

IV054 Coding, Cryptography and Cryptographic Protocols  
2010 - Exercises X.

1. We say that an algorithm  $A$   $\epsilon$ -distinguishes random variables  $X$  and  $Y$  if

$$|Pr[A(X) = 1] - Pr[A(Y) = 1]| \geq \epsilon.$$

Let  $U$  be the uniform distribution on the set  $\{0, 1\}$  and let  $X$  be the distribution generated by a biased coin which gives 1 with probability  $\frac{2}{3}$  and 0 with probability  $\frac{1}{3}$ . Determine the largest  $\epsilon$  for which there is a probabilistic polynomial algorithm which  $\epsilon$ -distinguishes  $U$  and  $X$ . Propose such an algorithm and show that it has the desired property.

2. Show how to utilize 1-out-of-2 oblivious transfer to implement a bit commitment protocol in which both parties can cheat with probability  $\leq 2^{-64}$ . Explain.
3. Let  $n = pq$  where  $p \equiv 3 \pmod{4}$ ,  $q \equiv 3 \pmod{4}$  be large primes. Peggy needs to prove to Victor that she knows the factors of  $n$  without revealing any information about them. She has developed the following protocol:

- Peggy and Victor perform the following actions 20 times.
  - (i) Victor randomly chooses an integer  $x < n$ , computes  $y = x^2 \pmod{n}$  and sends  $y$  to Peggy.
  - (ii) Peggy computes the four square roots of  $y \pmod{n}$ , randomly chooses one of them (let us denote it  $r$ ) and sends  $r$  to Victor.
  - (iii) Victor verifies whether  $r^2 \equiv y \pmod{n}$ .
- Victor accepts if and only if all the verifications have been successful.

Decide whether the protocol is a zero-knowledge proof. Justify your answer.

4. (*Bonus*)

Deus Auctor magnus.  
Rector Deus incompraehensibilis  
sapientissimus Deus.