Solutions to Sample Exam 2

1. (a) Round 1: Peggy chooses r_1 randomly, computes $h_1 \equiv \alpha^{r_1} \pmod{p}$ and computes $h_2 \equiv \beta h_1^{-1} \pmod{p}$. She sends h_1, h_2 to Victor. When Victor asks for r_1, she sends it. Round 2: Peggy chooses r_2 randomly, computes $h_2 \equiv \alpha^{r_2} \pmod{p}$ and computes $h_1 \equiv \beta h_2^{-1} \pmod{p}$. She sends h_1, h_2 to Victor. When Victor asks for r_2, she sends it.

(b) Peggy will need to solve $\alpha^{r_2} \equiv h_2 \pmod{p}$ for r_2. This is a discrete log problem, which is hard.

2. (a) If there are n possible birthdays and two lists, each with around $\sqrt{n}$ elements, then it is likely that some element from the first will match some element from the second. In part (a), Eve makes two lists: one is the hashes of 10^4 of Alice's checks, the other is the hashes of the 10^4 fraudulent checks. Since there are $n = 2^{20} \approx 10^6$ hash values, and 10^4 is much larger than $\sqrt{n} \approx 10^3$, there is almost certainly a match. Eve then takes the signature of the hash of Alice's check that matches the hash for a bad check, and uses Alice's signature on this fraudulent check.

(b) In this case, $n \approx 10^{60}$, so $\sqrt{n} \approx 10^{30}$, which is much larger than 10^4. Therefore it is unlikely that there is a match.

3. (a) $u_2 \equiv \beta^m r^r \equiv \alpha^{am}\alpha^{kr} \equiv \alpha^s \equiv u_1$.

(b) $am \equiv s - kr \pmod{p-1}$. There are $\gcd(m, p-1)$ solutions a to this congruence. Try each one until $\beta \equiv \alpha^a \pmod{p}$ is satisfied.

(c) Eve must satisfy the verification congruence $\alpha^s \equiv \beta^m r^r \pmod{p}$. She has already chosen m and r. Therefore she must solve (for s) the discrete log problem $\alpha^s \equiv c \pmod{p}$, where $c = \beta^m r^r$ is known to Eve. This should be hard to do because discrete logs are hard. (Note that no mention of a and k is made in the verification congruence.)

4. The whole situation does not depend on the choice of the function f. Switch left and right and put R_3L_3 into the encryption machine. Usually, the keys would have to be taken in reverse order, but here the key is the same for each round. After three rounds, R_0L_0 comes out. The verification is identical to the one given at the bottom of page 99 in the book. Switch left and right to get the original plaintext L_0R_0.

5. (a) Eve knows P_1 and $P_2 = bP_1$. Eve solves a discrete log to find b. Similarly, Eve knows P_2 and $P_3 = a_1P_2$. Eve solves a discrete log to find a_1. She then calculates $a \equiv a_1^{-1} \pmod{n}$ to get a.

(b) Alice and Bob publicly agree on a large prime p. Alice chooses a secret integer a with $\gcd(a, p-1) = 1$ and Bob chooses a secret integer b with $\gcd(b, p-1) = 1$. Alice sends $m_1 \equiv m^a \pmod{p}$ to Bob. Bob sends $m_2 \equiv m_1^b$ to Alice. Alice computes $a_1 \equiv a^{-1} \pmod{p-1}$ and sends $m_3 \equiv m_2^{a_1} \pmod{p}$ to Bob. Bob computes $b_1 \equiv b^{-1} \pmod{p-1}$ and computes $m_4 \equiv m_3^{b_1} \pmod{p}$. It can be shown that $m_4 \equiv m \mod p$.