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 8

Perfect secrecy

Can it be achieved!!!

Goal of secure encryption?

- How would you define what it means for encryption scheme (Gen, Enc, Dec) over message space $\mathcal{M}$ to be secure?

Perfect secrecy

- An encryption scheme(gen, Enc, Dec) with message space M is perfectly secret if and only if equation (a) holds for every m,m` ∈ M and every c ∈ C

Perfect (adversarial) indistinguishability

- observing a ciphertext and then trying to guess which of two possible messages was encrypted
- An encryption scheme is perfectly indistinguishable if no adversary A can succeed with probability better than ½.

DEFINITION 2.5 *Encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *is* perfectly indistinguishable *if for every* $\mathcal{A}$ *it holds that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}.$$

Probability distributions

- Let K be a random variable denoting the key
  - K ranges over $\mathcal{K}$

- Fix some encryption scheme (Gen, Enc, Dec)
  - Gen defines a probability distribution for K:
    Pr[K = k] = Pr[Gen outputs key k]

- Random variables M and K are *independent*

For example

- If M={a,b,c,d}
- K={k1,k2,k3}
- P(a)=1/4 p(b)=3/10 p(c)=3/20 p(d)=3/10
- P(k1)=1/4 p(k2)=1/2 p(k3)=1/4
- And encryption table for M and k is given by

	a	b	c	d
	3	**4**	**2**	**1**
K1	3	1	4	2
K2	4	3	1	2
K3				

find probability that enc algorithm outputs 1

That is need to find Pr(c=1)

- Pr(c=1)=0.2625
- Pr(c=2)=0.2625
- Pr(c=3)= 0.2625
- Pr(c=4)=0.2125

3	4	2	1
3	1	4	2
4	3	1	2

P(a)=1/4 p(b)=3/10
p(c)=3/20 p(d)=3/10

P(k1)=1/4 p(k2)=1/2
p(k3)=1/4

Example 2: when given plain text is = m what is the probability that ciphertext is c

- Pr(C=1|M=a)
- Pr(C=2|M=a)
- Pr(C=3|M=a)
- Pr(C=4|M=a)

3	4	2	1
3	1	4	2
4	3	1	2

P(a)=1/4 p(b)=3/10
p(c)=3/20 p(d)=3/10

P(k1)=1/4 p(k2)=1/2
p(k3)=1/4

Find the probability of message=m given the ciphertext is c

- Pr(M=a|c=1):

From bayes theorem

Pr(M=m|C=c)= Pr((C=c | M=m). Pr(M=m))/(pr(C=c))

3	4	2	1
3	1	4	2
4	3	1	2

P(a)=1/4 p(b)=3/10
p(c)=3/20 p(d)=3/10

P(k1)=1/4 p(k2)=1/2
p(k3)=1/4

Next Class

- Mandatory reading for the next class
  - https://www.cs.miami.edu/home/burt/learning/Csc609.011/Perfect/

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT

PESU Center for Internet of Things