SC402: Introduction to Cryptography

3/5/2022

Homework 2

Prof. Manish K. Gupta

Details:

Name: Madhvi Padshala
ID: 201901171

Q.1

Suppose we consider a random throw of a pair of dice. Let X be the random variable defined on the set X = {2, . . . , 12} , obtained by considering the sum of two dice. Further, suppose that Y is a random variable which takes on the value D if the two dice are the same (i.e., if we throw "doubles"), and the value N, otherwise. Determine all the joint and conditional probabilities, Pr[x, y], Pr[x|y], and Pr[y|x] , where x ∈ {2, . . . , 12} and y ∈ {D, N}.

Ans:

X = {1,2,3….12}
Y= {D,N}

X	Dies Rolls	P(x)	Count of D	Count of N
2	(1,1)	1/36	1	0
3	(1,2)(2,1)	2/36	0	2
4	(1,3)(2,2)(3,1)	3/36	1	2
5	(1,4)(2,3)(3,2)(4,1)	4/36	0	4
6	(1,5)(2,4)(3,3)(4,2)(5,1)	5/36	1	4
7	(1,6)(2,5)(3,4)(4,3)(5,2)(6,1)	6/36	0	6
8	(2,6)(3,5)(4,4)(5,3)(6,2)	5/36	1	4
9	(3,6)(4,5)(5,4)(6,3)	4/36	0	4
10	(4,6)(5,5)(6,4)	3/36	1	2
11	(5,6)(6,5)	2/36	0	2
12	(6,6)	1/36	1	0
			6	**30**

P(X,Y) = P(X=2,Y=D) = 1/36 , P(X=2,Y=N)=0

P(X=3,Y=D)=0	P(X=3,Y=N)=2/36
P(X=4,Y=D)=1/36	P(X=4,Y=N)=2/36
P(X=5,Y=D)=0	P(X=5,Y=N)=4/36
P(X=6,Y=D)=1/36	P(X=6,Y=N)=4/36
P(X=7,Y=D)=0	P(X=7,Y=N)=6/36
P(X=8,Y=D)=1/36	P(X=8,Y=N)=4/36
P(X=9,Y=D)=0	P(X=9,Y=N)=4/36
P(X=10,Y=D)=1/36	P(X=10,Y=N)=2/36
P(X=11,Y=D)=0	P(X=11,Y=N)=2/36
P(X=12,Y=D)=1/36	P(X=12,Y=N)=0

P(Y/X) = Probability of Y given X

P(Y=D/X=2)=1	P(Y=N/X=2)=0
P(Y=D/X=3)=0	P(Y=N/X=3)=1
P(Y=D/X=4)=3/3	P(Y=N/X=4)=2/3
P(Y=D/X=5)=0	P(Y=N/X=5)=1
P(Y=D/X=6)=3/5	P(Y=N/X=6)=4/5
P(Y=D/X=7)=0	P(Y=N/X=7)=1
P(Y=D/X=8)=1/5	P(Y=N/X=8)=4/5
P(Y=D/X=9)=0	P(Y=N/X=9)=1
P(Y=D/X=10)=1/3	P(Y=N/X=10)=2/3
P(Y=D/X=11)=0	P(Y=N/X=11)=1
P(Y=D/X=12)=1	P(Y=N/X=12)=0

$P(X|Y)$ = Probability of X given Y

Now as $Y = D$ is only possible per $X \to$ even and once in every even value of X.

$P\left(\frac{x \to \text{even}}{Y=D}\right) = \frac{1}{6}$ $\{x = 2, 4, 6, 8, 10, 12\}$

$P\left(\frac{x \to \text{odd}}{Y=D}\right) = 0$ $\{x = 3, 5, 7, 9, 11\}$

$P'(X/Y=N) \to$ Prob. of X given Y = N.

