MATH/CMSC 456 (Washington) **Name:**________________________________
Exam 2 **December 4, 2015**

1. (20 points = 10+10) **(a)** Let p be a 3000-digit prime, let h be a good cryptographic hash function, and let $H(x) = h(x \bmod p)$. The function H can be computed quickly. What other properties of cryptographic hash functions does H satisfy and what properties does it not satisfy? Explain your answers.
(b) Calculate the sum $(1, 2) + (2, 5)$ on the elliptic curve $y^2 \equiv x^3 + 3x \pmod{11}$.

2. (20 points = 10+10) Let p be a large prime, let g be a primitive root mod p, and let h be nonzero mod p. Peggy claims to know s such that $g^s \equiv h \pmod{p}$. She wants to prove this to Victor by the following procedure:

1. Peggy chooses a random integer $r_1 \pmod{p-1}$ and lets $r_2 \equiv s - r_1 \pmod{p-1}$.
2. Peggy computes $y_1 \equiv g^{r_1} \pmod{p}$ and $y_2 \equiv g^{r_2} \pmod{p}$ and sends y_1 and y_2 to Victor.
3. Victor chooses $i = 1$ or 2 and asks for r_i.
4. Peggy sends r_i to Victor.
5. Victor checks that $y_i \equiv g^{r_i} \pmod{p}$.
6. They repeat the previous steps several times.

(a) Suppose Peggy does not know s. Describe how she can successfully complete every repetition of this procedure successfully.
(b) Explain what step needs to be added in order to make the procedure into a zero-knowledge proof where Peggy will have difficulty cheating successfully.

3. (25 points = 10+10+5) **(a)** Each person in the world flips 100 coins and obtains a sequence of length 100 consisting of Heads and Tails. (There are $2^{100} \approx 10^{30}$ possible sequences.) Assume that there are approximately 10^{10} people in the world. What is the probability that two people obtain the same sequence of Heads and Tails? Your answer should be accurate to at least 2 decimal places.
(b) Let E_K denote DES encryption with key K. Suppose you quadruple encrypt by choosing two keys K_1 and K_2 and computing the ciphertext as $c = E_{K_1}(E_{K_1}(E_{K_2}(E_{K_2}(m))))$. Eve intercepts c and someone tells her what m is. Describe a method where Eve can find at least one key pair (L_1, L_2) that encrypts m to c by this quadruple encryption method.
(c) In part (b), suppose you take K_1 to be the key consisting of all 1's and K_2 to be the key consisting of all 0's. Eve examines some plaintext-ciphertext pairs and decides she does not need to do a meet-in-the-middle attack to read future messages. Why?

4. (35 points = 10+10+5+10) Consider the following variant of the ElGamal Signature Scheme: Alice chooses a large prime p, a primitive root g, and a secret integer a. She computes $h \equiv g^a \pmod{p}$. The numbers p, g, h are made public and a is kept secret. If $m < p - 1$, Alice signs m as follows: She chooses a random integer k and computes $r \equiv g^k \pmod{p}$ and $s \equiv am + kr \pmod{p-1}$. The signed message is (m, r, s). Bob verifies the signature by checking that $g^s \equiv h^m r^r \pmod{p}$. If $m \geq p - 1$, she breaks m into blocks and signs each block.
(a) Show that if Alice signs correctly then the verification congruence is satisfied.
(b) Suppose Eve has a document m_1 and she wants to forge Alice's signature on m_1. That is, she wants to find r_1 and s_1 such that (m_1, r_1, s_1) is valid. Eve chooses $r_1 = 2015$ and tries to find a suitable s_1. Why will it probably be hard to find s_1?
(c) Suppose Alice has a very long message m and wants to decrease the size of the signature. How can she

use a hash function to do this? Explicitly give the modifications of the above equations that must be done to accomplish this.

(d) If Alice uses an elliptic curve version of the signature procedure, she chooses an elliptic curve E, a point P on E, a secret integer a, and computes $Q = aP$. Give the equations that she uses to sign m and that Bob uses to verify the signature. (*Hint:* The integer s is defined as $s \equiv am + kx \pmod{n}$, where x is the x-coordinate of a point $R = (x, y)$, and where n is the number of points on E.)