Some More Cryptanalysis

Problem 1. Solve the following systems of congruences.

a.

$$\begin{aligned} 10x + 14y &\equiv 3 \pmod{65} \\ 44x + 26y &\equiv 18 \pmod{65} \end{aligned}$$

b.

$$\begin{aligned} x + 59y &\equiv 13 \pmod{98} \\ 27x + 90y &\equiv 69 \pmod{98} \end{aligned}$$

c.

$$\begin{aligned} 30x + 67y &\equiv 49 \pmod{74} \\ 11x + 8y &\equiv 61 \pmod{74} \end{aligned}$$

Problem 2. Does the system

$$\begin{aligned} 5x + 7y &\equiv 1 \pmod{12} \\ 7x + 8y &\equiv 1 \pmod{12} \end{aligned}$$

have any solutions?

Problem 3. The ciphertext message HVMZQQFGUCIIEQLKLFNQVYMEFJ MZZNYYNSNAIEOK was enciphered using a Hill cipher with a 2×2 integer matrix. Suppose you know that the last four letters of the corresponding plaintext are MICS. You attempt to implement the procedure we used in class to find the enciphering matrix, but you immediately encounter a problem: the matrix whose entries are the numerical equivalents of MICS is *not* invertible mod 26. But we can still find the inverse of the enciphering matrix and decrypt the message as follows. Let A denote the 2×2 enciphering matrix.

a. Write down the matrix congruence relating A and the blocks MICS and IEOK of corresponding plaintext and ciphertext.

b. Notice that the entries of the matrices appearing in part (a) (other than those in A, which we don't know) are all divisible by 2. Since 26 is divisible by 2, we can divide all of the entries by 2 and obtain a congruence mod 13.

c. Solve the congruence obtained in part (b) for A mod 13.

d. Find an inverse of A mod 13. Call this matrix B.

e. If C denotes the inverse of A mod 26 (the matrix we're after) show that $C \equiv B \pmod{13}$.

f. Show that part (e) implies there are only 16 possibilities for $C \pmod{26}$.

g. Attempt to decrypt the message with each of the matrices in part (f) until you find the one that works.

In case you aren't convinced that this saved you any time, keep in mind that if you had *no* information about A at all, then you would have to try as many as 157248 different matrices to decipher the message.

Problem 4. The message

TKZZWISCZCTASISRSTIQCBETCTQFFQAZSZCIISW
CFGARKXKTRKRKOYITRKTQCJKTBJEFGKXGQFK

was encrypted using an affine transformation. Use frequency analysis to find the encryption key and use this information to decrypt the message.