1. (15 points = 10+5) Victor designs a cryptosystem (called “Vector”) as follows: He writes the letters in the plaintext as numbers mod 26 (with a = 0, b = 1, etc.) and groups them five at a time into 5-dimensional vectors. His key is a 5-dimensional vector. The encryption is adding the key vector mod 26 to each plaintext vector (so this is a shift cipher with vectors in place of individual letters).
   (a) Describe a chosen plaintext attack on this system. You must give the explicit plaintext used and how you get the key from the information you obtain.
   (b) Victor’s system is not new. It is the same as what well-known system?

2. (20 points = 10+10)
   (a) You are told that exactly one of the numbers
   \[10^{100} + 267, \quad 10^{100} + 271, \quad 10^{100} + 273\]
   is prime and you have one minute to figure out which one. Describe calculations you could do (with software such as Matlab or Mathematica) that would give you a very good chance of figuring out which number is prime? Do not do the calculations. Do not try to factor the numbers. They do not have any prime factors less than 10^9. Your method does not need to be the best method, but it should be one that works quickly. You may not use commands of the form “IsPrime[n]” or “NextPrime[n].”
   (b) You are told that 7172^2 \equiv 60^2 \pmod{14351}. Use this information to factor 14351. You must use this information and you must give all steps of the computation (that is, give the steps you use if you are doing it completely without a calculator).

3. (25 points = 5+10+10) (a) You need to compute 12345678965537 \pmod{581859289607}. A friend offers to help: 1 cent for each multiplication mod 581859289607. Your friend is hoping to get more than $650. Describe how you can have the friend do the computation for less than 25 cents. (Note: 65537 = 2^{16} + 1 is the most commonly used RSA encryption exponent.)
   (b) Bob designs a very small RSA system, using p = 5, q = 11, e = 27. Alice sends Bob the ciphertext c = 48. What is the plaintext? (Hint: If you are not using a calculator, then the fact 48 \equiv -7 \pmod{55} can make the computations go faster.)
   (c) Bob’s RSA system uses n = 2776099 and e = 421. Alice encrypts the message 2718 and sends the ciphertext to Bob. Unfortunately (for Alice), 2718^{10} \equiv 1 \pmod{n}. Show
that Alice’s ciphertext is the same as the plaintext. (Do not factor n. Do not compute \(m^{421} \pmod{n}\) without using the extra information that \(2718^{10} \equiv 1\). Do not claim that \(\phi(2776099 = 10; it doesn’t.\)

4. (20 points = 8+7+5) (a) Suppose that you have a language with only the two letters A and B, and that they occur with frequencies .8, and .2, respectively. The following ciphertext was encrypted by the Vigenère method (shifts are mod 2, of course):

\[
BABABBBABABAAABAB.
\]

You are told that the key length is 1, 2, or 3. Decrypt the ciphertext.

(b) You encrypt messages using the affine function \(9x + 2 \pmod{26}\). Decrypt the ciphertext GM.

(c) You try to encrypt messages using the affine cipher \(4x + 1 \pmod{26}\). Find two letters that encrypt to the same ciphertext letter.

5. (20 points = 15 + 5)

(a) You encrypt the message zzzzzzzzzz (there are 10 z’s) using the following cryptosystems:

(i) affine cipher

(ii) Vigenère cipher with key length 7

(iii) Hill cipher with a \(2 \times 2\) matrix

Eve intercepts the ciphertexts. She knows the encryption methods (including key size) and knows what your plaintext is (she can hear you snoring). For each of the three cryptosystems, determine whether or not Eve can use this information to determine the key. Explain your answer.

(b) Suppose we build an LFSR-type machine that works mod 2. It uses a recurrence of length 2 of the form

\[
x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 1 \pmod{2}
\]

to generate the sequence 1,1,0,0,1,1,0,0. Find \(c_0\) and \(c_1\).