End Semester Examination, Autumn 2003-04

Solutions

---

1. **(a)** 10322, **(b)** 160, **(c)** 153, **(d)** 496, **(e)** 590.

2. **(a)** $f(X)$, if reducible in $\mathbb{F}_5[X]$, admits a linear factor in $\mathbb{F}_5[X]$, i.e., a root in $\mathbb{F}_5$. But $f(0) \equiv 4 \pmod 5$, $f(1) \equiv 7 \equiv 2 \pmod 5$, $f(2) \equiv 16 \equiv 1 \pmod 5$, $f(3) \equiv 37 \equiv 2 \pmod 5$ and $f(4) \equiv 76 \equiv 1 \pmod 5$.

(b) In order to compute b^{-1}, I should compute the extended gcd of $f(X)$ with $b(X) = 2X^2 + 3$ in $\mathbb{F}_5[X]$. The following table lists the relevant computations:

i	$r_i = r_{i-2}$ rem r_{i-1}	$q_i = r_{i-2}$ quot r_{i-1}	$v_i = v_{i-2} - q_i v_{i-1}$
0	$X^3 + 2X + 4$	$-$	0
1	$2X^2 + 3$	$-$	1
2	$3X + 4$	$3X$	$2X$
3	1	$4X + 3$	$2X^2 + 4X + 1$

Therefore, $b^{-1} = 2\alpha^2 + 4\alpha + 1$ and so $ab^{-1} = (3\alpha^2 + 2\alpha + 1)(2\alpha^2 + 4\alpha + 1) = \alpha^4 + \alpha^3 + 3\alpha^2 + \alpha + 1 = (\alpha^4 + 2\alpha^2 + 4\alpha) + (\alpha^3 + 2\alpha + 4) + (\alpha^2 + 2) = \alpha^2 + 2$.

3. **(a)** The signing equation for the modified ElGamal scheme is $H(M) \equiv d\bar{t} + d'H(s) \pmod{p-1}$. Exponentiation gives the congruence $g^{H(M)} \equiv \left(g^d\right)^{\bar{t}} s^{H(s)} \pmod p$ to be checked for verification.

(b) If d is known, one can generate the signature $(s, \bar{t}\,)$ on M in polynomial time. Conversely, suppose that an intruder chooses d' of her choice and somehow obtains the valid signature $(s, \bar{t}\,)$ on M. If $\bar{t}$ is invertible modulo $p - 1$, she can compute $d \equiv (\,\bar{t}\,)^{-1}[H(M) - d'H(s)] \pmod{p-1}$ in polynomial time.

(c) Precomputation of $d^{-1} \pmod{p-1}$ saves the time for computing a modular inverse during each signing operation. However, if $s, t, \bar{t}$ are known, one has:

$$\begin{aligned} H(M) &\equiv dH(s) + d't \pmod{p-1}, \\ H(M) &\equiv d\bar{t} + d'H(s) \pmod{p-1}. \end{aligned}$$

This is a system of two linear congruences, and if $H(s)^2 - t\bar{t}$ is invertible modulo $p - 1$, one can solve this system to obtain the unknown values d and d'.

4. **(a)** By Euler's criterion $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$, since $(p-1)/2 \equiv 1 \pmod 2$. Similarly for q.

(b) a has exactly two square roots modulo p, say $\pm u \pmod p$, and exactly two square roots $\pm v$ modulo q. Combining using CRT gives exactly four square roots (b_1, b_2, b_3, b_4) of a modulo n.

By Part (a) exactly one of u and $-u$ is a quadratic residue modulo p, and exactly one of v and $-v$ is a quadratic residue modulo q. Finally, note that b is a quadratic residue modulo n, if and only if b is a quadratic residue modulo both p and q.

(c) If Alice knows p and q, she can compute (in poly-time) the four square roots b_1, b_2, b_3, b_4 of a modulo n. Since b is a quadratic residue (x^2) modulo n, it is the unique square root of a which is a quadratic residue modulo n. Thus Alice succeeds in proving her identity.

On the other hand, suppose that an intruder can produce b for any given biquadratic residue (fourth power) a. By Parts (a) and (b) quadratic residues modulo n are biquadratic residues too; so the intruder can compute square roots of a modulo n for any $a \in \mathbb{Z}_n^*$. By our assumption this is infeasible.

(d) Bob randomly locates $b' \in \mathbb{Z}_n^*$ with $\left(\frac{b'}{n}\right) = -1$. This means that either $\left(\frac{b'}{p}\right) = -1$ or $\left(\frac{b'}{q}\right) = -1$, but not both. Bob sends $a := (b')^2 \pmod n$. Since quadratic residues modulo n are also biquadratic residues, $a \equiv x^4 \pmod n$ for some $x \in \mathbb{Z}_n^*$. Alice returns $b \equiv x^2 \pmod n$. But then $\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right) = 1$, i.e., b is congruent to b' modulo exactly one of p and q and not congruent to b' modulo the other prime. Thus $\gcd(b - b', n)$ is a non-trivial factor of n.

$h = mq + r$ for $0 < r < m$. Then $a^h = (a^m)^q a^r = a^r \neq e$ by the definition of m.

