1. (a) The line through $A$ and $B$ has slope 4. The line through $A$ and $C$ has slope $-1$. Therefore, the three points are not on the same line, so at least one must be incorrect.

(b) The line through $A$ and $C$ has slope $-1$, so it has equation $y \equiv -(x - 1) + 5 \equiv -x + 6 \pmod{11}$. The secret is the constant term, which is 6.

2. (a) There are round keys $K_1, \ldots, K_{16}$. Since $K$ is all 1s, each $K_i$ is all 1s. To decrypt, use the keys in reverse order: $K_{16}, \ldots, K_1$. Since all the keys are the same, this is the same as encryption.

(b) A birthday attack (with lists of length about $2^{28}$) will find two inputs $x_1$ and $x_2$ such that the rightmost 56 bits of $H(x_1)$ are the same as those for $H(x_2)$. This means that the keys $K_1, K_2$ for the second step are the same, so the outputs of Nelson’s hash are the same. Another way is to use a birthday attack with lists of length $2^{32}$ on the 64-bit output of $H_1$. A third way is to use a brute force search in place of these birthday attacks. This is possible on current large computers.

(c) Since $\alpha x \equiv \alpha x + p - 1 \pmod{p}$, we have $H_2(x) = H_2(x + p - 1)$. Therefore, $H_2$ is not collision free.

3. (a) $\alpha^{m_1} \equiv \beta^{r_1} r_1^{s_1} \equiv (\alpha^a)^{r_1} (\alpha^{-1} \beta)^{-r_1} \equiv \alpha^{ar_1} \alpha^{-1} \beta^{-1} \equiv \alpha^{r_1}$. Therefore, the message is $m_1 = r_1$.

(b) Let $H$ be the hash function. Sign $H(m)$ instead of $m$. Then Eve needs to find $m$ such that $H(m) = r_1$. This is very hard since $H$ is preimage resistant.

4. Victor sends Peggy $i, j \in \{1, 2, 3\}$. Peggy sends $r_i$ and $r_j$. Victor checks that $r_i^2 \equiv x_i$ and $r_j^2 \equiv x_j$. They repeat 5 times (with new $r_1, r_2, r_3$). The probability of Peggy successfully lying on a given round is 1/3, so after 5 rounds the probability is $(1/3)^5 < .01$.

Another possibility is for Victor to ask for only one $r_i$. Then Peggy has 2/3 probability of successfully cheating, so there should be 12 repetitions: $(2/3)^{12} < .01$.

5. (a) The first list is $c \cdot E_k(x)^{-1} \pmod{p}$ for random values of $x$. The second list is $E_k(y)$ for random values of $y$. If both lists have length approximately $\sqrt{p}$, then we expect a match. If $c \cdot E_k(x)^{-1} \equiv E_k(y)$, then

$$c \equiv E_k(x) E_k(y) \equiv x^k y^k \equiv (xy)^k \pmod{p}.$$ 

Therefore, the message is probably $m \equiv xy \pmod{p}$.

(b) $79 \equiv 2^{5431 - 10000} \equiv 2^{-4569} \pmod{p}$. Since $2^{12346} \equiv 1 \pmod{12347}$, we have

$$79 \equiv 2^{-4569} 2^{12346} \equiv 2^{7777}.$$ 

Therefore, $k = 7777$. 