MATH/CMSC 456 (Washington) Exam 2 May 2, 2006

Use 6 pages for your answers. Do Problem 1 on page 1, Problem 2 on page 2, etc.

1. (20 points = 10+10) (a) Let $H(x) = x \pmod{123456}$. Give two properties of a cryptographic hash function that $H(x)$ does not satisfy. Explicitly show that these properties fail.
(b) Let $P = (1, 3)$ and $Q = (-2, 0)$ be points on the elliptic curve $y^2 \equiv x^3 + 8 \pmod{11}$. Evaluate $P + Q$.

2. (15 points) Peggy claims that she knows an RSA plaintext. That is, n, e, c are public and Peggy claims that she knows m such that $m^e \equiv c \pmod{n}$. She wants to prove this to Victor using a zero knowledge protocol. Peggy and Victor perform the following steps:

1. Peggy chooses a random integer r_1 and computes $r_2 \equiv m \cdot r_1^{-1} \pmod{n}$ (assume that $\gcd(r_1, n) = 1$).
2. Peggy computes $x_1 \equiv r_1^e \pmod{n}$ and $x_2 \equiv r_2^e \pmod{n}$ and sends x_1, x_2 to Victor.
3. Victor checks that $x_1 x_2 \equiv c \pmod{n}$.

Give the remaining steps of the protocol. Victor should be at least 99% convinced that Peggy is not lying.

3. (15 points) Suppose the output of a hash function H is a string of 60 bits. Explain why H cannot be strongly collision resistant and give the details of how you find the collision. You may assume that your computer can store up to 2^{40} bits and do up to 2^{40} computations (that is, not enough to compute or store 2^{60} values of the hash function).

4. (14 points) Nelson produces budget encryption machines for people who cannot afford a full-scale version of DES. The encryption consists of one round of a Feistel system. The plaintext has 64 bits and is divided into a left half L and a right half R. The encryption uses a function $f(R)$ that takes an input of 32 bits and outputs a string of 32 bits. (There is no key: anyone dumb enough to buy this machine should not be trusted to choose a key.) The left half of the ciphertext is $C_0 = R$. The right half of the ciphertext is $C_1 = L \oplus f(R)$. Suppose Alice uses one of these machines to encrypt and send a message to Bob. Bob has an identical machine. How does he use the machine to decrypt the ciphertext he receives? Show that this decryption method works (do not quote results about Feistel systems; you are essentially justifying that a special case works).

5. (18 points = 8+10) Recall the Baby Step – Giant Step method for classical discrete logs: There is a large prime p and we want to solve $\beta \equiv \alpha^x \pmod{p}$ for x. We know that $0 \leq x < N^2$ for some N. We make two lists:

1. $\alpha^j \pmod{p}$ for $0 \leq j < N$

2. $\beta\alpha^{-kN} \pmod p$ for $0 \le k < N$.

(a) Explain how this will yield a solution to the discrete log problem and explain why it always works (assume that the numbers are small enough that the computer memory can store the lists). You may use the fact that every y with $0 \le y < N^2$ can be written in the form $y = y_0 + y_1 N$ with $y_1, y_2 \in \{0, 1, 2, \ldots, N-1\}$.
(b) Give the elliptic curve analog of the procedure. Namely, you have points A and B on an elliptic curve $E \pmod p$ and you want to find an integer x with $B = xA$. You know that $0 \le x < N^2$ for some N. You should give the steps needed to find x.

6. (18 points: 10+8) Recall that an ElGamal signature (m, r, s) is valid if $\alpha^m \equiv \beta^r r^s \pmod p$ (where (p, α, β) is the public information.
(a) Let $r \equiv \alpha\beta \pmod p$ and $s \equiv -r \pmod{p-1}$. Find a message m such that (m, r, s) is a valid ElGamal signature.
(b) Suppose that H is a good cryptographic hash function and that Alice signs $H(m)$ instead of m. In other words, (m, r, s) is valid if $\alpha^{H(m)} \equiv \beta^r r^s \pmod p$. Explain what property of H makes it difficult to use the method of part (a) to forge a valid signed message (m, r, s).