(b) Let $l := \mathrm{ord}_G(a^k)$. Since $k/\gcd(m,k)$ is an integer, we have $(a^k)^{m/\gcd(m,k)} = (a^m)^{k/\gcd(m,k)} = e$, and so by Part (a) $l \mid m/\gcd(m,k)$. Conversely, $a^{kl} = (a^k)^l = e$, i.e., $m \mid kl$, i.e., $m/\gcd(m,k)$ divides $(k/\gcd(m,k))l$. Since $\gcd(m/\gcd(m,k), k/\gcd(m,k)) = 1$, we have $m/\gcd(m,k) \mid l$.

6. (a) $\mathrm{ord}_n(a)$ divides $\phi(n)$ and hence $ed - 1 = 2^s t$ too, i.e., $\mathrm{ord}_n(a) = 2^{s'}t'$ for $0 \leqslant s' \leqslant s$ and $t' \mid t$. By Exercise 5(a) $\mathrm{ord}_n(a^t) = 2^{s'}t'/\gcd(2^{s'}t', t) = 2^{s'}t'/t' = 2^{s'}$.

(b) Let $v := \mathrm{v}_2(p-1)$, i.e., $p - 1 = 2^v r$ for some odd r. By definition $\mathrm{ord}_p(g) = 2^v r$, and so $\mathrm{ord}_p(g^k) = 2^v r/\delta$, where $\delta := \gcd(2^v r, k)$. If k is odd, δ is odd and divides r, i.e., $\mathrm{ord}_p(g^k) = 2^v(r/\delta)$. On the other hand, if k is even, δ is even too, and we can write $\delta = 2^{v'}r'$ for some $v' > 0$ and for some odd r' dividing r, so that $\mathrm{ord}_p(g^k) = 2^{v-v'}(r/r')$. It then follows that $\mathrm{ord}_p(a^t) = \begin{cases} 2^v & \text{if } k \text{ is odd,} \\ 2^{v-v'} & \text{if } k \text{ is even.} \end{cases}$

(c) Let $\mathrm{ord}_p(a^t) = 2^\sigma$ and $\mathrm{ord}_q(a^t) = 2^\tau$ with $\sigma \neq \tau$. We only consider $\sigma < \tau$ — the other case can be handled similarly. Consider the element $b := a^{2^\sigma t} = (a^t)^{2^\sigma} \pmod n$. By the choices of σ and τ we have $b \equiv 1 \pmod p$ and $b \not\equiv 1 \pmod q$, i.e., $p \mid (b-1)$ and $q \nmid (b-1)$, so that $\gcd(b-1, n) = p$.

(d) Let $v := \mathrm{v}_2(p-1)$ and $w := \mathrm{v}_2(q-1)$. Let g be a primitive element modulo p and h a primitive element modulo q. Consider the sets

$$\begin{aligned} S_0 &:= \{g^k \pmod p \mid k = 0, 2, 4, \ldots, p-3\}, \\ S_1 &:= \{g^k \pmod p \mid k = 1, 3, 5, \ldots, p-2\}, \\ T_0 &:= \{h^k \pmod q \mid k = 0, 2, 4, \ldots, q-3\}, \\ T_1 &:= \{h^k \pmod q \mid k = 1, 3, 5, \ldots, q-2\}. \end{aligned}$$

We have $\#S_0 = \#S_1 = (p-1)/2$ and $\#T_0 = \#T_1 = (q-1)/2$. Also recall that $\phi(n) = (p-1)(q-1)$.

Case 1: $v = w$

Take $x \in S_0$ and $y \in T_1$. By the CRT we have a (unique) $a \in \mathbb{Z}_n^*$ with $a \equiv x \pmod p$ and $a \equiv y \pmod q$. By Part (b) we have $\mathrm{v}_2(\mathrm{ord}_p(a^t)) < \mathrm{v}_2(\mathrm{ord}_q(a^t))$, i.e., in particular, $\mathrm{ord}_p(a^t) \neq \mathrm{ord}_q(a^t)$. This accounts for $[(p-1)/2][(q-1)/2] = \phi(n)/4$ elements $a \in \mathbb{Z}_n^*$ with $\mathrm{ord}_p(a^t) \neq \mathrm{ord}_q(a^t)$. Choosing $x \in S_1$ and $y \in T_0$ similarly gives us a (disjoint) set of $\phi(n)/2$ such elements.

Case 2: $v < w$

Take $x \in S_0 \cup S_1$ and $y \in T_1$ and follow an argument as in Case 1.

Case 3: $v > w$

Take $x \in S_1$ and $y \in T_0 \cup T_1$.

(e) One repeats the following procedure for random $a \in \{1, 2, \ldots, n-1\}$, until one succeeds to factor n. If $\gcd(a, n) > 1$, this gcd is a non-trivial factor of n. So assume $a \in \mathbb{Z}_n^*$. Compute $\gcd(a^{2^\sigma t} - 1, n)$ for $\sigma = 0, 1, \ldots, s-1$. With probability $1/2$ we have $\mathrm{ord}_p(a^t) \neq \mathrm{ord}_q(a^t)$, and if so, some σ will give us a non-trivial factor of n by Part (c).