REVA UNIVERSITY

Established as per the Section 2(f) of the UGC Act, 1956
Approved by AICTE, COA and BCI, New Delhi

QS I·GAUGE GOLD

nirf

CARE RATINGS KSURF

MHRD'S INNOVATION CELL (GOVERNMENT OF INDIA)

INSTITUTION'S INNOVATION COUNCIL (Ministry of HRD Initiative)

Lecture 1.1

Introductory Class

School of Computing and Information Technology

Prof.K.Jeevan pradeep

OUTLINE

Importance of Information and Network Security

Course Description

Course Objectives

Course Contents

Learning Resources

Additional Resources

Real World Applications

Information and Network Security Related Companies in India

Job Roles in Industry

Type of Assignments

Quizzes

Pedagogy

Marks Distribution

Course Delivery

B20EJ0601: Information and Network Security

6th Semester

Introduction Class

Information and Network Security

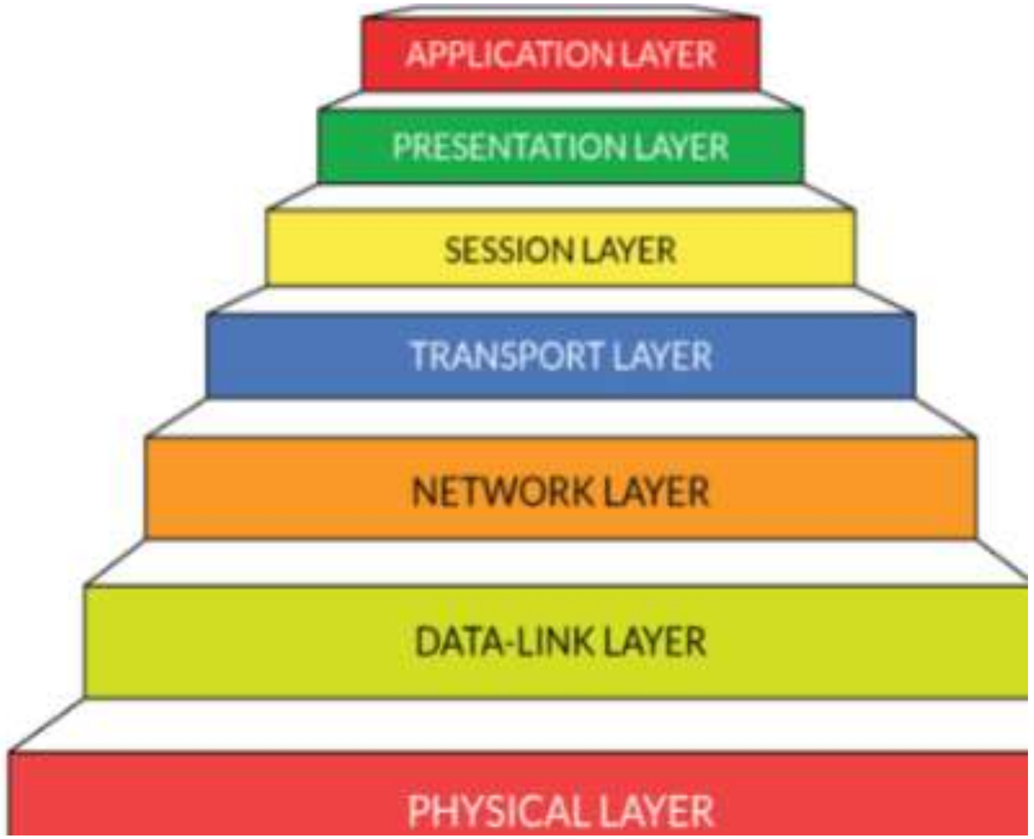
COMPUTER NETWORK DEFINITION & EXAMPLE

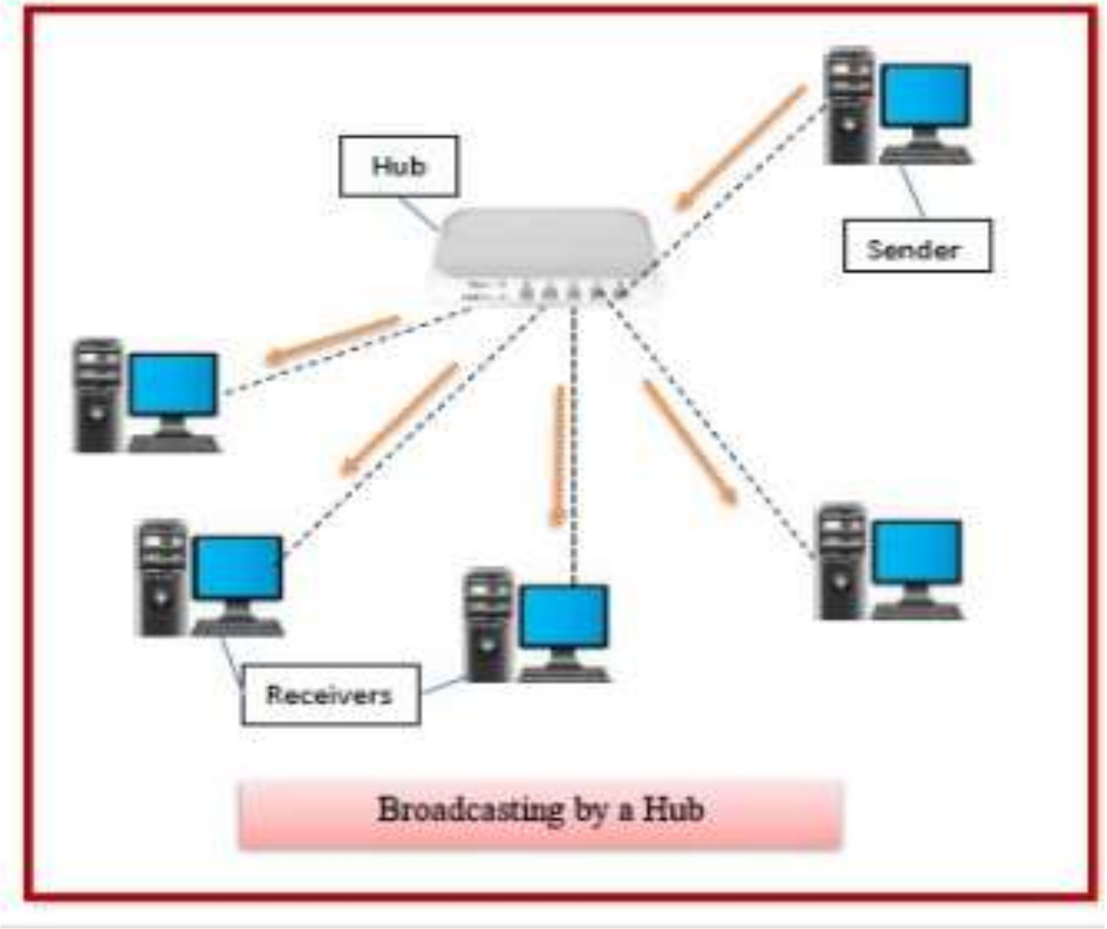
A computer network, also referred to as a **data network, is a series of interconnected nodes that can transmit, receive and exchange data, voice and video traffic**.

Examples of nodes in a network include servers or modems. computer networks commonly help endpoint users share resources and communicate.

