1. (20 points = 5+5+5+5) (a) Shift cipher: Either decrypt the ciphertext by computing all 26 shifts of the ciphertext; or look at the first two letters of the ciphertext: the first is a shift of $S$ so you know what the shift is and the second can be a shift of only one of $I$ and $P$; or the ciphertext for $m_0$ has the 9th and 10th letters equal while for $m_1$ the 8th and 9th are equal; etc.

(b) Vigenère cipher with key length 4: Use the first four letters of the ciphertext to figure out what the key must be if the plaintext starts with SIXM. Then see if this key decrypts the ciphertext to $m_0$. If not, then the message was $m_1$.

(c) RSA: Encrypt $m_0$ and $m_1$ and see which yields the ciphertext.

(d) One-time pad: There is no way to decide since the one-time pad has perfect secrecy.

2. (20 points = 7+7+6) (a) Look at the 1st, 3rd, 5th, 7th, 9th letters: BCBBB. These are shifts by the same amount, so they are probably shifts by 1 of ABAAA. Look at the 2nd, 4th, 6th, 8th, 10th letters: CCCCC. They are probably shifts by 2 of AAAAA. Put these together: the plaintext is probably AABAAAAAAA.

(b) If $y \equiv 9x + 1$, then $x \equiv 9^{-1}(y - 1) \equiv 3y - 3$, so this is the decryption function. Since $JLH = 9, 11, 7$, this decrypts to 24, 4, 18 = YES.

(c) Use the plaintext BAAABAAAB. This corresponds to using the vectors $(1,0,0)$, $(0,1,0)$, $(0,0,1)$. The encryptions of these are the entries of the matrix.

3. (20 points = 10+10) (a) Letting $n = 1$ yields $1 \equiv c_0 + c_2$. Letting $n = 2$ yields $1 \equiv c_1 + c_2$. Letting $n = 3$ yields $0 \equiv c_0 + c_1 + c_2$. Subtracting the first and third yields $c_1 = 1$. The second then yields $c_2 = 0$, and then we get $c_0 = 1$.

(b) Since cat is not a shift of mxp, if the ciphertext is mxp then the plaintext cannot be cat, so $P(M = \text{cat} \mid C = \text{mxp}) = 0$. If there is perfect secrecy, this should equal $P(M = \text{cat})$, which is nonzero. Therefore, there is not perfect secrecy.

4. (20 points = 10+10) (a) Since $(p-1)(q-1) = 396$, we must solve $de \equiv 1 \pmod{396}$. Since $e = 397 \equiv 1 \pmod{396}$, we need to solve $d \equiv 1 \pmod{396}$, so $d = 1$. The plaintext is $123^d \equiv 123^1 = 123$.

(b) We need $de \equiv 1 \pmod{n-1}$ (by Fermat’s theorem). Therefore, we need to solve $13d \equiv 1 \pmod{131302}$. Use the Extended Euclidean Algorithm to write $1 = 131302(-6) + 13(60601)$. This says that $13(60601) \equiv 1 \pmod{n-1}$, so $d = 60601$ is the decryption exponent.

5. (20 points = 10+10) (a) By Fermat, $b^6 \equiv 1 \pmod{7}$, $b^{12} \equiv 1 \pmod{13}$, and $b^{18} \equiv 1 \pmod{19}$. Raise these to the powers 288, 144, and 96 to get $b^{1728} \equiv 1 \pmod{7, 13, 19}$. Therefore, $b^{1728} - 1$ is a multiple of 7, 13, and 19, so it is a multiple of $7 \cdot 13 \cdot 19 = 1729$. This means that $b^{1728} \equiv 1 \pmod{1729}$.

(b) We have $1065^2 \equiv 1^2 \pmod{1729}$. Compute gcd(1065 − 1, 1729) = 133, which is a nontrivial factor of 1729.