MATH/CMSC 456 (Washington) Exam 2 Solutions May 5, 2015

1. (15 points = 5+5+5) **(a)** $b^{10} \equiv (14^{p-1})^3 \equiv 1^3 \equiv 1 \pmod{p}$ by Fermat.
(b) Since 14 is a primitive root, the smallest positive exponent that yields 1 is $p-1$, and $3(p-1)/10 < p-1$.
(c) $H(x+p-1) = H(x)$, so it is easy to find collisions, so H is not collision-free. Given y, solving $H(x) = y$ is a discrete log problem, which is hard. So H is preimage resistant.
2. (20 points = 10+10) **(a)** Eve chooses a pair (m, c) and makes two lists:
I. $D_{L_2}(D_{L_1}(c))$ for all keys L_1, L_2; **II.** $E_{L_3}(E_{L_4}(m))$ for all keys L_3, L_4.
She records all matches. For each (L_1, L_2, L_3, L_4) that gives a match, try with another (m, c). If more than one set survives this round, try with another (m, c). This probably gives the correct keys.
(b) The first round yields $L_1 = M$ and $R_1 = M \oplus (M \oplus K) = K$. The second round yields $L_2 = K$ and $R_2 = M \oplus (K \oplus K) = M$. Therefore, the left half of the ciphertext is the key and the right half is M. Very convenient for Eve!

3. (30 points = 5+5+5+5+5+5) **(a)** Since s goes in the exponent, it should be defined by a congruence mod $p-1$, so $X = p-1$.
(b) $h^r r^m \equiv (g^a)^r (g^k)^m \equiv g^{ar+km} \equiv g^s$.
(c) Eve needs to find s such that g^s is congruent to a known quantity mod p. This is a discrete log problem, and therefore probably hard.
(d) $h^r r^m \equiv h^r h^m g^m \equiv h^{r+m} = h^{p-1} g^m \equiv g^m \equiv g^s$.
(e) $r \equiv g^k$ and $s \equiv ar + k\,H(m) \pmod{p-1}$. To verify: $g^s \equiv h^r r^{H(m)} \pmod{p}$.
(f) The method of part (c) requires $H(m) = p - 1 - r$. Since H is preimage resistant, it is hard to find such an m.

4. (20 points = 10+10) **(a)** The line through (4,2) and (5,12) is $y = 10x - 38$ (or $10x + 1$ mod 13). Intersect: $(10x+1)^2 \equiv x^3 + x + 7$, so $0 \equiv x^3 - 100x^2 + \cdots$. The sum of the roots is $100 \equiv 4 + 5 + x$, so $x \equiv 0$. The y-coordinate is $10x + 1 \equiv 1$. Reflect to get $(0, -1)$, or $(0, 12)$.
(b) Make two lists of length at least $\sqrt{N} \approx 1000$:
I. iP for random values of i; **II.** $Q - jP$ for random values of j.
You expect a match, which yields $Q = (i+j)P$.

5. (15 points = 5+5+5) **(a)** Victor checks that $c_i \equiv r_i^e$. They repeat this procedure several times (with a new r_1 each time).
(b) Choose r_2 and compute $c_2 \equiv r_2^e \pmod{n}$. Then let $c_1 \equiv c c_2^{-1} \pmod{n}$.
(c) Choose r_1 randomly and then let $r_2 \equiv m r_1^{-1} \pmod{n}$.