MATH/CMSC 456 (Washington) Exam 2 Solutions December 4, 2015

1. (20 points = 10+10) **(a)** H has collisions because $H(x+p) = H(x)$. But H is preimage resistant: Given y, it is hard to find any z with $h(z) = y$. In particular, it is hard to find z with $0 \le z < p$ with $h(z) = y$.
(b) The line through the points is $y \equiv 3x - 1$. We need to solve $(3x-1)^2 \equiv x^3 + 3x$, which can be changed to $x^3 - 9x^2 + \cdots \equiv 0$. Then 9 is the sum of the roots: $9 \equiv 1 + 2 + x$, so $x = 6$. Then $y \equiv 3x - 1 \equiv 6$. Reflect across the x-axis to get $(6, -6)$, or $(6, 5)$.

2. (20 points = 10+10) **(a)** Peggy chooses any two values of r_1 and r_2, computes $y_1 \equiv g^{r_1}$ and $y_2 \equiv g^{r_2}$. Then she follows the given procedure.
(b) Between 2 and 3, Victor needs to check that $y_1 y_2 \equiv h$.

3. (25 points = 10+10+5) **(a)** There are $N = 2^{100} \approx 10^{30}$ "birthdays" and $r = 10^{10}$ people. The probability of a match is approximately $1 - e^{-r^2/2N} \approx 1 - e^{-5\times 10^{-11}} \approx 0.00$.
(b) Eve makes two lists: (1) $D_{L_1}(D_{L_1}(c))$ for all keys L_1, (2) $E_{L_2}(E_{L_2}(m))$ for all keys L_2. A match yields a desired pair (L_1, L_2). (A birthday attack could be used to make the lists shorter.)
(c) For these two choices of keys for DES (but not for most cryptosystems), encryption and decryption are the same, so $E_{K_2}(E_{K_2}(m)) = m$ and similarly for K_1. Therefore, the ciphertext equals the plaintext, so Eve doesn't need any attack to read future messages.

4. (35 points = 10+10+5+10) **(a)** $h^m r^r \equiv g^{am} g^{kr} \equiv g^{am+kr} \equiv g^s$.
(b) Eve needs to solve $g^{s_1} \equiv h^{m_1} 2015^{2015} \pmod{p}$. This is a discrete log problem, therefore probably hard. (*Note:* Eve does not need to produce s_1 by the formula, so the fact she does not know k and a is not necessarily relevant. She only needs to find s_1 that satisfies the verification equation.)
(c) $s \equiv aH(m) + kr$, $g^s \equiv h^{H(m)} r^r$.
(d) $R = kP = (x, y)$, and $s \equiv am + kx \pmod{n}$, where n is the number of points on E; Verification: $sP = mQ + xR$.