MATH/CMSC 456 (Washington) Final Exam May 16, 2002

1. (22 points= 9+9+4) (a) Solve $7d \equiv 1 \pmod{100}$.
(b) Suppose Alice encrypts a message m to get a ciphertext c using the formula $c \equiv m^7 \pmod{101}$. Describe how to decrypt c to obtain m. You may assume that $0 < m < 101$. You must use the result of part (a) in your answer.
(c) If m is an integer larger than 101, what should Alice do to encrypt m by the procedure of (b)?

2. (31 points=9+9+4+9) (a) A child writes a string of letters and a parent encrypts it with a Vigenère cipher with key length either 2 or 3, yielding the following ciphertext:

$$CATCTTDBTHBAH$$

Determine which is the more likely key length, two or three, and explain why. Do not decrypt the message.
(b) Explain how to do a chosen plaintext attack on an affine cipher (state what plaintexts you would choose and how you would find the encryption function).
(c) What was the main reason why DES needed to be replaced by AES?
(d) Let E be the elliptic curve $y^2 \equiv x^3 + 4x + 4 \pmod{7}$. Let $P = (0, 2)$ and $Q = (1, 4)$. Find the sum $P + Q$ on E.

3. (26 points=4+9+4+9) Alice and Bob play a game as follows. Alice chooses two large primes p and q with $p \neq q$ and with $p \equiv q \equiv 3 \pmod{4}$. She multiplies them and sends $n = pq$ to Bob. Bob chooses a random integer x with $\gcd(x, n) = 1$ and computes $y \equiv x^2 \pmod{n}$. He sends y to Alice. Alice computes a number s with $s^2 \equiv y \pmod{n}$ and sends s to Bob. If $s \equiv \pm x \pmod{n}$, then Bob says that Alice wins. If $s \not\equiv \pm x \pmod{n}$, then Bob says that he wins.

Note that Alice does not tell Bob what p and q are. Also, Bob does not tell Alice the value of x.

(a) How can Bob determine that $\gcd(x, n) = 1$ without factoring n? (your answer can be fewer than 6 words)
(b) How does Alice compute s? (The number $(p + 1)/4$ might be useful.)
(c) What is the probability that $s \equiv \pm x \pmod{n}$?
(d) If Bob wins, he can factor n. Explain how he can do this. (This allows Alice to check that Bob doesn't cheat.)

4. (14 points=5+9) Consider the following elliptic curve protocol: Alice wants to send a message m to Bob. Alice and Bob publicly determine an elliptic curve E mod a large prime p and an integer n such that $nP = \infty$ for all points P on E. Alice represents m as a point P_0 on E by some publicly known procedure (the procedure is known, but not P_0 or m). They perform the following steps:

(1) Alice chooses a secret integer a with $\gcd(a, n) = 1$ and Bob chooses a secret integer b with $\gcd(b, n) = 1$.
(2) Alice computes $P_1 = aP_0$ and sends P_1 to Bob.
(3) Bob computes $P_2 = bP_1$ and sends P_2 to Alice.
(4) Alice computes $a_1 \equiv a^{-1} \pmod{n}$ and computes $P_3 = a_1 P_2$. She sends P_3 to Bob.
(5) Bob computes $b_1 \equiv b^{-1} \pmod{n}$ and computes $P_4 = b_1 P_3$. It can be shown that $P_4 = P_0$, so Bob has received the message m (that is, he can extract m from P_0).

(a) Suppose Eve knows how to compute discrete logs for elliptic curves and she listens to the communications between Alice and Bob. How can she determine the secret integers a and b? (This also allows Eve to determine P_0, and therefore m, but don't show this.)
(b) Describe a classical version (that is, a non-elliptic curve version related to the classical discrete log problem) of the above protocol in which the message is now an integer m mod a large prime p.

5. (9 points) Your opponent uses RSA with $n = pq$ and encryption exponent e and encrypts a message m. This yields the ciphertext $c \equiv m^e \pmod{n}$. A spy tells you that, for this message, $m^{12345} \equiv 1 \pmod{n}$. Describe how to determine m. Note that you do not know p, q, $\phi(n)$, or the secret decryption exponent d. However, you should find a decryption exponent that works for this particular ciphertext. Moreover, explain carefully why your decryption works (your explanation must include how the spy's information is used).

6. (14 points=7+7) Recall the ElGamal signature scheme: Alice wants to sign a message m. She chooses a prime p, a primitive root α, and a secret integer a, and computes $\beta \equiv \alpha^a \pmod{p}$. The numbers p, α, β are made public. To sign m, Alice computes integers r and s. The signed message is (m, r, s). Bob verifies the signature by checking that $\beta^r r^s \equiv \alpha^m \pmod{p}$.
(a) Let u, v be integers with $\gcd(v, p-1) = 1$. Let $r_1 \equiv \alpha^u \beta^v \pmod{p}$ and $s_1 \equiv -r_1 v^{-1} \pmod{p-1}$. Let $m_1 \equiv s_1 u \pmod{p}$. Show that (m_1, r_1, s_1) is a valid signed message.
(b) Suppose $h(m)$ is a good cryptographic hash function that is made public. Suppose that the hash of a message is signed, instead of the message. Then a signed message is of the form (m, r, s), where (r, s) is a valid ElGamal signature for $h(m)$. If Eve chooses integers u, v as in part (a) and computes r_1 and s_1, why is it difficult for her to produce a signed message (m, r_1, s_1)?

7. (9 points) Let E_K and D_K denote the encryption and decryption functions with respect to a key K for some cryptosystem. Suppose double encryption is used, so a message m is encrypted as $E_{K_1}(E_{K_2}(m))$ to yield the ciphertext c. You obtain several plaintext-ciphertext pairs (m_i, c_i). How can you determine the pair of keys (K_1, K_2) that is being used for these encryptions?

Assume that there are approximately 10^{10} choices of keys K, so there are around 10^{20} pairs of keys (K_1, K_2), which is slightly more than you are able to check if you check the pairs one at a time. It is possible that there are several pairs of keys such that the encryption of some m_j with these keys yields c_j. However, you may

assume that there is only one key pair (K_1, K_2) that works for all of the pairs (m_i, c_i).. It is very likely that you will require more then one of the plaintext-ciphertext pairs to determine the correct key.

8. (15 points=5+5+5) Let $n = pq$ be the product of two distinct large primes. Let y be a square mod n. Peggy wants to convince Victor that she knows a square root s of y mod n, without revealing the value of s. They do the following: (1) Peggy chooses random integers r_1 and r_2 with $r_1 r_2 \equiv s \pmod{n}$. (2) She computes $x_1 \equiv r_1^2 \pmod{n}$ and $x_2 \equiv r_2^2 \pmod{n}$, and sends x_1 and x_2 to Victor. (3) Victor checks that $x_1 x_2 \equiv y \pmod{n}$. (4) Victor chooses either x_1 or x_2, call it x_i, and asks Peggy for a square root of x_i. (5) Peggy supplies the requested square root r_i.

Steps (1) through (5) are repeated several times.

(a) Why should Peggy choose new integers r_1 and r_2 each time?
(b) Suppose Peggy guesses correctly that Victor will ask for r_2 in the first round. If she does not know s, how does she provide numbers x_1, x_2 in step (2) in such a way that she will be able to complete this round successfully?
(c) If Peggy does not know s, what is the probability that she can successfully complete 10 rounds of the procedure?