MATH/CMSC 456 (Washington) **Name:**______________________________
Exam 2 May 5, 2015

1. (15 points = 5+5+5) You are given that 14 is a primitive root for the prime $p = 30000001$. Let $b \equiv 14^{9000000} \pmod{p}$. (The exponent is $3(p-1)/10$.)
(a) Explain why $b^{10} \equiv 1 \pmod{p}$.
(b) Explain why $b \not\equiv 1 \pmod{p}$.
(c) Let p be a 300-digit prime. Define a hash function

$$H(x) = 2^x \pmod{p}.$$

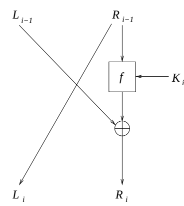
Although H can be computed quickly, it is not fast enough to be a good hash function. Give one more property of cryptographic hash functions that H does not satisfy and give one property that H satisfies. You must justify your answers.

2. (20 points = 10+10) **(a)** Alice wants to encrypt her messages securely, but she can afford only an encryption machine that uses a 25-bit key. To increase security, she chooses 4 keys K_1, K_2, K_3, K_4 and encrypts four times:

$$c = E_{K_1}(E_{K_2}(E_{K_3}(E_{K_4}(m)))).$$

Eve finds several plaintext-ciphertext pairs (m, c) encrypted with this set of keys. Describe how she can find (with high probability) the keys K_1, K_2, K_3, K_4. (For this problem, assume that Eve can do at most 2^{60} computations, so she cannot try all 2^{100} combinations of keys). (*Note:* If you use only one of the plaintext-ciphertext pairs in your solution, you probably have not done enough to determine the keys.)

(b) Bud gets a budget 2-round Feistel system. It uses a 32-bit L, a 32-bit R, a 32-bit key K, and the function $f(R, K) = R \oplus K$, with the same key for each round. Moreover, to avoid transmission errors, he always uses a 32-bit message M and lets $L_0 = R_0 = M$. Eve does



not know Bud's key but she obtains the ciphertext for one of Bud's encryptions. Describe how Eve can obtain the plaintext M and the key K.

3. (30 points = 5++5+5+5+5) Alice wants to sign a document m. She uses the following variant of the ElGamal Signature scheme. She chooses a prime p and a primitive root g. Then she chooses a random integer a and computes $h \equiv g^a \pmod{p}$. To sign m, she chooses a random integer k, computes $r \equiv g^k \pmod{p}$, and $s \equiv ar + km \pmod{X}$, where X is specified below. The signature is valid if $g^s \equiv h^r r^m \pmod{p}$.

(a) What is a suitable value of X ? Explain why.

(b) Show that if Alice signs correctly then the signature is valid.

(c) Suppose Eve tries to forge Alice's signature on a document m' by choosing a random k, computing $r \equiv g^k \pmod{p}$, and then finding s. Explain why Eve probably will not succeed. (*Hint:* The answer is not that Eve does not know a. Maybe she has a method that avoids knowledge of a.)

(d) Suppose Eve chooses $r \equiv hg \pmod{p}$ with $0 < r < p$ and then sets $s = m = p - 1 - r$. Show that (m, r, s) is a valid message.

(e) Suppose H is a cryptographic hash function, and Alice signs the hash of m. Give the equations Alice uses to generate a valid signed message (m, r, s) and those that Bob uses to verify the signature.

(f) When Alice signs with a cryptographic hash function, as in part (e), why is it hard for Eve to generate a valid signed message by the method of part (d)?

4. (20 points = 10+10) **(a)** Let E be the elliptic curve $y^2 \equiv x^3 + x + 1 \pmod{13}$. Evaluate $(4, 2) + (5, 12)$ on E.
(b) Let $p = 999983$, which is prime. The elliptic curve $E: \quad y^2 \equiv x^3 + 1 \pmod{p}$, has $N = 999984$ points. Suppose you are given points P and Q on E and are told that there is an integer k such that $Q = kP$. Describe a birthday attack that is expected to find k. (You should say approximately how long you will make your lists.)

5. (15 points = 5+5+5) Let n and e be an RSA modulus and encryption exponent, and suppose m is a message encrypted as $c \equiv m^e \pmod{n}$. Victor and Peggy know n, e, c. Peggy wants to use a zero-knowledge protocol to convince Victor that she knows m, without revealing any information about m. She writes $m \equiv r_1 r_2 \pmod{n}$ and she lets $c_1 \equiv r_1^e \pmod{n}$ and $c_2 \equiv r_2^e \pmod{n}$. She sends c_1 and c_2 to Victor, who checks that $c_1 c_2 \equiv c \pmod{n}$. Victor then chooses $i = 1$ or 2 and asks for r_i, which Peggy sends.

(a) Give the remaining steps in the protocol.

(b) Suppose Peggy does not know m but knows that Victor is going to ask for r_2. What should she do?

(c) If Peggy knows m, what is a good procedure for choosing r_1 and r_2? (choosing r_1 and r_2 randomly until their product is $m \bmod n$ is not a good method)