End Semester Examination, Autumn 2003-04

Total points: 100 November 22, 2003 Total time: $3 + \epsilon$ hours

---

1. In a cryptographic sense we call an algorithm infeasible, if it takes a time of 2^{80} or more floating point operations. Assume that some algorithm A takes a time of $f(t)$ floating point operations for an input of bit-size t. For each of the following cases find the least positive integer t for which A is infeasible. (Show your calculations.) **(3×5)**

(a) $f(t) = t^6$.

(b) $f(t) = 2^{t/2}$.

(c) $f(t) = \exp(2\sqrt{t \ln t})$.

(d) $f(t) = \exp(\sqrt{t \ln t})$.

(e) $f(t) = \exp(1.923\, t^{1/3} (\ln t)^{2/3})$.

2. In this exercise one studies the arithmetic in the finite field $\mathbb{F}_{125} = \mathbb{F}_{5^3}$.

(a) Show that $f(X) := X^3 + 2X + 4 \in \mathbb{F}_5[X]$ is irreducible. **(5)**

(b) Let us represent $\mathbb{F}_{125}$ as $\mathbb{F}_5[X]/\langle f(X) \rangle$. Call $\alpha := X + \langle f(X) \rangle \in \mathbb{F}_{125}$ and consider the elements $a := 3\alpha^2 + 2\alpha + 1$ and $b := 2\alpha^2 + 3$ in $\mathbb{F}_{125}$. Compute ab^{-1} in this representation of $\mathbb{F}_{125}$. You should compute the canonical representative of ab^{-1} in $\mathbb{F}_{125}$, i.e., a polynomial in α of degree < 3. **(10)**

3. Let p be a prime and g a generator of $\mathbb{F}_p^*$. Suppose that Alice's private and public keys are respectively d and g^d. Recall that an ElGamal signature (s, t) of Alice on a message M is computed for a random d' as:

$$\begin{aligned} s &:= g^{d'} \pmod{p}, \\ t &:= (d')^{-1}[H(M) - dH(s)] \pmod{p-1}. \end{aligned}$$

(a) Consider a variant of the ElGamal scheme, in which s is computed as above, but the rôles of d and d' are interchanged in the second equation, i.e., the modified signature $(s, \bar{t}\,)$ on M is generated as:

$$\begin{aligned} s &:= g^{d'} \pmod{p}, \\ \bar{t} &:= d^{-1}[H(M) - d'H(s)] \pmod{p-1}. \end{aligned}$$

Write the verification routine for the modified scheme. **(5)**

(b) Show that forging modified ElGamal signatures is as difficult as computing discrete logarithms in $\mathbb{F}_p^*$. You may assume that a forger can arrange d' of her choice. **(5)**

(c) Explain why signature generation is (a bit) more efficient in the modified scheme. Suppose that because of this enhanced performance Alice decided to switch to the modified scheme, but for backward compatibility she maintained both the original signature (s, t) and the modified signature $(s, \bar{t}\,)$ on a message M. What went wrong? **(2+3)**

4. Let $n := pq$ with distinct primes p and q each congruent to 3 modulo 4.

(a) Show that -1 is a quadratic non-residue modulo p and modulo q. **(5)**

(b) If $a \in \mathbb{Z}_n^*$ is a quadratic residue modulo n, prove that a has exactly four square roots modulo n, of which exactly one is a quadratic residue modulo n. **(5)**

(c) Consider the following identification protocol in which Alice wants to prove to Bob her knowledge of the factorization of $n = pq$.

- Bob sends a to Alice.
- Alice computes four square roots of a modulo n and picks up the unique square root b which is a quadratic residue modulo n.
- Alice sends b to Bob.
- Bob accepts Alice's claim, if and only if $b \equiv x^2 \pmod{n}$.

Assume that p and q are sufficiently large so that computing square roots modulo n is infeasible without the knowledge of the factorization of n. Argue that Alice can prove her identity to Bob, if and only if she knows the factorization of n. **(5)**

(d) Conclude that this is not a good zero-knowledge protocol, by demonstrating that Bob can maliciously send a bad a to Alice so that during the execution of the protocol he gathers enough information to factor n. **(5)**

5. Let G be a finite multiplicative Abelian group with identity e. Recall that for $a \in G$ the order $\operatorname{ord}_G(a)$ is defined to be the smallest of the *positive* integers h such that $a^h = e$. Let $m := \operatorname{ord}_G(a)$ for some $a \in G$ and let $k \in \mathbb{N}$. Prove the following assertions:

(a) $a^h = e$, if and only if $m \mid h$. **(5)**

(b) $\operatorname{ord}_G(a^k) = m / \gcd(m, k)$. **(5)**

6. Let $n := pq$ with two distinct odd primes p and q, $\gcd(e, \phi(n)) = 1$ and $ed \equiv 1 \pmod{\phi(n)}$, i.e., (n, e) is an RSA public-key and d the corresponding private key. In this exercise one derives that factoring n is (probabilistic) polynomial-time equivalent to the problem of computing d from (n, e) (without the knowledge of p or q or $\phi(n)$). If the factorization of n is provided, one can compute d from (n, e) as in the RSA key generation procedure. In the following parts you are asked to prove the converse. Write $ed - 1 = 2^s t$ with t odd. Since $ed - 1$ is a multiple of $\phi(n) = (p-1)(q-1)$, we have $s \geqslant 2$.

(a) Show that for any $a \in \mathbb{Z}_n^*$ one has $\operatorname{ord}_n(a^t) \mid 2^s$, where $\operatorname{ord}_n(x)$ denotes the (multiplicative) order of $x \in \mathbb{Z}_n^*$. **(5)**

(b) We know that the group $\mathbb{Z}_p^*$ is cyclic. Let g be a generator of $\mathbb{Z}_p^*$. Take $a := g^k \pmod{p}$ for some $k \in \{0, 1, \ldots, p-2\}$ and let $\operatorname{ord}_p(a^t) = 2^\sigma$. Show that $\sigma = \mathrm{v}_2(p-1)$ if k is odd, and $\sigma < \mathrm{v}_2(p-1)$ if k is even. Here $\mathrm{v}_2(p-1)$ stands for the multiplicity of 2 in $p-1$, i.e., the largest exponent e such that $2^e \mid (p-1)$. An analogous result holds for the other prime q. **(5)**

(c) If $\operatorname{ord}_p(a^t) \neq \operatorname{ord}_q(a^t)$ for some $a \in \mathbb{Z}_n^*$, prove that there exists $\sigma \in \{0, 1, 2, \ldots, s-1\}$ such that $\gcd(a^{2^\sigma t} - 1, n)$ is a non-trivial factor (p or q) of n. **(5)**

(d) Demonstrate that there are at least $\phi(n)/2$ elements a in $\mathbb{Z}_n^*$ with the property that a^t has different orders modulo p and q. **(5)**

(e) Design a probabilistic polynomial-time algorithm for factoring n from the knowledge of n, e and d. **(5)**