$P(x=2/y=N) = 0$ $\quad$ $P(x=3/y=N) = 2/30$

$P(x=4/y=N) = 2/30$ $\quad$ $P(x=5/y=N) = 4/30$

$P(x=6/y=N) = 4/30$ $\quad$ $P(x=7/y=N) = 6/30$

$P(x=8/y=N) = 4/30$ $\quad$ $P(x=9/y=N) = 4/30$

$P(x=10/y=N) = 2/30$ $\quad$ $P(x=11/y=N) = 2/30$

$P(x=12/y=N) = 0$

Q.2

Let P = {a, b} and let K = {K1, K2, K3, K4, K5}. Let C = {1, 2, 3, 4, 5} , and suppose the encryption functions are represented by the following encryption matrix:

	a	b
K_1	1	2
K_2	2	3
K_3	3	1
K_4	4	5
K_5	5	4

Now choose two positive real numbers α and β such that α + β = 1, and define Pr[K1] = Pr[K2] = Pr[K3] = α/3 and Pr[K4] = Pr[K5] = β/2.

Prove that this cryptosystem achieves perfect secrecy.

Ans:

P = {a,b}
K = {K1, K2,K3,K4,K5}
C = {1,2,3,4,5}

- ⇨ Alpha + beta = 1

Pr[K1] = Pr[K2] = Pr[K3] = $\alpha/3$
Pr[K4] = Pr[K5] = $\beta/2$

Let P(a) = x and P(b)= 1-x
Here we need to prove P(X)=P(X/4)

Y=1,2,3

P(y) = P(X=a,y) + P(X=b,y)
= x($\alpha/3$) + (1-x)($\alpha/3$)
= $\alpha/3$ ………………………(1)

P(y/x) = P(Key) where Key=K1,K2,K3
= P(K1)= $\alpha/3$ ……………………(2)

From Eq 1 and 2
P(y) = P(y/x)
For,
P(x/y) = P(x)*P(y/x) / P(y)
So, P(x/y) = P(x) -----→ for Y=1,2,3

Y=4,5

P(y) = P(x=a,y) + P(x=b,y)
= x($\beta/2$) + (1-x)($\beta/2$)
= $\beta/2$……………………………….(3)

P(y/x) = P(Key) where Key=K4,K5
= P(Key)= $\beta/2$ ……………………(4)

Similarly,
P(x/y) = P(x) * P(y/x) / P(y)
= P(x)

P(x/y) = P(x)

So now, We can say that, Cryptosystem achieve perfect secrecy.

Q.3

A) Prove that the Affine Cipher achieves perfect secrecy if every key is used with equal probability 1/312.

Ans:

Probability = 1/312
Since equal probability for each k belong to K
We get Pk(K) = 1/312

We show that there are exatly 12 keys that encrypt x to y for any combination of plain text – cipher text letter (x,y)

For every different different value of ‘a’ , the key (a, y - axe) encrypts ‘x’ to ‘y’.
There are 12 keys that map a given plaintext letter to a given cipher text letter since there are 12 possibilities for a,

Pk(K) * Pp(d_k(y)) = $\frac{12}{312}\ Pp(a) + \frac{12}{312}\left(Pp(b)\right) + \ldots\ldots + \frac{12}{312} Pp(z)$

$= \frac{12}{312} * 1$

$= \mathbf{\frac{1}{26}}$

Also , Pc(y/x) = $\sum^{K=x=dk(y)} Pk(K)$

= 12/312

=1/26

Pp(x/y) = $\frac{\mathrm{Pp(x)} * \mathrm{Pc}\left(\frac{y}{x}\right)}{\mathrm{Pc(y)}}$

= $\frac{Pp(x)*1/26}{1/26}$

= Pp(x)

So using Baye's theorem, we see that if we use every key with equal probability 1/312 then we can achieve perfect secrecy.

B) More generally, suppose we are given a probability distribution on the set

{a ∈ Z26 : gcd(a, 26) = 1}.

Suppose that every key (a, b) for the Affine Cipher is used with probability Pr[a]/26.

Prove that the Affine Cipher achieves perfect secrecy when this probability distri-bution is defined on the keyspace.

