MATH/CMSC 456 Sample Problems Exam 2 Solutions

1. Victor stands outside so that he cannot see into the tunnels. Peggy goes in and goes through a tunnel to the central chamber. If she can unlock the door, she enters the central chamber. If not, she waits outside the door. Victor, after giving Peggy time to do this, goes into the entrance to the system of tunnels. He call out the name of one of the tunnels. Peggy should come out of the central chamber via that tunnel. They repeat this procedure several time until Victor is convinced.

2. (a) $(g^{(p-1)/2})^2 = g^{p-1} \equiv 1 \pmod{p}$. Therefore, $g^{(p-1)/2} \equiv \pm 1$. But g is a primitive root, so $p-1$ is the first exponent where you get $+1$. Therefore, $g^{(p-1)/2} \equiv -1$.

(b) Since 5 is a primitive root, $5^{611} \equiv -1 \pmod{1223}$. Therefore, $1 \equiv 3^{611} \equiv 5^{611x} \equiv (-1)^x$, so x is even.

3. Alice finds the square roots of x mod p and mod q, then uses the Chinese Remainder Theorem to find the four square roots of x_2 mod n. She divides x_1 by each of these four possible values of x to get four possible values of m. Probably only one m will be a meaningful message.

If Eve has a way to find m, then she can divide x_1 by m and get x. This means that she can do square roots mod n, which is equivalent to being able to factor n.

4. (a) s occurs in the exponent, and exponents arew always mod $p-1$.

(b) Eve notices that $r = h$ (or β) and therefore knows that $k = a$. Since Eve knows s, m, r, p, and she also knows that $as = ks \equiv m + ar$, she can write $a(s-r) \equiv m$. She divides by $s-r$ and gets $\gcd(s-r, p-1)$ possibilities for a. She tries these to see which gives $h \equiv g^a \pmod{p}$ (or $\alpha^a \equiv \beta$).

5. Switch left and right halves and use the same procedure as encryption. Then switch the left and right of the final output. Verification is the same as that on pages 115-116.