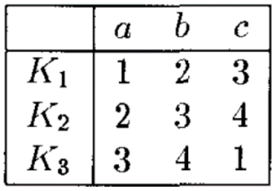
COMP 7370/7376
Advanced Computer and Network Security
Homework Assignment 2, Mar. 3
Due on Tuesday, Mar. 16 in class (submit your answer sheet)

Instruction: Every student should finish the following questions independently. Give justification for the results (i.e., show the calculation process/steps) to receive full credits.

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

1. 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**).

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

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

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

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

3. (Discrete Logarithm) Let p = 227. The element α=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).()

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