COMP 7370/7376
Advanced Computer and Network Security
Homework Assignment, Feb. 24
Due on Monday, Mar. 17 on Canvas (upload 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. Scan your answer sheet and upload it to Canvas.

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 (mod 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 (mod 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} mod 101

(b) 357^{-1} mod 1234

(c) 3125^{-1} mod 9987

5. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a shift cipher:

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.

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.

6. Consider a cryptosystem in which $\mathcal{P}=\{a, b, c\}$, $\mathcal{K}=\{K_1, K_2, K_3\}$, and $\mathcal{C}=\{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Given that keys are chosen equiprobably, and the plaintext probability distribution is Pr[a]=1/2, Pr[b]=1/3, Pr[c]=1/6, compute the entropies H(**P**), H(**C**), H(**K**), H(**K**|**C**) and H(**P**|**C**).

7. (Chinese Remainder Theorem) Solve the following system of congruences:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27}.$$

8. (Discrete Logarithm) Let $p = 227$. The element $\alpha=2$ is primitive in Z_p^*.

(a) Compute α^{32}, α^{40}, α^{59} and α^{156} modulo p, and factor them over the factor base {2, 3, 5, 7, 11}.

(b) Using the fact that log 2 = 1, compute log 3, log 5, log 7 and log 11 from the factorizations obtained above (all logarithms are discrete logarithms in Z_p^* to the base α).

9. Compute gcd(57, 93), and find integers s and t such that $57s+93t = \gcd(57, 93)$.