MATH/CMSC 456 (Washington) Final Exam May 14, 2007

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

1. (14 points = 7+7) (a) The ciphertext TBQ was encrypted using the affine function $9x + 1 \bmod 26$. Find the plaintext. (Recall that $a = 0, b = 1, c = 2, d = 3, e = 4, f = 5, g = 6, h = 7, i = 8, j = 9, k = 10, l = 11, m = 12, n = 13, o = 14, p = 15, q = 16, r = 17, s = 18, t = 19, u = 20, v = 21, w = 22, x = 23, y = 24, z = 25$.)
(b) A third-order LFSR sequence (generated by a relation $x_{n+3} \equiv c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2} \pmod 2$) starts 001110. Find the next 4 elements of the sequence.

2. (11 points = 7+4) (a) Let $p = 7$ and let $m = 5$ be the secret. You want to share a secret among 4 people A, B, C, D so that any two can recover the secret, but no 1 person alone can recover it. Explicitly list numbers you could give to each person in order to accomplish this (your answer should have actual numbers, not just letters).
(b) Suppose Person A tries to use only her share to guess the secret. How many possibilities are there for her secret? Explain. (The number of possibilities should be a number from 1 to 7, since the secret is a number mod 7.)

3. (20 points = 12+8) (a) Which of the following can be broken quickly (in less than 10 minutes on a small computer) if a sufficiently long (but not more than 1 million bits) ciphertext-plaintext pair is known:

(1) Vigenère
(2) Hill cipher
(3) RSA (with a 300-digit n)
(4) DES

(b) Alice is trying to factor $n = 57677$. She notices that $1234^4 \equiv 1 \pmod n$ and that $1234^2 \equiv 23154 \pmod n$. How does she use this information to factor n? Describe the steps but do not actually factor n.

4. (14 points: 7+7) (a) Let p be a prime. Use Fermat's theorem to show that if $x \equiv y \pmod{p-1}$ then $m^x \equiv m^y \pmod p$, where x, y, m are integers with $\gcd(m, p) = 1$. (You need to use Fermat's theorem explicitly; you may not simply say that working mod $p-1$ in the exponent gives congruences mod p, since that is what you are proving.)
(b) Nelson tries to implement a budget version of RSA, so he chooses only one prime; call it p. He chooses e with $\gcd(e, p-1) = 1$. He makes e and p public. Alice wants to send Nelson a message m. She computes $c \equiv m^e \pmod p$ and sends c to Nelson. How can Eve decrypt c and obtain m?

5. (10 points: 7+3) Consider the following variation of the ElGamal signature scheme. Alice chooses a large prime p and a primitive root α. She also chooses a function $f(x)$ that, given an integer x with $0 \le x < p$, returns an integer $f(x)$ with $0 \le f(x) < p-1$. (For example, $f(x) = x^7 - 3x + 2 \pmod{p-1}$ for $0 \le x < p$ is one such function.) She chooses a secret integer a and computes $\beta \equiv \alpha^a \pmod p$.

The numbers p, α, β and the function $f(x)$ are made public.

Alice wants to sign a message m:

(1) Alice chooses a random integer k with $\gcd(k, p-1) = 1$
(2) She computes $r \equiv \alpha^k \pmod{p}$
(3) She computes $s \equiv k^{-1}(m - f(r)a) \pmod{p-1}$.

The signed message is (m, r, s).

Bob verifies the signature as follows:

(1) He computes $v_1 \equiv \beta^{f(r)} r^s \pmod{p}$.
(2) He computes $v_2 \equiv \alpha^m \pmod{p}$.
(3) If $v_1 \equiv v_2 \pmod{p}$, he declares the signature to be valid.

(a) Show that if all procedures are followed correctly, then the verification equation is true.
(b) Suppose Alice is lazy and chooses the constant function satisfying $f(x) = 0$ for all x. Show that Eve can forge a valid signature on every message m_1. (Give a value of k and of r and s that will give a valid signature for the message m_1.)

6. (11 points = 7+4) Alice's RSA public key is (n, e) and her private key is d. Recall that a document with an RSA signature (m, s) is valid if $m \equiv s^e \pmod{n}$. Bob wants Alice to sign a document m but he does not want Alice to read the document. Assume $m < n$. They do the following:

(1) Bob chooses a random integer k with $\gcd(k, n) = 1$. He computes $m_1 \equiv k^e m \pmod{n}$.
(2) Alice signs m_1 by computing $s_1 \equiv m_1^d \pmod{n}$.
(3) Bob divides s_1 by k mod n to obtain $s \equiv k^{-1} s_1 \pmod{n}$.

(a) Show that (m, s) is valid.
(b) Why is it assumed that $\gcd(k, n) = 1$?

7. (10 points) E is an elliptic curve mod a prime p, and A and B are points on E. Peggy claims to know an integer s such that $sA = B$. She wants to prove this to Victor without revealing any information about s. Let n be an integer such that $nA = \infty$.

They do the following:

(1) Peggy chooses a random integer r_1 and lets $r_2 \equiv s - r_1 \pmod{n}$.
(2) Peggy computes $R_1 = r_1 A$ and $R_2 = r_2 A$.

Describe the remainder of the procedure. Victor should be at least 99.9% sure that Peggy knows s.

8. (10 points) Suppose Alice signs contracts using a 30-bit hash function h (and h is known to everyone). If m is the contract, then $(m, sig(h(m)))$ is the signed contract (where *sig* is some public signature function). Eve has a file of 2^{20} fraudulent contracts. She finds a file with 2^{20} contracts with valid signatures (by Alice) on them. Describe how Eve can accomplish her goal of putting Alice's signature on at least one fraudulent document.