1. Label the tunnels 1, 2, 3, 4. Peggy enters one of the tunnels while Victor waits outside. Then Victor goes to the entrance and calls out 1, 2, 3, or 4. Peggy is required to come out via that tunnel. This is repeated several times.

2. (a) Let $x = g^{(p-1)/2}$. Then $x^2 \equiv g^{p-1} \equiv 1 \pmod{p}$. Therefore $x \equiv \pm 1 \pmod{p}$. But $g$ is a primitive root, which means that $p-1$ is the smallest positive exponent $k$ such that $g^k \equiv 1 \pmod{p}$. Since $0 < (p-1)/2 < p-1$, we cannot have $g^{(p-1)/2} \equiv 1$. Therefore, $g^{(p-1)/2} \equiv -1 \pmod{p}$.

(b) Raise both sides to the $611 = (p-1)/2$ power to obtain $5^{611x} \equiv 3^{611} \equiv 1 \pmod{1223}$. Since $5^{611} \equiv -1$ by part (a), we have $(-1)^x \equiv 1$. Therefore $x$ is even.

3. Alice knows $p$ and $q$ and therefore can find the four square roots $s_1, \ldots, s_4$ of $x_2 \pmod{n}$. She computes $x_1s_1^{-1}, x_2s_2^{-1}$ and sees which is a meaningful message. It should be $m$.

Eve cannot find the square root $x$ of $x_2$, since being able to find square roots is as hard as factoring. Note that finding $x$ is equivalent to finding $m$, since $x \equiv x_1m^{-1}$ and $m \equiv x_1x^{-1}$.

4. (a) $s$ appears in the exponent in the verification congruence. Since the congruence is mod $p$, the exponent must be mod $p-1$.

(b) If $k = a$, then $\beta = r$, so Eve will recognize this. Also, $s \equiv a^{-1}(m-ar) \equiv a^{-1}m-r \pmod{p-1}$. Therefore, $a^{-1}m \equiv r + s$. Let $d = \gcd(m, p-1)$. Then there are $d$ values of $a^{-1}$ satisfying this congruence, so we have $d$ possible values of $a$. Try each one and see which satisfies $a^a \equiv \beta \pmod{p}$. This will be the correct $a$.

5. Switch $M_2$ and $M_3$ and input $M_3M_2$. First use key $K_2$. This round outputs $M_2$ on the left and $M_3 \oplus f(K_2, M_2)$ on the right. But $M_3 = M_1 \oplus f(K_2, M_2)$, so the output on the right is $M_1$. Therefore we have $M_2M_1$ after one round of decryption. For the second round, use key $K_1$. By the same reasoning, with all subscripts lowered by 1, we see that the output of this round is $M_1M_0$. Switch left and right to obtain the plaintext $M_0M_1$. 