PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

APPLIED CRYPTOGRAPHY

Lecture 7

Probability, Conditional probability and Law of total probability

Success or failure rates

probability

- Probability is the branch of mathematics concerning numerical descriptions of how likely an event is to occur or how likely it is that a proposition is true.
- Pr[K = k] denotes the probability that the key output by Gen is equal to k
- Pr[M = m] denotes the probability that the message takes on the value m $\in$M

Basics of probability

- If E is an event denotes complement of event
- Then pr[E]= 1-pr[$\bar{E}$]
- If E1 and E2 are events than E1^E2 is the event that both e1 and e2 occurs
- If pr[E1^E2]= pr[E1].pr[E2] then E1 and E2 are independent events
- Addition Theorem on probability
  - n(AUB)= n(A)+n(B)-N(A ∩ B)

Conditional probability

- Conditional probability of A and B denoted as P[A|B]
  - The probability that A and B occur is equal to the probability that A occurs times the probability B occurs given that A has occurred
- P[A|B]= P[A^B]/Pr[B]
- Therefore P[A^B]= P[A|B]/P[B]
- Given P[B]!=0

Example 1: suppose P(A)=0.34 and P(B)=0.50 and P(AUB)=0.7 find P(A|B)

- P(A|B)= P(A^B)/P(B)
- P(AUB)= P(A)+P(B)-P(A∩B)
- Therefore P(A∩B)= p(A)+P(B)-P(AUB)

Example 2: rolling of dice once
event A={1,4} B={2,3,4,6} C={1,3,5} find P(AUB|C)

- Sample space={1,2,3,4,5,6}
- P(AUB|C)= P((AUB) ∩ C)/P(C)

Problems on venn diagram

- Given $P(A)=0.43$ $P(B)=0.29$ $P(C)= 0.30$
  $P(A \cap B)=0.13$ $P(A \cap C)=0.15$ $P(B \cap C)=0.07$
  $P(A \cap B \cap C)= 0.03$ find
  $P(A \cap C \mid B \cap C)$
- $P(A \cap B \mid B \cap C) = (P(A \cap B) \cap P(B \cap C))/P(B \cap C)$ use venn diagram

If A and B are two possible events of an experiment such that p(A U B)=0.6 p(A)=0.3 then find p(B)

1. A and B are mutually exclusive event
2. A and B are independent event

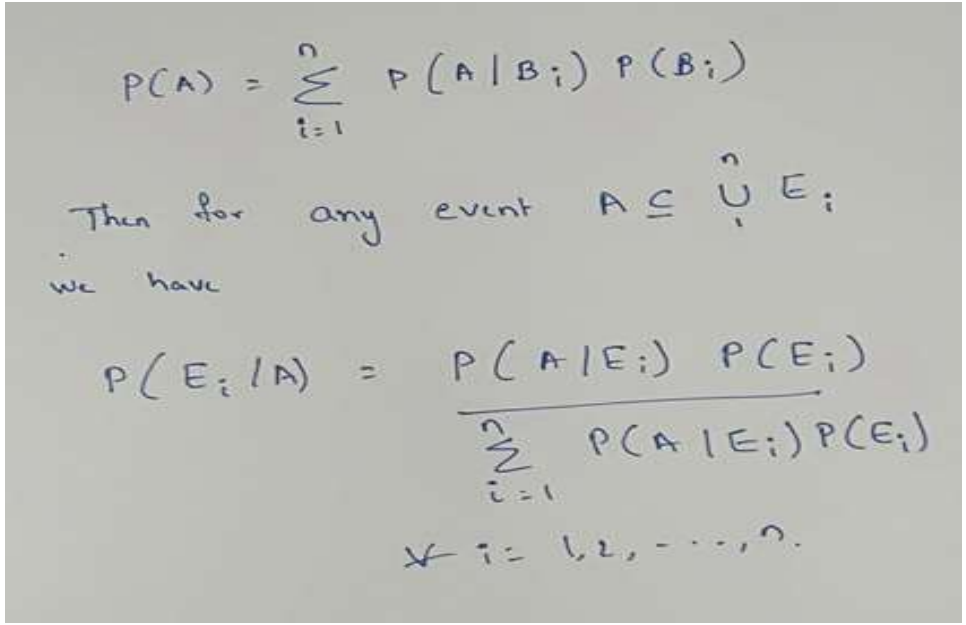
$P(AUB)= P(A)+P(B)-P(A \cap B)$

For mutually exclusive event $p(A \cap B)=0$

For independent event $p(A \cap B) = p(A).P(B)$

Law of Total probability

- the total probability of an outcome which can be realized via several distinct events



Bayes theorem
Pr[E1|E2] = (pr[E2|E1].Pr[E1])/pr[E2]

- Enables us to find the probability of various events E that can cause E2 to occur
- Therefore bayes theorem is also called as theorem on the probability of causes

Problem on total prabability

- Three urns A,B,C have
  1 white 2 black 3 red balls,
  2 white 1 black 1 red balls ,
  4 white 5 black 3 red balls respectively
  one urn is chosen at random and two balls are drawn. They happen to be white and red balls what is the probability that they come from urn B.

Solution

Event of choosing A B C= 1/3

Condition from A= (1c1+3c1)/6c2= 1/5

B=(2c1+1c1)/4c2=1/3

C=(4c1+3c1)/12c2=2/11

Probability from urn B = 1/3/(1/5+1/3+2/11)=55/118

Note : C(n,r) = n! / r! (n - r)!

- If we have K = {0,...,25}with Pr[K = k] = 1/26 for each k ∈K Pr[M = a] = 0.7 and Pr[M = z] = 0.3
  What is the probability that the ciphertext is B?

Solution: possible only when

M = a and K = 1 c=B,

or

M = z and K = 2 c=B

Solution

$$\Pr[M = \mathtt{a} \wedge K = 1] = \Pr[M = \mathtt{a}] \cdot \Pr[K = 1] \; = 0.7 \cdot \left(\frac{1}{26}\right)$$

$$\Pr[M = \mathtt{z} \wedge K = 2] = \Pr[M = \mathtt{z}] \cdot \Pr[K = 2] = 0.3 \cdot \left(\frac{1}{26}\right)$$

$$\begin{aligned}\Pr[C = \mathtt{B}] &= \Pr[M = \mathtt{a} \wedge K = 1] + \Pr[M = \mathtt{z} \wedge K = 2] \\ &= 0.7 \cdot \left(\frac{1}{26}\right) + 0.3 \cdot \left(\frac{1}{26}\right) \; = \; 1/26.\end{aligned}$$

Solve this

Consider the shift cipher, with the following distribution over M: Pr[M = kim] = 0.5, Pr[M = ann] = 0.2, Pr[M = boo] = 0.3.

What is the probability that C = DQQ

Next Class

- ☞ Mandatory reading for the next class
  - ☞ http://theory.cse.iitm.ac.in/tcslab/cryptpage/report1.pdf

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT

PESU Center for Internet of Things