1. (a) $11 \equiv 44 \cdot 2^{-2} \equiv 3^6 \cdot 3^{-20} \equiv 3^{-14}$. Since $3^{136} \equiv 1$, we have $11 \equiv 3^{-14+136} \equiv 3^{122}$. Therefore, $x = 122$.
(b) Since $H(x + 10^{100}) = H(x)$, it is easy to find collisions.

2. (a) If $\beta^{-1} \alpha^{-1} \equiv \alpha^{-j}$, then $\beta \equiv \alpha^{i+j}$, so $x \equiv i + j \pmod{p-1}$.
(b) If there are $N$ birthdays, the birthday attack needs approximately $\sqrt{N}$ on each list to get a 50% chance of a match. Therefore, $M$ should be approximately $10^{15}$.

3. (a) $v_1 \equiv \alpha (m \alpha^{-k})^s (\alpha^a)^{f(r)} \equiv m^s \alpha^{1-ks-af(r)} \equiv m^s \alpha^0 \equiv v_2$.
(b) One way: Eve follows steps (1) through (4). Since $a$ is multiplied by $f(r) = 0$, she never needs $a$, which is the only secret Alice has.
Another way: Choose $s = 1$ and $r \equiv \alpha^{-1}m$.

4. (a) Peggy chooses random integers $r_1$ and $r_3$ and computes $m_1 \equiv \alpha^{r_1}$ and $m_3 \equiv \alpha^{r_3}$. She lets $m_3 \equiv \beta m_1^{-1} m_3^{-1}$. Since Victor does not ask for $r_2$, Peggy does not need to know it.
(b) If Peggy does not know $x$, then she cannot know all of $r_1, r_2, r_3$, since $r_1 + r_2 + r_3 \equiv x \pmod{p-1}$. Therefore, there is at least one of the $r_i$’s that Peggy does not know. The probability is $2/3$ that Victor will ask for that value in any given round. Therefore, after several rounds, it is very likely that he will discover that Peggy does not know $x$.

5. Note that $L_2 = R_1$ and $R_2 = L_1 \oplus f(K, R_1)$. Switch $L_2$ and $R_2$ to get $R_2 L_2$.
Now put these into the encryption machine. After one round, we obtain:
On the left: $L_2 = R_1$.
On the right: $R_2 \oplus f(K, L_2) = (L_1 \oplus f(K, R_1)) \oplus f(K, R_1) = L_1$.
Therefore, one round yields $R_1 L_1$.
The same reasoning shows that the second round yields $R_0 L_0$. Now switch left and right to obtain $L_0 R_0$.

6. (a) Choose any quadratic polynomial with the secret 2 as the constant term. For example, let’s choose $f(x) = 2 + x^2$. Give A the point $(1, f(1)) = (1, 3)$, give B the point $(2, 6)$, give C the point $(3, 11) \equiv (3, 4)$ and give D the point $(4, 18) \equiv (4, 4)$.
(b) Knowing only your share, you cannot eliminate any secrets, so all of them are still possible. Therefore, there are $p = 7919$ secrets.