You may use calculators.

1. (10 points) Bob's RSA modulus is $979 = 11 \times 89$ and his encryption exponent is $e = 587$. Alice sends him the ciphertext $c = 10$. What is the plaintext?

2. (10 points) You want to find a 300-digit prime whose first nine digits are 123456789 (there are around 1.4×10^{288} of them). Describe a method that is very likely to yield such a prime. You are not allowed to use the command `nextprime`$(123456789 * 10^{291})$ or similar. Essentially, the problem is asking what you would do to write a `nextprime` function.

3. (10 points) Suppose a message m is chosen randomly from the set of all 5-letter English words and is encrypted using an affine cipher mod 26, where the key is chosen randomly from the 312 possible keys. The ciphertext is $HHGZC$. Compute the conditional probability
Prob$(m = HELLO \mid c = HHGZC)$. Use the result of this computation to determine whether of not affine ciphers have perfect secrecy.

4. (10 points) Suppose there is a language that has only the letters a and b. The frequency of the letter a is .1 and the frequency of b is .9. A message is encrypted using a Vigenère cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA. The key length is 1, 2, or 3.

(a) Show that the key length is probably 2.

(b) Using the information on the frequencies of the letters, determine the key and decrypt the message.

5. (10 points) The ciphertext 75 was obtained using RSA with $n = 437$ and $e = 3$. You know that the plaintext is either 8 or 9. Determine which it is without factoring n.

6. (10 points) Let p and q be distinct odd primes. A slight strengthening of Euler's theorem says that if $\gcd(b, pq) = 1$ then

$$b^{\frac{1}{2}(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

(You may assume this fact.) Suppose Bob chooses e and d so that $de \equiv 1 \pmod{\frac{1}{2}(p-1)(q-1)}$. Alice chooses a message m with $\gcd(m, pq) = 1$ and computes $c \equiv m^e \pmod{pq}$. Show that $c^d \equiv m \pmod{pq}$. Indicate explicitly how you are using this strengthening of Euler's theorem.

7. (10 points) Eve thinks that she has a great strategy for breaking Alice's RSA that uses a modulus n that is the product of two 300-digit primes. She decides to make a list of all messages of length at most 600-digits along with their encryptions. Then, whenever she intercepts a ciphertext from Alice, she looks up the ciphertext on her list and sees the corresponding plaintext. Why won't this strategy work?

8. (10 points) Suppose Alice has a block cipher with 2^{50} keys, Bob has one with 2^{40} keys, and Carla has one with 2^{30} keys. The only known way to break each system is by brute force, namely trying all keys. Alice uses her system with single encryption. Bob uses his with double encryption. Carla uses hers with triple encryption. Who has the most secure system? Who has the weakest? (Assume that double and triple encryption do not reduce to using fewer encryptions.) Explain your answers.

9. (10 points) Alice uses an affine cipher, but works mod 100 instead of mod 26. Her encryption function is $87x + 1 \pmod{100}$. What is the decryption function?

10. (10 points) 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). For example, if the plaintext is `HELLOTODAY` and the key is `(1,0,2,3,5)`, the encryption is

$$\texttt{(H, E, L, L, O)} + (1,0,2,3,5) = \texttt{(I, E, N, O, T)}$$

$$\texttt{(T, O, D, A, Y)} + (1,0,2,3,5) = \texttt{(U, O, F, D, D)}.$$

(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?

11. (10 points) There are 124 two-letter words that are allowed in certain word games. Of these, 7 of them consist of two consecutive letters: *AB, DE, EF, HI, NO, OP, ZA*. Alice chooses a two-letter word at random and encrypts using a shift cipher, obtaining a ciphertext c.
(a) What is the conditional probability Prob($m = HI \mid c = YZ$)?
(b) What is the conditional probability Prob($m = HI \mid c = BE$)?

12. (10 points) Eve loves to do double encryption. She starts with a message m. First, she encrypts it twice with a one-time pad (the same one each time). Then she encrypts the result twice using a Vigenère cipher with key $NANANA$. Finally, she encrypts twice with RSA using modulus $n = pq = 7919 \times 17389$ and exponent $e = 66909025$. It happens that $e^2 \equiv 1 \pmod{(p-1)(q-1)}$. Show that the final result of all this encryption is the original plaintext. Explain your answer fully. Simply saying something like "decryption is the same as encryption" is not enough. You must explain why.

13. (10 points) Suppose you use an affine cipher. The plaintext consists of two letters and the encryption function is $y \equiv 21x + 2 \pmod{26}$. The ciphertext is the first two letters of your last name (for me the ciphertext is WA). Find the plaintext.

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

14. (25 points = 10+10+5) **(a)** The LFSR sequence $10011001\cdots$ 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.

15. (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 $1/26^3$). Eve intercepts the ciphertext *fcmlgh*.
(a) Compute the conditional probability $P(M = attack \mid C = fcmlgh)$.
(b) Use your result from part (a) to show that the Vigenère cipher does not have perfect secrecy.

16. (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.

17. (20 points = 5+5+5+5) At the end of the semester, the professor randomly chooses and sends one of two possible messages:
$m_0 =$*YOUPASSED* and $m_1 =$*YOUFAILED*.
To add to the excitement, the professor encrypts the message using one of the following methods:
(a) Shift cipher
(b) Vigenère cipher with key length 3

(c) RSA with a public 300-digit modulus n and encryption exponent $e = 65537$ (the message is not padded with extra bits)
(d) One-time pad
You receive the ciphertext and want to decide (in less than one minute, but you have a computer) whether the professor sent m_0 or m_1. For each method (a), (b), (c), and (d), explain how to decide which message was sent or explain why this is impossible. (*Notes:* You may assume that you know which method is being used. For the Vigenère, do not use frequency analysis; the message is too short.)