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)

2/2/22 K016 - Dinesh - Crypto - Quiz - 5

Given

9)

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

$P = \{a, b, c\}$, $K = \{K_1, K_2, K_3\}$ and $C = \{1, 2, 3, 4\}$ with
$p[a] = 1/2$, $p[b] = 1/3$, $P[c] = 1/6$.
$p[K_1] = p[K_2] = p[K_3] = 1/3$

~~1. Find $p[1] = p[K_1]\, p[a] = \left(\frac{1}{3}\right)\left(\frac{1}{2}\right) = \frac{1}{6}$~~

~~2. Find $p[2] =$~~

1. Find $p[1] = p[K_1]\, p[a] + p[K_3]\, P[c] = \left(\frac{1}{3}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{6}\right) = \frac{2}{9}$ //

2. Find $p[2] = p[K_1]\, p[b] + p[K_2]\, p[a] = \left(\frac{1}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{2}\right) = \frac{5}{18}$ //

3. Find $P[3] = p[K_1]\, p[c] + p[K_2]\, p[b] + p[K_3]\, p[a] = \left(\frac{1}{3}\right)\left(\frac{1}{6}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{2}\right) = \frac{1}{3}$ //

4. Find $p[4] = p[K_2]\, p[c] + p[K_3]\, p[b] = \left(\frac{1}{3}\right)\left(\frac{1}{6}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{3}\right) = \frac{1}{6}$ //

5. To find conditional probability $p[3|b]$

=> In this we need to find the probability of 3 when b is given, From the above table we observe that 3 lies under the column b and belongs to the row K_2. Such that probability of K_2 equal to $\frac{1}{3}$

$\therefore\ P[3|b] = \frac{1}{3}$ //

Page No.
Date :

6] By usind Bayes theorem, find the conditional probability p[b|3]

⇒ Baye's theorem :

$$P[x|y] = \frac{P[x]\,P[y|x]}{P[y]}$$

~~Given~~ To find :

$$P[b|3] = \frac{P[b]\,P[3|b]}{P[3]} = \frac{(1/3)\,(1/3)}{\frac{1}{3}} = \frac{1}{3}$$ //

Q7] To find the joint probability, $P[b, 3]$

$$P[b,3] = P(b|3) \times P(b)$$
$$= \frac{1}{3} \times \frac{1}{3}$$
$$= \frac{1}{9}$$

Q8] Given

Formula , $H(X) = -\sum p[x] \log_2 P[x]$

To find $H(P)$

$P[a] = \frac{1}{2}$, $P[b] = \frac{1}{3}$, $P[c] = \frac{1}{6}$ [Given in the 1st Q]

$$H(P) = -\left(\frac{1}{2}\right)\log_2\left(\frac{1}{2}\right) - \left(\frac{1}{3}\right)\log_2\left(\frac{1}{3}\right) - \left(\frac{1}{6}\right)\log_2\left(\frac{1}{6}\right)$$

$$= 1.459$$

Q9] $H(K) = ?$

Given $p[K_1] = p[K_2] = p[K_3] = \frac{1}{3}$

$$= -\frac{1}{3}\log_2\left(\frac{1}{3}\right) - \frac{1}{3}\log_2\left(\frac{1}{3}\right) - \frac{1}{3}\log_2\left(\frac{1}{3}\right)$$

$$= 1.584$$

DATE:

Q10] $H(C) = ?$

$C = \{1, 2, 3, 4\}$ with $\underbrace{p[1] = \frac{2}{9},\ p[2] = \frac{5}{18},\ p[3] = \frac{1}{3},\ p[4] = \frac{1}{6}}_{\text{found in the above Q's}}$

$$H(C) = -\frac{2}{9}\log_2\left(\frac{2}{9}\right) - \frac{5}{18}\log_2\left(\frac{5}{18}\right) - \frac{1}{3}\log_2\left(\frac{1}{3}\right) - \frac{1}{6}\log_2\left(\frac{1}{6}\right)$$

$$= 1.95$$