MATH 4282 – Cryptography — Assignment #2
Winter 2019

Instructions

- Answer each question completely; justify your answers.

1. Once more Eve has been monitoring communication between Alice and Bob. However, this time Alice and Bob are using a Vigenère cipher.

   You are Eve, and you have intercepted several ciphertexts that Alice sent to Bob. (copies of the ciphertexts are available on the course website). Determine the keys that Alice and Bob are using, and decipher their messages.

2. Suppose that M is a square matrix over $\mathbb{Z}_n$.
   Prove that if M^{-1} exists then $\gcd(\det(M), n) = 1$.

3. Consider the plaintext "*no new news at nine to noon*".

   (a) Determine the index of coincidence of the plaintext.

   (b) Encrypt the plaintext using the Vigenère cipher, with "*NOW*" as the keyword, and determine the index of coincidence of the corresponding ciphertext.

   (c) Encrypt the plaintext using the Hill cipher, with $\begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix}$ as the key, and determine the index of coincidence of the corresponding ciphertext.

4. Suppose you intercept the following ciphertext:

   BLPZQFSNEQLOOCMXHCVVNNKTGMDFCKIWLNRBXH

   You know the ciphertext was generated via the Hill cipher but you do not know the key. However, you have been able to ascertain that the corresponding plaintext is likely to be:

   january twenty-sixth. ten am. no enemy activity.

   Determine the key that is being used, assuming that the key is a 2 by 2 matrix.

5. The Hill cipher requires that the key matrix be invertible, modulo 26. Find three distinct matrices, K_1, K_2, and K_3, such that $xK_1 = xK_2 = xK_3$ for the plaintext string $x =$ "*th*". Which of your matrices is invertible?