

**COMP 7370**  
**Advanced Computer and Network Security**  
**Homework Assignment 1, Feb. 4**  
**Due on Thursday, Feb. 13 in class (submit your answer sheet)**

**Instruction: Every student should finish the following questions independently. Give justification for the results (i.e., show the calculation process and the corresponding diagram) to receive credits.**

In all the following encryption/decryption questions, let's assume that "a" corresponds to 0, "b" to 1, and so on.

1. Suppose you are given with an affine cipher with the following encryption function:  $c = 5m + 7 \pmod{26}$ . What's the ciphertext of the plaintext "helpme"?
2. Suppose you are given with an affine cipher with the following encryption function:  $c = 11m + 2 \pmod{26}$ . What's the plaintext of the ciphertext "vmwz"?
3. Let's consider a Hill cipher of block size 2 and its encryption function is given by  $C = MK$ , where M is the plaintext row vector and C is the ciphertext row vector. If the ciphertext of plaintext "friday" is "pqcfku," please calculate the encryption key K of the Hill cipher.
4. Please use extended Euclidean algorithm to calculate the multiplicative inverse of the following numbers. You must show the calculation steps to receive full credits.
  - (a)  $17^{-1} \pmod{101}$
  - (b)  $357^{-1} \pmod{1234}$
  - (c)  $3125^{-1} \pmod{9987}$
5. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a shift cipher:

**BEEAKFYDJXUQYHYJ I QRYHTYJ I QFBQDUYJ I I KFUHCQD.**

To answer this question, you should write a small program using any programming language that you prefer for the brute-force exhaustive key search. Please list/print all 26 trials (i.e., the tentative plaintext and its corresponding key value) from your key search and circle the correct one. Please print out your program and submit it together with your answer sheet.