Cryptography Quiz 5

Each problem worths two points:

Consider the cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{k_1, k_2, k_3\}$, and $\mathcal{C} = \{1, 2, 3, 4\}$ with $p[a] = 1/2$, $p[b] = 1/3$, $p[c] = 1/6$ and the keys are chosen equiprobably, that is, $p[k_1] = p[k_2] = p[k_3] = 1/3$. The encryption matrix is given as follows:

	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

1. Find $p[1]$
2. Find $p[2]$
3. Find $p[3]$
4. Find $p[4]$
5. Find the conditional probability $p[3|b]$.
6. By using Bayes' theorem or directly, find the conditional probability $p[b|3]$.
7. Find the joint probability $p[b, 3]$
8. By using the formula $H(X) = -\sum p[x] \log_2 p[x]$, compute H(P)
9. Compute H(K)
10. Compute H(C)