HUB

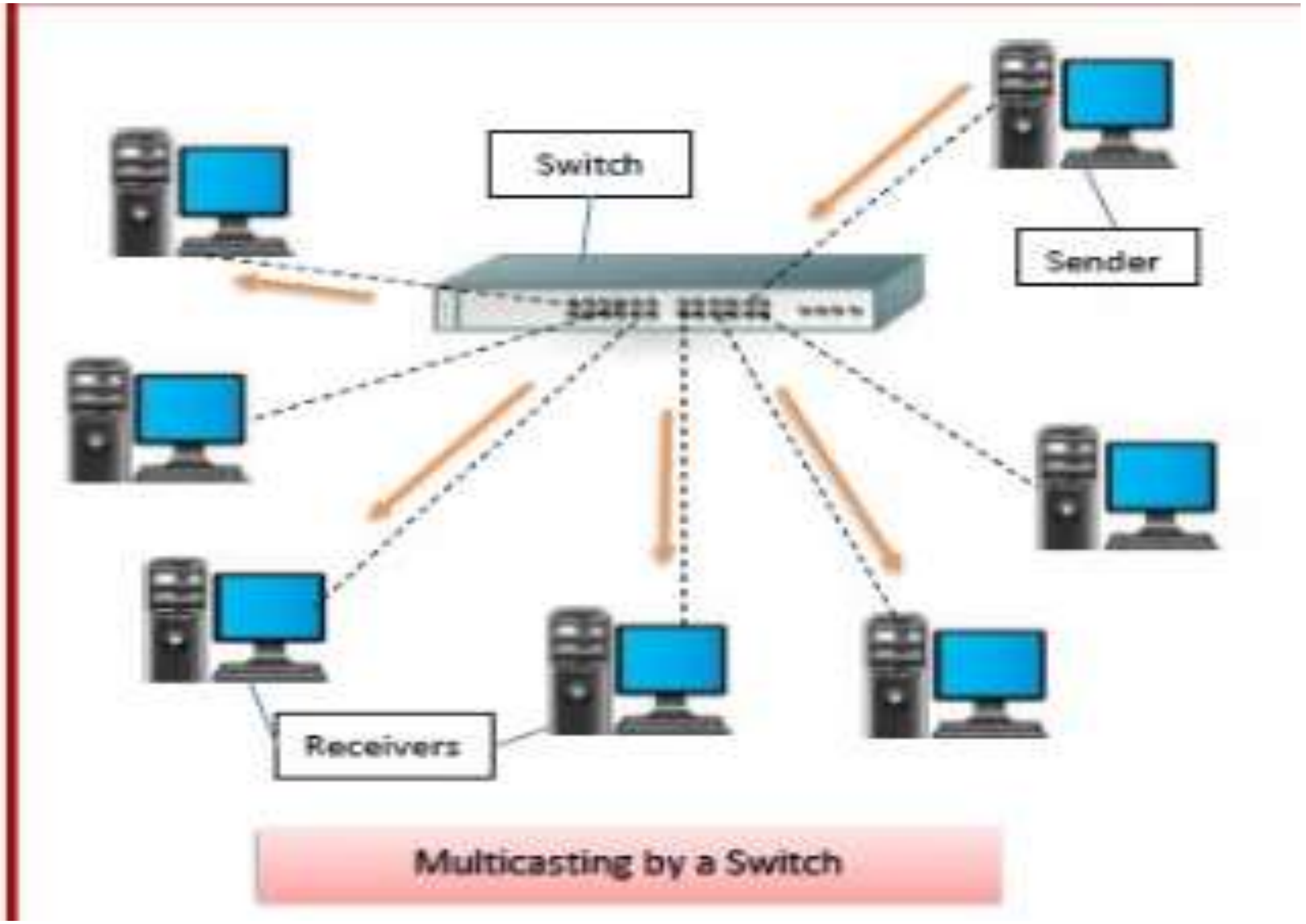
HUBS are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. they are generally used to connect computers in a LAN.