Ans:

The probability of key (a,b) should be Pr.[a]/26.

proceding as in part(a), for any $y \in \{1, \ldots, n\}$,

$$Pr[Y=y] = \sum_{x \in 1 \text{ to } n} \sum_{a \in Z_{26}^*} Pr[K=(a, b(x,y,a))] Pr[x]$$

$$= \sum_{x \in 1 \text{ to } n} \sum_{a \in Z_{26}^*} (Pr[a]/26) \times Pr(X=x)$$

$$= \sum_{x \in 1 \text{ to } n} \frac{1}{26} \times Pr(X=x)$$

$$= \frac{1}{26}$$

Then for any $x, y \in \mathbb{Z}_{26}$, we compute

$$Pr[Y = y \,/\, X = x] = \sum_{a \in \mathbb{Z}_{26}^{*}} Pr[K = (a, b(x,y,a))]$$

$$= \sum_{a \in \mathbb{Z}_{26}^{*}} Pr[a]/26$$

$$= 1/26$$

Finally using Bay's theorem, we see that

$$Pr[X = x \,/\, Y = y] = Pr[X = x]$$

for all x, y

Q.4

Suppose that S is a random variable representing the sum of a pair of dice. Compute H(S).

Ans:

S is sum of pair of dies
So S $\in \{2,3,4,5,..12\}$

P(S=2) = 1/36 = p(S=12)
P(S=3) = 2/36 = p(S=11)
P(S=4) = 3/36 = S(S=10)
P(S=5) = 4/36 = p(S=9)
P(S=6) = 5/36 = p(S=8)
P(S=7) = 6/36

H(S) = $\sum_{i=2}^{12} P(S = i) * \log_2 \frac{1}{Ps(i)}$

H(S) = $\frac{2* \log_2 36}{36} + \frac{2*2* \log_2 36/2}{36} + \frac{2*3* \log_2 36/3}{36} + \frac{2*4* \log_2 36/4}{36} + \frac{2*5* \log_2 36/5}{36} + \frac{6* \log_2 36/6}{36}$

$= \frac{2}{36} (\log_2 36 + 2 * \log_2 \frac{36}{2} + 3 * \log_2 \frac{36}{3} + 4 * \log_2 \frac{36}{4} + 5 * \log_2 \frac{36}{5} + 3 * \log_2 \frac{36}{6})$

= 2.5686

Q.5 Consider a cryptosystem 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
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Given that keys are chosen equiprobably, and the plaintext probability distribution is

Pr[a] = 1/2, Pr[b] = 1/3, Pr[c] = 1/6, compute H(P), H(C), H(K), H(K|C), and

H(P|C).

Ans.

P= {a,b,c}
Pr[a] = 1/2, Pr[b] = 1/3, Pr[c] = 1/6
K = {K1,K2,K3} = Pr[K1] = Pr[K2] = Pr[K3]= 1/3
C = {1,2,3,4}

H(P) = $\frac{\log_2 2}{2} + \frac{\log_2 3}{3} + \frac{\log_2 6}{6}$
= 0.50 + 0.53 + 0.43
= 1.46

H(K) = $\frac{\log_2 3}{3} + \frac{\log_2 3}{3} + \frac{\log_2 3}{3}$
= 1.58

Pr[C=1] = Pr[a] * Pr[K1] + Pr[c] * Pr[K3]
= 1/6 + 1/18 => 2/9

Pr[C=2] = 5/18 Pr[C=3] = 1/3 Pr[C=4] = 1/6

H(C) = $\frac{2}{9}(\log_2 9 - \log_2 2) + \frac{5}{18}(\log_2 18 - \log_2 5) + \frac{1}{3}(\log_2 3 - \log_2 1) + \frac{1}{6}(\log_2 6 - \log_2 1)$
= 0.48 + 0.51 + 0.53 + 0.43
= 1.95

H(K|C) = H(K) + H(P) – H(C)
= **1.09**

For H(P|C),

Pr[p=a, y], y=1,2,3
= 1/6

Pr[p=b, y], y=2,3,4
= 1/9

Pr[p=c, y], y=1,3,4
= 1/18

H(P,C) = 3 $\left(\frac{\log_2 6}{6} + \frac{\log_2 9}{9} + \frac{\log_2 18}{18}\right)$
$\cong$ 3.044

H(P|C) = H(P,C) – H(C)
= 3.044 – 1.95
= **1.094**