Math 3C43, Solutions to Assignment #1

Chap. 2 #10: We compare the shifted (or translated) ciphertext to itself for different values of k counting matches. Since the ciphertext is short (10 characters), I wrapped the ciphertext for comparison. Here is a little table:

k	B A B A B A A A B A	Matches.
1	× × × × × × ✓ ✓ × ×	2
2	✓ ✓ ✓ ✓ ✓ ✓ × ✓ × ✓	8
3	× × × × × × ✓ × × ✓	2
4	× ✓ ✓ ✓ ✓ ✓ × ✓ ✓ ✓	8

✓ means the character matches the one k spots before it and × means it doesn't (remember I am wrapping the ciphertext).

Given the frequency counts for this two-letter alphabet are $(.1, .9)$ for a and b respectively we expect a match about $(.1, .9) \cdot (.1, .9) = .82$ or 82% of the time if we are using the correct key length. For a 10 letter ciphertext then we expect 8.2 matches. So $k = 2$ looks to be the key length.

To determine the key, look for the most frequent letter in the $1^{st}, 3^{rd}, 5^{th}, 7^{th}, 9^{th}$ spot: B B B A B $\rightsquigarrow$ so B is likely b.
and $2^{nd}, 4^{th}, 6^{th} \ldots$ spot: A A A A A $\rightsquigarrow$ so A is likely b.

The key is then $(0, 1)$ written mod 2 and the decyphered text is B B B B B B A B B B.

#13 If you are given the matrix used in a Hill cipher, to decrypt you only need to find the inverse mod 26.

All the basic tricks regarding linear algebra and matrix multiplication algebra apply mod 26 so if

$$A = \begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix} \quad \text{then} \quad A^{-1} = \det(A)^{-1} \begin{pmatrix} 3 & -13 \\ -2 & 9 \end{pmatrix}$$

$\det(A) = 27 - 26 = 1$ which is <u>really</u> convenient.

So $A^{-1} = \begin{pmatrix} 3 & -13 \\ -2 & 9 \end{pmatrix}$

YIFZMA is encoded as $(24, 8, 5, 25, 12, 0)$

$(24, 8)A^{-1} = (4, 20)$ $\quad (5, 25)A^{-1} = (18, 4)$

$(12, 0)A^{-1} = (10, 0)$

and $(4, 20, 17, 4, 10, 0)$ is EUREKA.

#15 If you have a plaintext/ciphertext pairing from a Hill cipher, you use this to construct the unknown M as follows:

(b, a) ⇝ (1, 0) becomes (7, 2) (H, C) and
(z, z) ⇝ (-1, -1) becomes (6, 19) (G, T).

So $(1,0)M = (7,2)$ and $(-1,-1)M = (6,19)$ (all mod 26).

This gives the equation

$$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} M = \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \quad \text{and} \quad \det \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} = -1 \text{ which is invertible.}$$

$$\text{So } M = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 13 & 5 \end{pmatrix}.$$

#18 A chosen plaintext attack means that we have access to the encryption machine. If $(e,f) = (0,0)$ we know that encrypting e_1 and e_2 will give us the unknown matrix. If we don't know (e,f), notice that if you encrypt $(0,0)$ the result will be (e,f).

You can the proceed to decypher the resulting Hill cipher as usual.