, soundness and zero-knowledge properties.