CSI 4108
Cryptography

Assignment #1
Due: Friday, September 22, 2017 (before 16:00, to be e-mailed to the Corrector)

1. In class it was shown that the Hill cipher can be broken using a known-plaintext attack. Using an even stronger model of the adversary, we find that the Hill cipher can be easily broken with a chosen-plaintext attack. Explain how a chosen-plaintext attack can be used to determine the encryption key without requiring the execution of a matrix inversion or the solution of a set of linear equations. Is it realistic to assume that an adversary can mount a chosen-plaintext attack in real life? Why or why not (give a convincing answer)? Compared with a chosen-plaintext attack, would a chosen-ciphertext attack be more effective, less effective, or equally effective against this cipher? [1.5 marks]

2. The Caesar cipher is an example of a cipher based on a shifted alphabet, where each letter of the plaintext is shifted by \( k \) positions (that is, \( c = p + k \mod 26 \)). A generalization uses multiplication as the basis, so that \( c = pk \mod 26 \). In such a cipher, the values \( k = 0 \) and \( k = 1 \) would obviously not be wise choices. List all other values for \( k \) that would be unwise. What is unwise about these choices? In this multiplicative cipher, if the ciphertext is KSHUKRANMGUH, find \( k \) and \( p \). Does the multiplicative version have any advantages over the original Caesar cipher? [1.5 marks]

3. A further generalization of the Caesar cipher is the affine substitution cipher, in which \( c = (pk_1 + k_2) \mod 26 \). What is the size of the key space for this cipher? If it is suspected that the plaintext letter \( e \) (4) corresponds to the ciphertext letter \( p \) (15), what is the new size of the key space for the attacker? If it is known that the plaintext letter \( e \) (4) corresponds to the ciphertext letter \( p \) (15) and that the plaintext letter \( h \) (7) corresponds to the ciphertext letter \( e \) (4), break the cipher by solving for \( k_1 \) and \( k_2 \) (use brute force as well as a more efficient method). If we further generalize this cipher to \( c = pk_1k_2 + k_3 + k_4 \mod 26 \), how much security have we gained (in terms of key space and in terms of difficulty to break)? [3 marks]

4. Consider the transposition cipher, which permutes each block of \( m \) plaintext (alphabetic) characters in an \( n \)-bit message using a fixed \( m \)-valued permutation key. Someone tells you that because the data is very confidential, they will use double encryption (i.e., the ciphertext will be re-encrypted using an independent \( m \)-valued permutation key). Compute the additional security that this will provide in terms of \( m \) and \( n \). [2 marks]