SWITCH

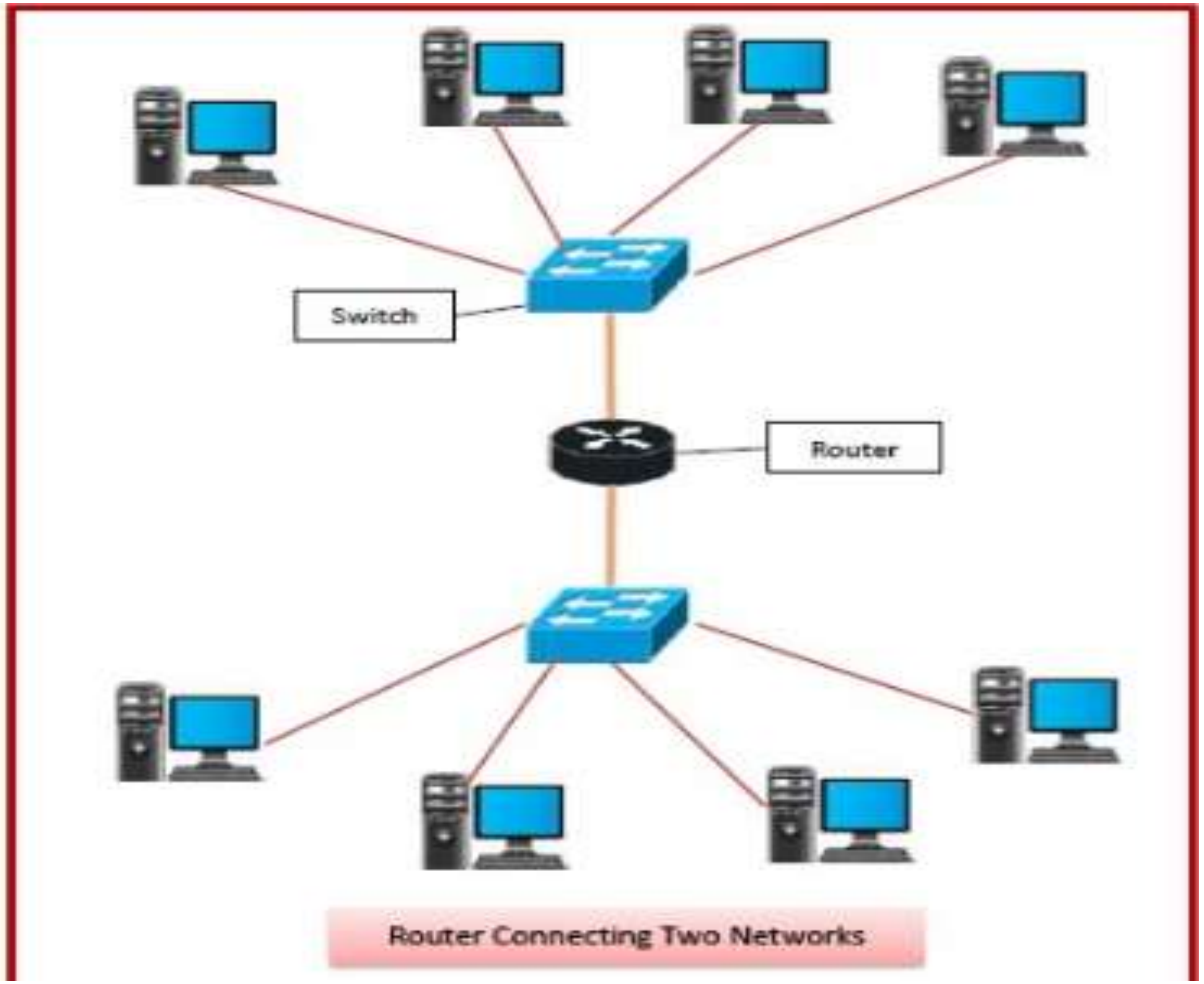
SWITCHES are networking devices operating at layer 2 or a data link layer of the OSI model.
they connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
it supports unicast, multicast as well as broadcast communications.



Multicasting by a Switch

ROUTER

ROUTERS are networking devices operating at layer 3 or a network layer of the OSI model. they are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. when a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



Router Connecting Two Networks

WHAT IS THE **DIFFERENCE** BETWEEN NETWORK SECURITY AND INFORMATION SECURITY?

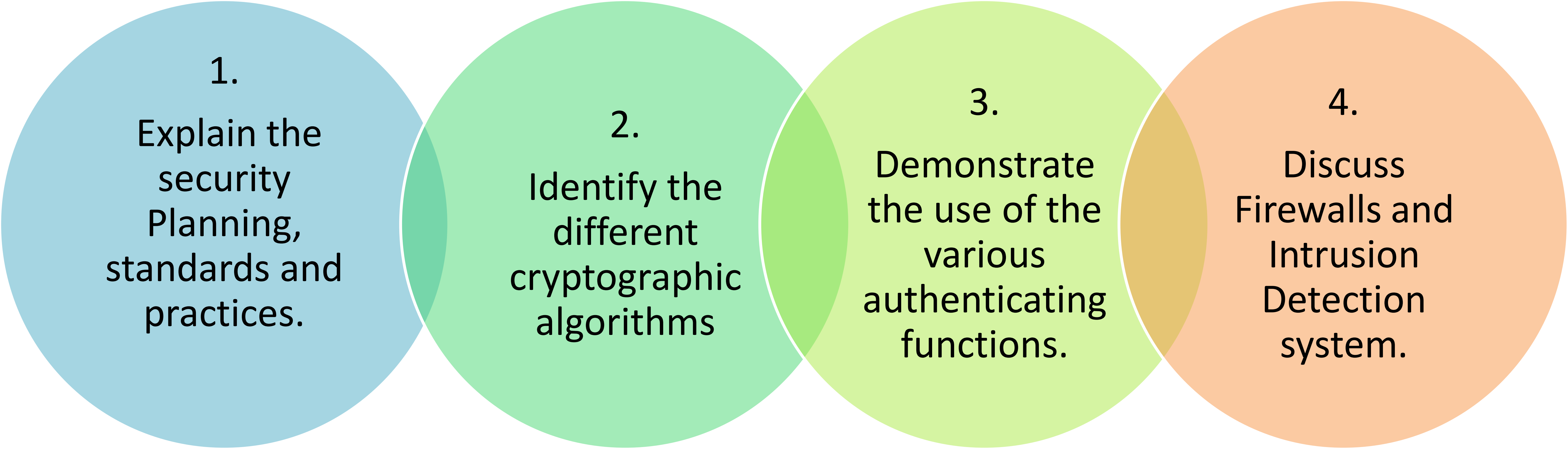
WHAT IS THE **DIFFERENCE** BETWEEN NETWORK SECURITY AND INFORMATION SECURITY?

