Math/Cmsc 456, Jeffrey Adams

Test I, March 28, 2008 SOLUTIONS

For full credit you must show your work.

1. $E_{a,b}(E_{c,d})(x) = E_{a,b}(cx+d) = a(cx+d)+b = (ac)x+(ad+b)$ (all (mod 26)) so $e = ac \pmod{26}$ and $f = ad+b \pmod{26}$.

2. By the basic principle $(11144-9663, 30815167)$ is a proper divisor of $= 30815167$. In fact $30815167 = (11144-9663)(1114+9663) = 1481 * 20807$, and both factors are prime.

3. Since $39 = 3*13$, by the Chinese Remainder Theorem this is equivalent to the two equations

$$x^2 \equiv 1 \mod (3)$$
$$x^2 \equiv 1 \mod (13)$$

   Each equation has two solutions $x = \pm 1$, i.e. $x \equiv \pm 1 \mod (3)$ and $x \equiv \pm 1 \mod (13)$.

   To find simultaneous solutions to the equation $\mod (39)$ we take $x = \pm 1 \mod (3)$ and $x = \pm 1 \mod (13)$. There are 4 cases, or two cases $\pm a, \pm b$. Obviously ± 1 are solutions. We need to find one more. To do this, solve

$$x \equiv 1 \mod (3)$$
$$x \equiv -1 \mod (13)$$

   This has solution $x \equiv 25 \mod (39)$. The four solutions are thus $\pm 1, \pm 25 \pmod{39}$ or $1, 14, 25, 38 \pmod{39}$.

4. Take the equation $3^x = 65,281$. Since $65,281^2 = -1 \pmod{p}$, square both sides to get get $3^{2x} = -1$. Square again to get $3^{4x} = 1$. Therefore, since 3 is a primitive root, $p-1$ divides $4x$. Therefore $4x = k(p-1)$, and $x = \frac{k(p-1)}{4}$. The four distinct possibilities $\mod (p-1)$ are therefore $p-1, \frac{p-1}{4}, \frac{2(p-1)}{4} = \frac{p-1}{2}, \frac{3(p-1)}{4}$.

   Obviously $p-1$ isn't correct, since $3^{p-1} = 1$. Also $3^{\frac{p-1}{2}} = -1$, so this isn't correct either. The two reasonable possible solutions are $x = \frac{p-1}{4}$ and $x = \frac{3(p-1)}{4}$. In fact $x = \frac{p-1}{4}$.

   Another way to do this is by Pollig-Hellman. Note that $p-1 = 2^{16}$, so we only have to work $\mod (2)$. Write $x = x_0 + 2x_1 + 4x_2 + \ldots$. Since $\beta^2 = 1$, $\beta^{(p-1)/2^k} = 1$ for $k = 0, 1, \ldots, 14$. This says that $x_0 = x_1 = \ldots x_{13} = 0$, and $x_{14} = 1$. That is $x = 2^{14} = \frac{p-1}{4}$.

5. From the description we have $m^{e*e} = m \mod (n)$. But of course $m^{e*d} = m \mod (n)$ where d is the decryption key. Apparently $d = e$. Since d is defined by $e * d \equiv 1 \mod \phi(n)$, it must be that $e^2 \equiv 1 \mod (\phi(n))$. This is indeed the case.

   Since $e = d$ the same thing will hold for any message. That is 49693658 encrypted twice will give back 49693658.

6. Since Eve knows both e and f she can use the Euclidean algorithm to find x, y so that $xe + yf = 1$. Then $m^{xe+yf} = m^1 = m$, i.e. $(m^e)^x(m^f)^y = m$. Since Eve has x,y, m^e and m^f she can compute $(m^e)^x(m^f)^y = m$.

7. After one round we have

$$\begin{aligned} L_1 &= R_0 \\ R_1 &= L_0 \oplus R_0 \end{aligned}$$

   Then

$$\begin{aligned} L_2 &= R_1 = L_0 \oplus R_0 \\ R_2 &= L_1 \oplus R_1 = R_0 \oplus (L_0 \oplus R_0) = L_0 \end{aligned}$$

   The next step is

$$\begin{aligned} L_3 &= R_2 = L_0 \\ R_3 &= L_2 \oplus R_2 = (L_0 \oplus R_0) \oplus L_0 = R_0 \end{aligned}$$

   so we're done, and $n = 3$.