**MATH/CMSC 456 CRYPTOLOGY**
**FINAL EXAM SPRING 2003**

**1.** (15 points) Describe how you would choose your plaintext for a chosen plaintext attack on each of the following, and say how would you obtain the key:
(a) Vigenère cipher.
(b) Hill cipher (with a $2 \times 2$ matrix).
(c) Affine cipher.

**2.** (15 points = 7+8) Suppose your RSA modulus is $n = 55 = 5 \times 11$ and your encryption exponent is $e = 3$.
(a) Find the decryption modulus $d$.
(b) Show that if $c \equiv m^3 \pmod{55}$ is the ciphertext, then the plaintext is $m \equiv c^d \pmod{55}$. You may assume that $\gcd(m, 55) = 1$. You may not quote the fact that RSA decryption works. That is what you are showing in this specific case.

**3.** (14 points = 7+7) (a) Suppose you know that

$$33335^2 \equiv 670705093^2 \pmod{670726081}.$$

Describe how you can use this information to factor 670726081 (do not actually factor it).

(b) Consider the sequence starting $k_1 = 1, k_2 = 0, k_3 = 1$, and defined by the third order recurrence

$$k_{n+3} \equiv k_{n+2} + k_{n+1} + k_n \pmod{2}.$$

This sequence can also be given by a second order recurrence. Determine this second order recurrence by setting up and solving the appropriate equations.

**4.** (15 points = 6+4+5) Alice signs documents as follows: She has an RSA modulus $n$, public encryption exponent $e$, and private decryption exponent $d$. To sign $m$, she computes $s \equiv m^d \pmod{n}$. Then $(m, s)$ is the signed message. Bob verifies that this is a valid signature by checking that $m \equiv s^e \pmod{n}$.
(a) Suppose Eve has a message $m_1$ that she wants to sign. Why should it be difficult for Eve to find $s_1$ such that $(m_1, s_1)$ is a valid signed message? Your answer should relate Eve's problem to the security of RSA.
(b) Eve can produce a valid signed message $(m_2, s_2)$ as follows: She chooses a random $s_2$ and sets $m_2 \equiv s_2^e \pmod{n}$. Show that this yields a valid message, although it is likely that $m_2$ will be meaningless.
(c) Suppose $H$ is a cryptographic hash function. Instead of signing $m$, suppose people sign $H(m)$. A valid signed message is therefore $(m, s)$, where $s^e \equiv H(m) \pmod{n}$. Explain why it should be difficult for Eve to produce a valid signed

message by the method of (b) (that is, explain why is it difficult for Eve to choose a random $s_3$ and find a message $m_3$ such that $(m_3, s_3)$ is a valid signed message).

**5.** (8 points = 4+4) Consider the following DES-like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length $n$ (a left half and a right half): $M_0M_1$. The key consists of $n$ bits. One round of encryption starts with a pair $M_jM_{j+1}$. The output is the pair $M_{j+1}M_{j+2}$, where

$$M_{j+2} = M_j \oplus K \oplus M_{j+1}.$$

($\oplus$ means XOR, which is addition mod 2 on each bit). This is done for $m$ rounds, so the ciphertext is $M_mM_{m+1}$.
(a) Suppose the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the key? Justify your answer.
(b) Suppose the encryption process consists of $m = 3$ rounds. Why is this system not secure? Justify your answer.

**6.** (8 points) Let $p$ be a large prime, let $\alpha$ be a primitive root mod $p$, and let $\beta \equiv \alpha^x \pmod{p}$. Peggy claims to know $x$. Victor wants to verify this without determining the value of $x$. The first few steps of the procedure are as follows. Peggy chooses two random numbers $r_1$ and $r_2$ such that $r_1 + r_2 \equiv x \pmod{p-1}$, then computes $x_1 \equiv \alpha^{r_1} \pmod{p}$ and $x_2 \equiv \alpha^{r_2} \pmod{p}$. She sends $x_1$ and $x_2$ to Victor. Before proceeding, Victor of course checks that $\beta \equiv x_1x_2 \pmod{p}$. Describe a zero-knowledge verification that Peggy knows $x$, using these steps as the beginning of the procedure. The procedure should be such that Victor believes the chance Peggy does not know $x$ is less than 1/1000.

**7.** (10 points = 5+5) Suppose we have a (2,4) Shamir secret sharing scheme mod the prime $p = 13$. Participants A, B, C are given the following valid shares:

$$A: \quad (1, 11), \qquad B: \quad (2, 3), \qquad C: \quad (3, 8).$$

(a) What is the secret?
(b) Suppose D has the point (4, 7). Is this a valid share? Explain why or why not.

**8.** (15 points = 3+5+7) Let $E$ be an elliptic curve and let $Q$ be a point on $E$. Both $E$ and $Q$ are publicly known. Alice and Bob want to establish a key for some cryptographic purpose. They proceed as follows:

(1) Alice chooses a secret integer $a$ and Bob chooses a secret integer $b$.
(2) Alice computes $A = aQ$ and Bob computes $B = bQ$.
(3) Alice sends $A$ to Bob and Bob sends $B$ to Alice.
(4) Alice computes $aB$ and Bob computes $bA$. They extract the last 100 bits of the $x$-coordinates of these points to obtain the key.

(a) Show that $aB = bA$.
(b) Suppose Eve knows how to compute discrete logs for elliptic curves and assume Eve intercepts all communications between Alice and Bob. Show how she can find the key that Alice and Bob establish.
(c) Give a non-elliptic curve version of this protocol. Namely, replace $E$ by integers mod a prime $p$ and replace $Q$ by a primitive root mod $p$, and describe the steps Alice and Bob follow.