C&O 685
The Mathematics of Public-Key Cryptography

Final Exam (take-home)

December 5, 2000

Instructions

- You are not permitted to discuss *any* of the exam questions with anyone else.
- Answer all five questions.
- Show all your computations, including output of any Maple sessions.
- Hand in the exam, by noon on Dec. 6, to Frances Hannigan in MC 5027.
- You can contact me by email if you have any questions about the exam, e.g., if you need some clarification about what a particular question on the exam is asking for.
- If I need to correct a mistake, I will post any changes on the course web page.
- If you get completely stuck on a question, I will provide a hint, the cost of which is a loss of at most 25% of the available marks on that question.

Questions

1. Suppose that Bob is using the ElGamal signature scheme to sign messages. The parameters of the scheme are $p = 28703$, $\alpha = 5$ and $\beta = 11339$. In order to save time in generating the random numbers k used to sign messages, Bob chooses an initial random value k_0, and then signs the ith message using the value $k_i = k_0 + 2i \bmod (p-1)$. Suppose that Alice observes two consecutive messages signed by Bob:
$$\begin{array}{ll} x_i = 12000 & sig(x_i) = (26530, 19862) \\ x_{i+1} = 24567 & sig(x_{i+1}) = (3081, 7604). \end{array}$$
   (a) Describe how Alice can easily compute Bob's secret key, a, given this information. (The main step of the attack consists of solving a system of two congruences in two unknowns. Note that the value of i does not have to be known for the attack to succeed.)
   (b) Use the attack you describe to find the value of a.

2. Consider an elliptic curve E described by the formula $y^2 \equiv x^3 + ax + b \pmod p$, where $4a^3 + 27b^2 \not\equiv 0 \pmod p$ and $p > 3$ is prime.
   (a) It is clear that a point $P = (x_1, y_1) \in E$ has order 3 if and only if $2P = -P$. Use this fact to prove that, if $P = (x_1, y_1) \in E$ has order 3, then
$$3{x_1}^4 + 6a{x_1}^2 + 12x_1 b - a^2 \equiv 0 \pmod p. \tag{1}$$
   (b) Conclude from equation (1) that there are at most 8 points of order 3 on the elliptic curve E.
   (c) Using equation (1), determine all points of order 3 on the elliptic curve $y^2 \equiv x^3 + 34x \pmod{73}$.

3. In this question we consider a modification of the Rabin Cryptosystem in which the encryption operation has the form $x \mapsto x^d \bmod n$.

   (a) Suppose that p is prime and $d > 1$ is an integer such that $p - 1 \equiv 0 \pmod{d}$. Prove that any $y \in \mathbb{Z}_p{}^*$ has either 0 or d dth roots in $\mathbb{Z}_p{}^*$.

   (b) Suppose that n is the product of two distinct odd primes p and q, and let $d = \gcd(p-1, q-1)$. Suppose that $y = x_0{}^d \bmod n$ for some $x_0 \in \mathbb{Z}_n{}^*$. Prove that there are exactly d^2 elements $x \in \mathbb{Z}_n{}^*$ such that $y = x^d \bmod n$.

   (c) (This part of the question establishes that a decryption algorithm can be used to factor n, in the situation where $d = 4$.) Suppose that n is the product of two distinct odd primes p and q, where $\gcd(p-1, q-1) = 4$. Suppose that $y = x_0{}^4 \bmod n$ for some $x_0 \in \mathbb{Z}_n{}^*$, and suppose that x_1 is chosen randomly from the set $\{x \in \mathbb{Z}_n{}^* : y = x^4 \bmod n\}$. Then $x_0{}^4 - x_1{}^4 \equiv 0 \pmod{n}$. Observe that $x_0{}^4 - x_1{}^4$ can be factored as $(x_0{}^2 + x_1{}^2)(x_0 - x_1)(x_0 + x_1)$. Suppose that we compute $\gcd(x_0 - x_1, n)$, $\gcd(x_0 + x_1, n)$, and $\gcd(x_0{}^2 + x_1{}^2, n)$ in an attempt to factor n. Prove that n will successfully be factored by this technique with probability at least 5/8.

4. (a) Determine the NAF signed digit representation of the integer 87.

   (b) Let P be a point on an elliptic curve E over a finite field $\mathbb{Z}_p$, where $p > 3$ is prime, and let m be a positive integer. Give a pseudocode description of a "double and (add-or-subtract)" algorithm which computes the point mP on the curve E given an arbitrary signed digit representation of m.

   (c) Using the NAF representation of 87, use the algorithm described above to compute $87P$, where $P = (2, 6)$ is a point on the elliptic curve $y^2 \equiv x^3 + x + 26 \bmod 127$ defined over $\mathbb{Z}_{127}$. Show the partial results during each iteration of the algorithm.

5. Suppose that E is an elliptic curve defined over $\mathbb{Z}_p$, where $p > 3$ is prime. Suppose that $\#E$ is prime, $P \in E$, and $P \neq \mathcal{O}$.

   (a) Prove that the discrete logarithm $\log_P(-P) = \#E - 1$.

   (b) Describe how to compute $\#E$ in time $O(p^{1/4})$ by using Hasse's bound on $\#E$, together with a modification of Shanks' discrete logarithm algorithm. Give a pseudocode description of the algorithm.