MATH/CMSC 456 (Washington) **Final Exam** **May 14, 2004**

Use 8 pages. Do a separate problem on each page. Write your name on each page. Do not staple.

1. (15 points=5+5+5) (a) Let $h(m) = m \pmod{2^{128}}$. Why is $h(m)$ a bad cryptographic hash function?
(b) Suppose Alice encrypts a 20-bit message by using a one-time pad. Eve intercepts the ciphertext and tries to use a brute force attack to determine the correct plaintext and the key? Will she succeed? Why or why not?
(c) Let E_K be the encryption function for DES using the key K. Suppose K consists of a string of sixty-four 1's. Explain why $E_K(E_K(m)) = m$ for every message m.

2. (14 points = 7+7) Let p and q be two distinct,large primes, and let $n = pq$.
(a) Suppose Eve knows a number x such that $x^2 \equiv 4 \pmod{n}$, but $x \not\equiv \pm 2 \pmod{n}$. How can Eve factor n?
(b) Suppose Alice knows p and q. Describe how she can find a number x such that $x^2 \equiv 4 \pmod{n}$, but $x \not\equiv \pm 2 \pmod{n}$.

3. (15 points = 10+5) (a) Let p and q be two distinct, large primes, and let $n = pq$. Let d and e be integers such that $de \equiv 1 \pmod{(p-1)(q-1)}$. Suppose $\gcd(x, n) = 1$. Show that if $c \equiv x^e \pmod{n}$, then $x \equiv c^d \pmod{n}$. You must indicate explicitly how Euler's theorem is being used. (You may not simply say that the problem is true because RSA works; this is what you are proving.)
(b) Suppose Bob's public key is $n = 2181606148950875138077$ and he has $e = 7$ as his encryption exponent. Alice encrypts the message *hi eve* $= 080900052205 = m$. By chance, the message m satisfies $m^3 \equiv 1 \pmod{n}$. If Eve intercepts the ciphertext, how can Eve read the message without factoring n?

4. (13 points = 9+4) (a) Let E mod p be an elliptic curve mod a large prime p. Let A and B be points on E and suppose $B = kA$ for some integer k. Peggy claims that she knows k. She wants to prove this to Victor without allowing Victor to determine k. Peggy starts by doing the following:
(i) She chooses a random integer r_1 and lets $r_2 = k - r_1$.
(ii) She computes $X_1 = r_1 A$ and $X_2 = r_2 A$.
(iii) She sends X_1, X_2 to Victor.
Describe what Victor and Peggy should do to complete the zero knowledge proof? (Victor should be at least 99.9% convinced.)

(b) Describe the analogue of the above steps (i), (ii), (iii) for proving that Peggy knows the solution to a classical discrete log problem ($\beta \equiv \alpha^k \pmod{p}$).

5. (10 points = 5+5) Recall the verification for the ElGamal signature scheme: Alice has published numbers p, α, β. A signature (m, r, s) is valid if $\alpha^m \equiv \beta^r r^s \pmod{p}$. Here is the basic existential forgery attack. Eve chooses u, v such that $\gcd(v, p-1) = 1$. She computes $r \equiv \beta^v \alpha^u \pmod{p}$ and $s \equiv -rv^{-1} \pmod{p-1}$.

(a) Prove that the pair (r, s) is a valid signature for the message $m = su \pmod{p-1}$ (of course, it is likely that m is not a meaningful message).
(b) Suppose a hash function h is used and the signature must be valid for $h(m)$ instead of for m (so we need to have $h(m) = su$). Explain how this scheme protects against existential forgery. That is, explain why it is hard to produce a forged, signed message by the this procedure.

6. (13 points = 5+5+3) (a) The sequence $001001001\cdots$ is generated by a third order recurrence $x_{n+3} \equiv c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2} \pmod 2$. Find c_0, c_1, c_2.
(b) Consider the elliptic curve $y^2 \equiv x^3 + 3 \pmod 7$. Find the sum of the points $(1, 2)$ and $(6, 3)$.
(c) Eve tries to find the sum of the points $(1, 2)$ and $(6, 3)$ on the elliptic curve $y^2 \equiv x^3 + 3 \pmod{35}$. What information does she obtain?

7. (13 points = 5+3+3+2) Let p be a large prime and suppose $\alpha^{(10^{18})} \equiv 1 \pmod p$. Suppose $\beta \equiv \alpha^k \pmod p$ for some integer k. You want to determine k.
(a) Explain why we may assume that $0 \le k < 10^{18}$.
(b) Describe a birthday attack to find k
(c) Describe a Baby Step, Giant step attack to find k. (*Hint:* One list can contain numbers of the form $\beta\alpha^{-10^9 j}$.)
(d) State at least one significant difference between the attacks in (b) and (c).

8. (7 points) The ciphertext *GBSP* (= 6, 1, 18, 15) is intercepted by Eve. She finds out that an affine cipher is being used and that the plaintext starts *do* (= 3, 14). Determine the two remaining letters of the plaintext.