1. (25 points = 10+15) (a) There is not enough storage in the world to store $10^{300}$ ciphertexts since there are approximately $10^{85}$ particles in the universe. Also, Alice’s plan would take too much time.

(b) Since $m \equiv m_1 \pmod{p}$ but $m \not\equiv m_1 \pmod{q}$, the same holds for $c$ and $c_1$. Therefore, $\gcd(c-c_1, n) = p$.

2. (20 points = 5+5+10) (a) If the key has length 3 then the first three letters $zzz$ encrypt to the same as the second three letters. Therefore, it is impossible for $zzzzzz$ to encrypt to $abcdef$, so the conditional probability is 0.

(b) Since the one-time pad has perfect secrecy, $\Pr(m = abcefg \mid c = zzzzzzz) = \Pr(m = abcefg) = 1/26^6$.

(c) $c^e \equiv m^d \equiv m \pmod{n}$.

3. (30 points = 15+15) (a) $4113^2 \equiv 1^2 \pmod{n}$ and $4113 \not\equiv \pm1 \pmod{n}$. Compute $\gcd(4113 - 1, n) = 257$. Also, $n/257 = 17$.

(b) Since $m^8 \equiv 1$, we have $c \equiv m^{881} \equiv m \cdot (m^8)^{110} \equiv m \pmod{n}$. The ciphertext equals the plaintext.

4. (25 points = 10+15) (a) Solve the equation

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$  

The solution is $c_0 = c_2 = 1$, $c_1 = 0$.

(b) If $y \equiv 9x + 1$, then $3y \equiv x + 3$, so $x \equiv 3y - 3$ gives the decryption function. Therefore, $CXD = 2$, 23, 3 decrypts to $3, 14, 6 = DOG$.  
