T-79.5502 Advanced Course in Cryptology
Exam
May 11, 2006

1. (6 pts) Differentiate and relate the following concepts:
   (a) Turing computable problem,
   (b) intractable problem,
   (c) deterministic polynomial time algorithm,
   (d) efficient algorithm,
   (e) practically efficient algorithm, and
   (f) negligible quantity.

2. (6 pts) Let us denote by $PO_{N,e}$ the RSA parity oracle, which for given input $m^e($ mod $N)$ returns m mod 2. Give an outline of a decryption algorithm for RSA, which with input $m^e(\text{mod} N)$ makes $\lceil \log_2 N \rceil$ calls to $PO_{N,e}$ and then returns m.

3. (a) (3 pts) State the Decisional Diffie-Hellman (DDH) Assumption.
   (b) (3 pts) Describe an efficient reduction from an IND-CPA attacker on ElGamal encryption to an attacker on DDH.

4. (6 pts) Assume that there are two disjoint worlds $\textsc{Exp}_0$ and $\textsc{Exp}_1$. Bob's task is to distinguish between the two worlds. Bob is given a sample σ, which is drawn from $\textsc{Exp}_0$ with probability 1/2 and from $\textsc{Exp}_1$ with probability 1/2. Bob has a friend Alice, who with input σ guesses a bit $B(\sigma)$. Alice returns $B(\sigma) = 0$ with probability p in case σ is drawn from $\textsc{Exp}_0$. In case σ is drawn from $\textsc{Exp}_1$ Alice is completely helpless, that is, cannot do any better than randomly guess the value of the bit $B(\sigma)$.

   Bob's algorithm is as follows. Let $\sigma \in \textsc{Exp}_b$ be given to Bob. Bob forwards σ to Alice, who then returns $B(\sigma)$. Bob guesses $b = B(\sigma)$.

   Determine the probability that Bob's guess is correct. Show that this probability is different from 1/2 if and only if $p \neq 1/2$.