Sample Problem:

Consider a situation in which you are seeking to decrypt ciphertext on $\mathbf{Z}_{26}$. Suppose there is a string of length 4 for which corresponding plaintext/ciphertext is known, as given below.

Ciphertext string:	R	M	L	R
Ciphertext Integer values in $\mathbf{Z}_{26}$:	17	12	11	17

Corresponding plaintext string:	A	R	K	A
Ciphertext Integer values in $\mathbf{Z}_{26}$:	0	17	10	0

For the purposes of part (a) and (b) of this problem, you may assume that the encryption function is known to be either a shift cipher or an affine cipher.

a) Is the encryption function a shift cipher?
If yes, provide the corresponding decryption function (specified as a function operating on integers in $\mathbf{Z}_{26}$), and describe your reasoning used to identify this encryption function.
If no, describe your reasoning in reaching this conclusion.

b) Is the encryption function an affine cipher?
If yes, provide the corresponding decryption function (specified as a function operating on integers in $\mathbf{Z}_{26}$), and describe your reasoning used to identify this encryption function.
If no, describe your reasoning in reaching this conclusion.

c) In parts (a) and (b), you were allowed to take as known information that the encryption function was either a shift cipher or an affine cipher, and therefore, you knew it belonged to the set of encryption functions we termed monoalphabetic ciphers.
Suppose you were NOT given the information that the encryption was known to be either shift or affine. based on this limited evidence of four characters, describe why it is ***more likely*** that the encryption is a monoalphabetic cipher.

Sample Problem:

The index of coincidence (IC) may be thought of as the ratio of two quantities, computed for a given message, with message length denoted by n.

a) Provide a short description interpreting the numerator term in the IC ratio, and the denominator term in the IC ratio.

b) The IC computation is typically used as a “building block” in computations to estimate a particular numeric parameter value, for a particular class of encryption function. What parameter is the IC typically used to help estimate, for what class of encryption functions?

c) For the plaintext message of length 14 below, compute the IC value. Decompose the numerator of the IC quantity as a sum of 8 terms, and compute the value of each term in the sum associated each distinct character in the message.

   plaintext = ‘DOGDAYSDIDDRAG’

Sample Problem:

Suppose we have a character set of nine letters from the Greek alphabet, and these characters have an associated probability distribution as shown below.

α (alpha)	β (beta)	λ (lambda)	ω (omega)	τ (tau)	ε (epsilon)	θ (theta)	σ (sigma)	π (pi)
0.1545	0.1718	0.0241	0.1732	0.1199	0.0185	0.0528	0.1037	0.1811

a) Compute the entropy value for the probability distribution given for these characters. Will this entropy value be greater than, less than or equal the entropy for a nine-element probability distribution in which all characters have equal probability? Briefly justify you answer regarding this inequality, based on the interpretation of entropy of character sets in the cryptographic context.

b) Suppose you were to construct a Huffman encoding for this character set. What is the shortest achievable average bit length you would expect (averaged over the nine characters, with the probabilities as given above)? Justify your conclusion based on the value for entropy you obtained in (a).

c) What character must be among the set of characters that get assigned the shortest bit length in the Huffman encoding? What character must be among the set of characters that get assigned the longest bit length in the Huffman encoding?

d) Suppose we modified the probability distribution above, and in the new distribution the epsilon character had probability zero (0.0000), while all other characters had non-zero probabilities. Describe how the epsilon character would be treated in a Huffman encoding scheme.

Sample Problem:

Suppose we wish to produce a pseudo-random sequence using the Linear Feedback Shift Register approach. The specific LFSR has order n=3, and coefficients $c_2=1$, $c_1=0$, $c_0=1$.

a) Staring from initial sequence values $x_0=1$, $x_1=1$, $x_2=1$, compute the sequence values through iteration x_9,; that is, compute x_3, x_4, x_5, x_6, x_7, x_8, x_9.
b) Repeat the same computation of (a) again, but for the different initialization of $x_0=0$, $x_1=1$, $x_2=0$.
c) Based on your results of (a) and (b), would you judge that the associated characteristic polynomial f(X)=1 + X^2 +X^3 to be a primitive polynomial on $\mathbf{Z}_2$? Justify your conclusion.