Math/Cmsc 456, Jeffrey Adams
Test I, March 28, 2008
For full credit you must show your work.
Calculators allowed but not required

1. [10 points] Consider the affine ciphers \( E_{a,b}(x) = ax + b \mod 26 \). Given \( a, b, c, d \) with \((a, 26) = (c, 26) = 1\) find \( e, f \) so that \( E_{a,b}(E_{c,d}(x)) = E_{e,f}(x) \).

2. [15] We want to factor \( n = 30, 815, 167 \). We notice that
\[ 11144^2 = 9663^2 \mod n \]
Use this information to factor \( n \). It is enough to find an expression for a factor of \( n \) as a GCD.

3. [15] Find all solutions to \( x^2 \equiv 1 \mod 39 \).

4. [15] Let \( p = 65, 537 \). Note that 3 is a primitive root \( \mod p \). Let \( \beta = 65, 281 \). We compute \( \beta^2 = -1 \mod p \). We want to compute \( L_3(65, 281) \), i.e. solve \( 3^x = 65, 281 \mod p \).

Based on this information, find 2 possible candidates for \( L_3(65, 281) \). (This can be done with only a small computation. Recall \( L_3(p) \) is defined \( \mod p - 1 \).)

5. [15 points] Alice uses RSA with \( p = 7919, q = 17389 \) and \( e = 66909025 \). She decides to encrypt twice (she thinks) for extra security: she encrypts the message \( m = 3748976597 \) to get \( c \), and then encrypts \( c \), and the result is \( m \) again. Explain why this happened. What will happen if she encrypts \( m = 49693658 \) twice? Obviously you can do this without calculation.

See other side
6. [15] Suppose Alice and Bob have the same RSA modulus $n$ with different encryption exponents $e$ and $f$. Assume $e$ and $f$ are relatively prime. Suppose Charles sends a message $m$ to both Alice and Bob, i.e. he sends the ciphertexts $m^e \pmod{n}$ and $m^f \pmod{n}$. Suppose Eve intercepts both messages. You may also assume Eve knows the encryption method being used, $n$, $e$ and $f$. Show that Eve can find $m$. Hint: find $x, y$ so that $xe + yf = 1$.

7. [15] Consider the following Feistel system. The message $M$ has 8 bits. We split it into $M = L_0R_0$ where $L_0, R_0$ each have 4 bits. At each round $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus R_{i-1}$ (where $\oplus$ is bitwise addition, i.e. XOR).

The Feistel system repeats after $n$ steps for some $n$, i.e. $L_n = L_0$, and $R_n = R_0$. Find $n$ and compute $L_1, R_1$, and $L_2, R_2$, ... $L_n, R_n$ in terms of $L_0, R_0$. 