1. (25 points = 5+10+10) Alice invents her own cipher: She writes all the letters in the plaintext as numbers mod 26 in the standard way (with $a = 0$ and $z = 25$) and she chooses integers $b$, $c$, and $d$. She then alternates the shift by $b$ with the affine function $cx + d$. That is, she shifts the 1st, 3rd, 5th, etc. letters of the plaintext by $d$ and applies the affine function $cx + d$ mod 26 to the 2nd, 4th, 6th, etc. letters.

(a) What condition does $c$ need to satisfy for Bob (who knows the key) to be able to decipher the message?

(b) Describe a chosen plaintext attack that will yield the key $(b, c, d)$. You know the encryption method, but not $b, c, d$. You must explicitly say what plaintexts you use.

(c) Suppose you intercept the ciphertext $JNNIQ$ and know that the plaintext is $HELLO$. Determine the values $b, c, d$. 

\[a \ b \ c \ d \ e \ f \ g \ h \ i \ j \ k \ l \ m \ n \ o \ p \ q \ r \ s \ t \ u \ v \ w \ x \ y \ z\]

\[0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20 \ 21 \ 22 \ 23 \ 24 \ 25\]
2. (15 points = 10+5) Alice needs to send a 6-digit number $m$ to Bob, so Bob chooses the usual RSA numbers $n, e, d$, and sends $n$ and $e$ to Alice. Alice computes $c \equiv m^e \pmod{n}$ and sends $c$ to Bob.
(a) Eve intercepts $c$ and knows $n$ and $e$. Moreover, Eve knows that $m$ is a 6-digit number. Describe a method by which Eve can obtain $m$ (there is more than one possible way).
(b) What can Alice do to prevent Eve from obtaining $m$?

(a) Eve encrypts each $m < 10^6$
and sees what matches $c$

(b) Alice adds 100 random bits onto the end of $m$. 


3. (25 points = 5+10+10) (a) Eve thinks that she has a great strategy for breaking RSA that uses a modulus \( n \) that is the product of two 300-digit primes. She decides to make a list of all 300-digit primes and then divide each of them into \( n \) until she factors \( n \). Why won't this strategy work?

(b) Suppose you know that \( 709^2 \equiv 1 \mod 4189 \). Use this information to factor 4189 (you must use this information; answers that do not use 709 will not receive credit).

(c) You are auditioning for the Factoring Superstars Show. You are told that exactly one of the following numbers is prime:

\[
10^{500} + 247, \quad 10^{500} + 651, \quad 10^{500} + 961.
\]

You have one minute to decide which one. You have access to a laptop and Mathematica, MATLAB, or whatever your favorite software is. But the factoring programs have been disabled. Describe the calculations you can do to have a very good chance of winning.

(a) There are more than \( 10^{297} \) such primes, many more than the number of particles in the universe, so Eve can't store the primes, even if she could compute them (which she probably can't).

(b) \( 709^2 \equiv 1 \mod 4189 \), \( 709 \not\equiv 1 \mod 4189 \):

\[
\text{Compute } \gcd(709-1, 4189) = 4189/59 = 59.71.
\]

(c) Compute \( 2^{n-1} \equiv \ ? \mod n \) for each \( n \).

If \( ? \not\equiv 1 \), then \( n \) is not prime.

If \( ? \equiv 1 \), then \( n \) is probably prime.
4. (25 points = 10+10+5) (a) The LFSR sequence 10011001... is generated by a recurrence relation of length three: \( x_{n+3} \equiv c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2} \pmod{2} \). Find the coefficients \( c_0, c_1, c_2 \).

(b) In RSA, suppose \( n = 187(=11 \cdot 17) \) and \( e = 13 \). Find the decryption exponent \( d \). (Hint: If you get \( d = 72 \), try again.)

(c) Alice uses encryption exponent \( e = 67 \) for RSA, so she needs to compute \( m^{67} \pmod{n} \). Describe how she can do this computation using at most 10 multiplications mod \( n \).

\[
\begin{align*}
(a) & \quad 10011001 \\
 1 & \quad 5 \\
 2 & \quad 8 \\
\end{align*}
\]

\[ n=1: 1 \equiv c_0 + c_1 + c_2 \Rightarrow c_0 = 1 \]

\[ n=2: 1 \equiv 0c_0 + c_1 + c_2 \Rightarrow c_2 = 1 \]

\[ n=3: 0 \equiv 0c_0 + 1c_1 + c_2 \Rightarrow c_1 = 1 \]

\[
\begin{align*}
(b) & \quad ed \equiv 1 \pmod{(p-1)(q-1)} \\
 & \quad 13d \equiv 1 \pmod{160} \\
Use Extended Euclidean: & \\
160 & \quad 1 \quad 0 \\
13 & \quad 0 \quad 1 \\
4 & \quad 1 \quad -12 \\
1 & \quad -3 \quad 37 \Rightarrow l = -3(160) + 37(13) \\
& \Rightarrow 37 \cdot 13 \equiv 1 \pmod{160} \\
& \Rightarrow d = 37 \\
\end{align*}
\]

\[
\begin{align*}
(c) & \quad m \\
m^2 & \quad m^2 \\
m^4 \equiv (m^2)^2 & \quad 1 \\
m^8 \equiv (m^4)^2 & \quad 2 \\
m^{16} \equiv (m^8)^2 & \quad 4 \\
m^{32} \equiv (m^{16})^2 & \quad 5 \\
m^{64} \equiv (m^{32})^2 & \quad 6 \\
m^{67} & \equiv m^{64} \cdot m^2 \cdot m^1 \quad 7, 8 \\
\end{align*}
\]
5. (10 points = 5+5) Alice is learning about the Vigenère cipher. She chooses a random 6-letter word (so all 6-letter words in the dictionary have the same probability) and encrypts it using a Vigenère cipher with a randomly chosen key of length 3 (that is, each possible key has probability 1/26³). Eve intercepts the ciphertext fecnlgh.

(a) Compute the conditional probability \( P(M = \text{attack} \mid C = \text{fecnlgh}) \).

(b) Use your result from part (a) to show that the Vigenère cipher does not have perfect secrecy.

\[ P(M = \text{attack} \mid C = \text{fecnlgh}) = P(M = \text{attack}) > 0. \]

But perfect secrecy \( \Rightarrow P(M = \cdots \mid C = \cdots) = P(M = \cdots) \).