MATH/CMSC 456 (Washington) Exam 2 Solutions April 29, 2010

1. (20 points = 5+5+10) (a) The powers of 3 mod 7 are 1, 3, 2, 6, 4, 5. This gives all nonzero congruence classes.
(b) The powers of 2 mod 7 are 1, 2, 4. This misses 3, 5, 6. Therefore, 2 is not a primitive root for 7.
(c) Divide $3^6 \equiv 2^2 \cdot 11 \pmod{137}$ by the square of $3^{10} \equiv 2 \pmod{137}$. This yields $11 \equiv 3^{6-20} \equiv 3^{-14} \pmod{137}$. (Therefore, any $x \equiv -14 \pmod{136}$ works.)

2. (20 points = 15 + 5) (a) Step 4: Victor checks that $h_1h_2h_3 \equiv \beta \pmod{p}$. Step 5: Victor checks that $h_i \equiv \alpha^{r_i}$ and $h_j \equiv \alpha^{r_j} \pmod{p}$. Step 6: They do Steps 1 through 5 at least 5 times (Since there is 1/3 probability that Peggy guesses which r is not asked for, Peggy has 1/3 chance of being lucky at any step, and $(1/3)^5 < .01$).
(b) Choose r_1 and r_2 randomly and then let $r_3 \equiv a - r_1 - r_2 \pmod{p-1}$.

3. (20 points) Suppose we are given y and want to find x such that $H(x) = y$. Probably the only way to try to do this is first to find z such that $H_2(z) = y$ and then find x such that $H_1(x) = z$. Since H_2 is strong, the first step should be impossible, and the second step is also probably impossible. Brute force would take around 2^{60} computations, so cannot be done. Therefore, H is probably preimage resistant.

To find collisions, make a list of around 2^{30} values of H_1. The birthday paradox says that we should expect a collision: $H_1(x_1) = H_2(x_2)$. Then $H(x_1) = H_2(H_1(x_1)) = H_2(H_1(x_2)) = H(x_2)$, so we have a collision for H.

4. (20 points = 6+7+7) (a) If $k = 1$, then Eve recognizes this because $r = \alpha$. Eve then knows that $s \equiv m - ar$, so $ar \equiv m - s \pmod{p-1}$. This can be solved for a, where there might be more than one solution. Trying these possible values of a until $\alpha^a \equiv \beta \pmod{p}$ should yield the correct value of a and therefore break the system.
(b) We need $\beta^r(\alpha\beta)^s \equiv \alpha^{-r}$. It is easy to see that $s \equiv -r \pmod{p-1}$ works.
(c) $r \equiv \alpha\beta \pmod{p}$. To work in the exponent, we need a congruence mod $p - 1$.
(d) We need to find m with $H(m) \equiv -r \pmod{p-1}$. Since H should be preimage resistant, this should be hard to do.

5. (20 points = 10 + 10) (a)

$$(1 - \frac{1}{12})(1 - \frac{2}{12})(1 - \frac{3}{12})(1 - \frac{4}{12}).$$

The approximation is $e^{-25/24}$.
(b) Preimage resistant since it is hard to find square roots mod n. It is easy to find Collisions: $H(n - x) = H(x) = H(x + n) = \cdots$.