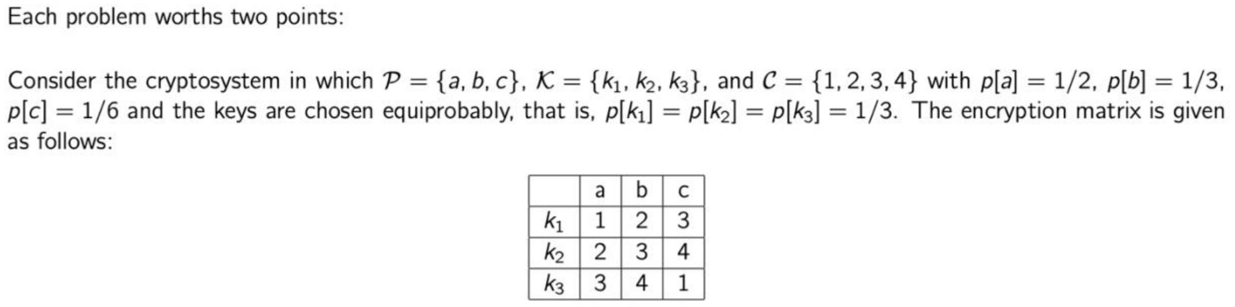
INTRODUCTION TO CRYPTOGRAPHY – QUIZ 5
B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of submission: 03/02/2022

Quiz



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]

   ➔ p[k$_1$]p[a] + p[k$_3$]p[c] = (1/3)(1/2) + (1/3)(1/6) = 2/9

2. Find p[2]

   ➔ p[k$_2$]p[a] + p[k$_1$]p[b] = (1/3)(1/2) + (1/3)(1/3) = 5/18

3. Find p[3]

   ➔ p[k$_1$]p[c] + p[k$_2$]p[b] + p[k$_3$]p[a] = (1/3)(1/6) + (1/3)(1/3) + (1/3)(1/2) = 1/3

4. Find p[4]

   ➔ p[k$_2$]p[c] + p[k$_3$]p[b] = (1/3)(1/6) + (1/3)(1/3) = 1/6

5. Find the conditional probability p[3|b]

   ➔ We get cipher text equal to 3 when plain text is b only when key k2 is chosen and the probability of choosing k2 is 1/3

   Therefore, p[3|b] = p[k$_2$] = 1/3

6. By using the Baye's theorem or directly, find the conditional probability p[b|3]

   ➔ p[b|3] = p[3|b]p[b]/p[3] = ((1/3)(1/3))/(1/3) = 1/3

7. Find the joint probability p[b,3]

   ➔ p[b,3] = p[b|3]p[3] = (1/3)(1/3) = 1/9

8. By using the formula H(X) = - Σp[x]log$_2$p[x], compute H(P)

➔ $H(P) = -((1/2) \log_2(1/2) + (1/3) \log_2(1/3) + (1/6) \log_2(1/6)) = 1.459$

9. Compute H(K)

   ➔ $H(K) = -((1/3) \log_2(1/3) + (1/3) \log_2(1/3) + (1/3) \log_2(1/3)) = - \log_2(1/3) = 1.584$

10. Compute H(C)

    ➔ $H(C) = -((2/9) \log_2(2/9) + (5/18) \log_2(5/18) + (1/3) \log_2(1/3) + (1/6) \log_2(1/6)) = 1.95$