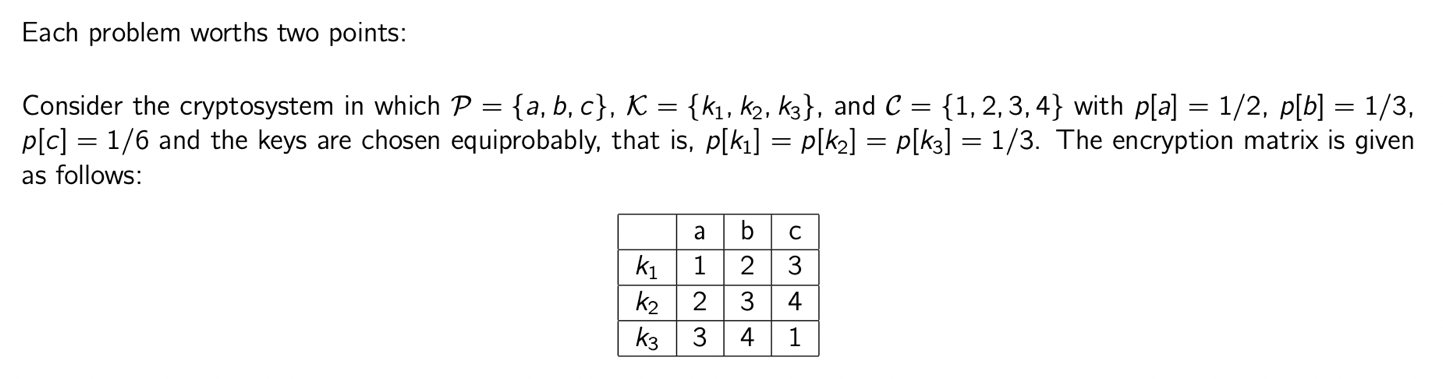
INTRODUCTION TO CRYPTOGRAPHY – QUIZ 5

B.Tech. Computer Science and Engineering (Cybersecurity)

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

Quiz



1. Find p[1]

* p[k1]p[a] + p[k3]p[c] = (1/3)(1/2) + (1/3)(1/6) = 2/9

1. Find p[2]

* p[k2]p[a] + p[k1]p[b] = (1/3)(1/2) + (1/3)(1/3) = 5/18

1. Find p[3]

* p[k1]p[c] + p[k2]p[b] + p[k3]p[a] = (1/3)(1/6) + (1/3)(1/3) + (1/3)(1/2) = 1/3

1. Find p[4]

* p[k2]p[c] + p[k3]p[b] = (1/3)(1/6) + (1/3)(1/3) = 1/6

1. 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[k2] = 1/3

1. 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

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

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

1. By using the formula H(X) = - Σp[x]log2p[x], compute H(P)

* H(P) = - ((1/2) log2(1/2) + (1/3) log2(1/3) + (1/6) log2(1/6)) = 1.459

1. Compute H(K)

* H(K) = - ((1/3) log2(1/3) + (1/3) log2(1/3) + (1/3) log2(1/3)) = - log2(1/3) = 1.584

1. Compute H(C)

* H(C) = - ((2/9) log2(2/9) + (5/18) log2(5/18) + (1/3) log2(1/3) + (1/6) log2(1/6)) = 1.95