1. (25 points = 10+15) (a) Eve thinks she knows how to break Bob’s RSA. Bob is using a 300-digit modulus $n$ and encryption exponent $e = 65537$. Eve says she will encrypt every possible plaintext and store all the plaintexts along with their encryptions. Why won’t this strategy work? 

(b) Bob sets up his RSA system with 200-digit primes $p$ and $q$, so he has modulus $n = pq$ and encryption exponent $e$. He tests his system by choosing a message $m$ that he encrypts to get $c \equiv m^e \pmod{n}$. He posts $c$ on his web page. Alice tells him that this method of encryption is not secure and that he should pad the plaintext with some random bits. Therefore, he chooses a random 10-digit number $r$ and lets $m_1 = m + rp$. He encrypts $m_1$ to get $c_1 \equiv m_1^e \pmod{n}$ and puts $c_1$ on his web page. Eve sees both $c$ and $c_1$ and hears Bob describe his “improved” encryption method. How does Eve use this information to factor $n$? 

2. (20 points = 5+5+10) (a) Alice encrypts a message $m$ consisting of 6 randomly chosen letters. She uses the Vigenère cipher with key length 3. Compute the conditional probability $\text{Prob}(m = \text{abcdef} \mid c = \text{zzzzzz})$.

(b) Alice encrypts a message $m$ consisting of 6 randomly chosen letters. This time she uses a one-time pad. Compute the conditional probability $\text{Prob}(m = \text{abcdef} \mid c = \text{zzzzzz})$.

(c) Bob sets up his RSA system with public key $(n, e)$ and private key $d$. But he makes a big mistake. He takes a message $m$, encrypts it as $c \equiv m^d \pmod{n}$, and send $c$ to Alice. Eve knows $n$ and $e$ but doesn’t know $d$, and she intercepts $c$. She also hears about Bob’s mistake. How can Eve determine the message $m$?

3. (30 points = 15+15) (a) Bob sets up his RSA cryptosystem with $n = 4369$ and $e = 881$. Alice encrypts the message $m = 1798$ but accidentally computes $m^8 \pmod{n}$ instead of $m^{881}$. She discovers that $m^8 \equiv 1 \pmod{n}$. Looking back at her calculations, she sees that $m^2 \equiv 4113, \quad m^4 \equiv 1, \quad m^8 \equiv 1 \pmod{n}$.

Use this information to factor $n$. (You must use this information. You must produce actual numbers $p$ and $q$ such that $n = pq$.) 

(b) Suppose that Alice had computed $c \equiv m^{881} \pmod{n}$ to encrypt $m$ in part (a). What would the ciphertext $c$ be?

4. (25 points = 10+15) (a) An LFSR uses a recurrence relation of length 3 to output the sequence $011101001$. 

Find the recurrence relation that is used to generate this sequence. 

(b) The ciphertext $C XD$ was encrypted by the affine function $9x + 1 \mod{26}$. Find the plaintext.