MATH/CMSC 456 (Washington) Sample Problem for Exam 2

1. Suppose you have the following arrangement of doors and tunnels. Each door can be opened from inside the Central Chamber. However, if you are in a tunnel, then it requires opening a lock to open a door and enter the Central Chamber. Peggy claims she can unlock one of the doors. Victor wants to verify this claim. Peggy does not want Victor to know which door she can open. Describe a zero-knowledge type procedure for Victor to verify Peggy's claim.

(Look at the figure on page 233 of the book)

2. (a) Let p be prime and let g be a primitive root. Show that $g^{(p-1)/2} \equiv -1 \pmod{p}$.

(b) 5 is a primitive root for the prime 1223. You want to solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Given that $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd.

3. Consider the following public key system. Alice secretly chooses large primes p and q, both $\equiv 3 \pmod{4}$, and computes $n = pq$, which she makes public. Bob has a message m that he wants to send to Alice. He randomly chooses an integer x, checks that $\gcd(x, n) = 1$, calculates $x_1 \equiv xm \pmod{n}$ and $x_2 \equiv x^2 \pmod{n}$, and sends the pair (x_1, x_2) to Alice.

Explain how Alice decrypts to find m, and explain why the evil eavesdropper Eve cannot find m. Be sure to give all the steps Alice uses, and what she can do that Eve cannot do.

4. Recall that the ElGamal signature scheme is as follows:

Suppose Alice wants to sign a message. She chooses a large prime p, a primitive root α, and a secret integer a such that $1 \leq a \leq p-2$, and calculates $\beta \equiv \alpha^a \pmod{p}$. The values of p, α, and β are made public.

In order for Alice to sign a message m she does the following:

(1) Selects a secret random k such that $\gcd(k, p-1) = 1$.
(2) Computes $r \equiv \alpha^k \pmod{p}$
(3) Computes $s \equiv k^{-1}(m - ar) \pmod{p-1}$

The signed message is the triple (m, r, s).

Bill can verify the signature as follows:

(1) Compute $v_1 \equiv \beta^r r^s \pmod{p}$, and $v_2 \equiv \alpha^m \pmod{p}$.
(2) The signature is declared valid if and only if $v_1 \equiv v_2 \pmod{p}$.

(a) Explain why the congruence defining s is mod $p-1$, instead of mod p.

(b) Suppose Alice's random number generator is broken, so she uses $k = a$ in the signature scheme. How will Eve notice this and how can Eve determine the values of k and a (and thus break the system)?

5. 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 2 subkeys K_1, K_2 of k bits each, for some integer k. There is a function $f(K, M)$ that takes an input of k bits and n bits and gives an output 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

$$M_{j+2} = M_j \oplus f(K_{j+1}, M_{j+1}).$$

($\oplus$ means XOR, which is addition mod 2 on each bit). This is done for 2 rounds, so the ciphertext is M_2M_3.

How would you use the *same* machine to decrypt the ciphertext M_2M_3? You should say what the input to the machine is and what keys are to be used, and you should show that the decryption actually works. (You may not simply quote results about systems such as this.)