MATH/CMSC 456 (Washington) Exam 1 Solutions 3/10/2005

1. (a) The inverse of 5 (mod 39) is 8. Therefore, $x \equiv 5^{-1}(y-2) \equiv 8(y-2) \equiv 8y+23 \pmod{39}$ is the decryption function.
(b) Any two letters differing by 3 positions will work. For example, a and d both encrypt to C.

2. BABABAAABA. (a) Displace by 1 and get 2 matches. Displace by 2 and get 6 matches. Displace by 3 and get 2 matches. Therefore, 2 is the most likely key length.
(b) Look at the 1st, 3rd, 5th, 7th, 9th letters: $BBBAB$. Since b is most common in the plaintext, these are probably unshifted, so the first key letter is a. Now look at the 2nd, 4th, 6th, 8th, 10th letters: $AAAAA$. These are probably shifted from b's, so the second key letter is probably b. The decrypted message is *bbbbbbabbb*.

3. Letting $n = 1$ yields $1 \equiv c_0 \cdot 0 + c_1 \cdot 1 + 2$, so $c_1 \equiv -1 \equiv 4$. Letting $n = 2$ yields $0 \equiv c_0 \cdot 1 + c_1 \cdot 1 + 2 \equiv c_0 - 1 + 2$, so $c_1 \equiv -1 \equiv 4$.

4. Write $ed = 1 + 958230k$. Then $c^d \equiv m^{ed} \equiv m(m^{958230})^k \pmod{n}$. Since $m^{958230} \equiv 1 \pmod{n}$ by assumption, we get $m(1)^k \equiv m \pmod{n}$.

5. $(x_1x_3x_4)^2 \equiv (2 \cdot 3^5 \cdot 7)^2 \pmod{n}$. Compute $\gcd(x_1x_3x_4 - 2 \cdot 3^5 \cdot 7, n)$. If $x_1x_3x_4 \not\equiv \pm 2 \cdot 3^5 \cdot 7 \pmod{n}$, then this yields a nontrivial factor of n. It fails if $x_1x_3x_4 \equiv \pm 2 \cdot 3^5 \cdot 7 \pmod{n}$.

6. Compute $2^{n-1} \pmod{n}$. If this is not 1, then n is composite, by Fermat's theorem. If it is 1, then n is probably prime.