MATH/CMSC 456 (Washington) Exam 1 March 21, 2003

1. (20 points = 14+6) Suppose that you want to encrypt a message using an affine cipher. You let $a = 0$, $b = 1$, ..., $z = 25$, but you also include ? = 26, ; = 27, " = 28, ! = 29. Therefore, you use $x \mapsto \alpha x + \beta \pmod{30}$ for your encryption function, for some integers α and β.
(a) Show that there are exactly eight possible choices for the integer α (that is, there are only eight choices of α (with $0 < \alpha < 30$) that allow you to decrypt).
(b) Suppose you try to use $\alpha = 10$, $\beta = 0$. Find two plaintext letters that encrypt to the same ciphertext letter.

2. (20 points) Suppose Eve knows that the plaintext is *aaaaaaaa*... and Eve has intercepted the ciphertext. For each of the following cipher systems, state whether or not Eve can determine the key:
(a) shift cipher
(b) affine cipher
(c) Hill cipher, with a 2×2 matrix
(d) Vigenère cipher

3. (12 points) The sequence 1010001101000110 was generated by a recurrence

$$x_{n+4} \equiv c_0 x_n + c_1 x_{n+1} + c_2 c_{n+2} + c_3 x_{n+3} \pmod{2}.$$

Set up, but do not solve, the matrix equation to find the coefficients c_0, c_1, c_2, and c_3.

4. (15 points) Bob's RSA modulus is $n = pq$ for some large distinct primes p, q. His encryption exponent is e. Alice sends Bob the message m, encrypted as $c \equiv m^e \pmod{n}$. After decrypting the message, Bob remarks to Eve that the message has the interesting property that $m^{12345} \equiv 1 \pmod{n}$. Eve knows n, e, c, but does not know p, q, m. Explain how Eve can use Bob's remark to find the message m. Prove that this method actually finds m. You may assume that $\gcd(e, 12345) = 1$. (*Note:* Eve does not factor n and she cannot calculate $\phi(n)$. Also, she cannot find all messages with $m^{12345} \equiv 1$ since she cannot factor n. Instead, she finds a decryption exponent that works for this particular message.)

5. (13 points) Suppose you have two distinct large primes p and q. Explain how you can find an integer x such that

$$x^2 \equiv 49 \pmod{pq}, \qquad x \not\equiv \pm 7 \pmod{pq}.$$

6. (20 points: 10+10) Suppose n is a large odd number. You calculate $2^{(n-1)/2} \equiv k \pmod{n}$, where k is some integer with $k \not\equiv \pm 1 \pmod{n}$.
(a) Suppose $k^2 \not\equiv 1 \pmod{n}$. Explain why this implies that n is not prime.
(b) Suppose $k^2 \equiv 1 \pmod{n}$. Explain how you can use this information to factor n.