CS 355, Fall, 2019, Homework 2

1. Let the 26 letters have the numerical values A = 0, B = 1, ..., Z = 25. Write plaintext as $M = m_0 m_1 \ldots$ and ciphertext as $C = c_0 c_1 \ldots$, where the m_i and c_i are letters of the alphabet. Recall that the Vigenère cipher (after Blaise de Vigenère) with key word $K = k_0 k_1 \ldots k_{t-1}$ enciphers m_i with the formula

$$c_i = (m_i + k_{(i \bmod t)}) \bmod 26$$

and deciphers c_i with the formula $m_i = (c_i - k_{(i \bmod t)}) \bmod 26$.

The Beaufort cipher (after English Admiral Sir Francis Beaufort, but invented earlier by Giovanni Sestri) is similar to the Vigenère cipher in that it has a key word of length t letters. The Beaufort cipher enciphers the i-th plaintext letter m_i with the formula $c_i = (k_{(i \bmod t)} - m_i) \bmod 26$.

a. Encipher the plaintext ATTACKATDAWN using the Beaufort cipher with key word KEY.

b. Write the formula used by the Beaufort cipher to decipher the i-th ciphertext letter c_i.

2. Suppose a Kasiski analysis identifies these six pairs of repeated sequences in the ciphertext of a Vigenère cipher:

Location of start of						
first occurrence	10	21	37	49	58	72
second occurrence	34	65	109	105	162	132

Assume that at most one or two pairs of repeated ciphertext are just coincidences, but that the other four or five pairs come from repeated plaintext. What can you conclude about the length t of the key word used to encrypt the message? Explain your answer.

3. One hundred characters of ciphertext from a suspected Beaufort cipher were intercepted by one of your agents. Here is the frequency distribution of the letters of the alphabet in this sample of ciphertext:

A	B	C	D	E	F	G	H	I	J	K	L	M
2	10	2	5	3	8	1	2	2	5	1	3	1

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	10	1	8	1	8	5	2	1	3	5	1	8

In other words, there are two As, ten Bs, etc., in the ciphertext.

a. Compute the Index of Coincidence IC for this sample.

b. What can you conclude about the length d of the key word used to encrypt the message? Explain your answer.

4. A message is enciphered using a product cipher that consists of one Hill cipher followed by (composed with) another Hill cipher. Each of these Hill ciphers uses a 4×4 matrix that is invertible modulo 26.

a. Use a theorem from linear algebra to explain why the product cipher has a well defined inverse (deciphering) function.

b. Is the product cipher more secure, less secure or just as secure as a single Hill cipher? Justify your answer.