1) Consider a cipher that has three keys, three plaintexts, and four ciphertexts that are combined using the following encryption table.

	m1	m2	m3
k1	c2	c4	c1
k2	c1	c3	c2
k3	c3	c1	c2

Suppose further that the plaintexts and keys are used with the following probabilities.

$$p(m1)=p(m2)=\frac{2}{5}$$

$$p(m3)=\frac{1}{5}$$

$$p(k1)=p(k2)=p(k3)=\frac{1}{3}$$

Does the above cryptosystem has perfect secrecy?

2) The One-Time Pad (OTP) is defined as follows. A plaintext is considered as a random variable $X \in \{0,1\}^n$, where n is some positive integer. It is encrypted with a uniformly distributed random key $K \in \{0,1\}^n$, independent of X, using a bitwise XOR operation. The ciphertext is thus $Y = X \oplus K$. Prove that the OTP provides prefect secrecy.

3) Consider a crypto system in which P = {a, b, c}, K = {k1, k2, k3} and C = {1, 2, 3, 4}. Suppose the encryption matrix is as follows:

	a	b	c
k1	1	2	3
k2	2	3	4
k2	3	4	1

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