NETWORK SECURITY INVOLVES METHODS OR PRACTICES USED TO PROTECT A COMPUTER NETWORK FROM UNAUTHORIZED ACCESSES, MISUSES OR MODIFICATIONS

WHEREAS INFORMATION SECURITY PREVENTS UNAUTHORIZED ACCESSES, MISUSES AND MODIFICATIONS TO INFORMATION SYSTEMS.

Course Objectives

Objectives of this course are to :



1. Explain the security Planning, standards and practices.

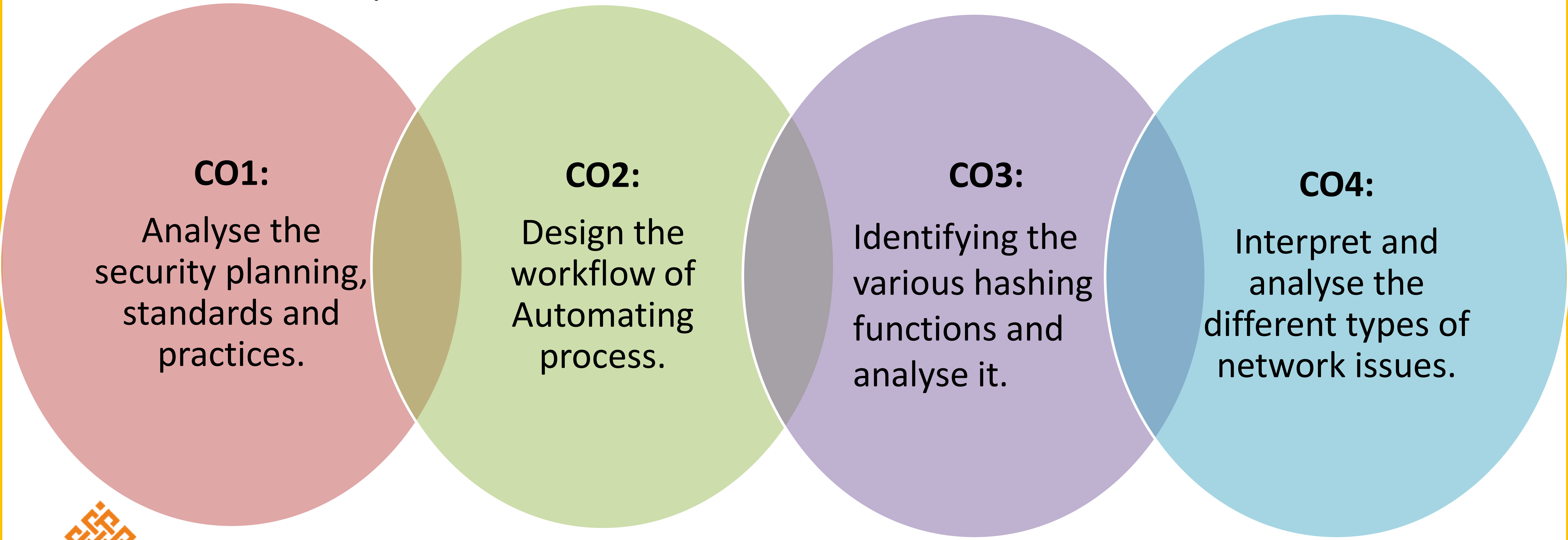
2. Identify the different cryptographic algorithms

3. Demonstrate the use of the various authenticating functions.

4. Discuss Firewalls and Intrusion Detection system.

COURSE OUTCOMES

On successful completion of this course; student shall be able to:



CO1:

Analyse the security planning, standards and practices.

CO2:

Design the workflow of Automating process.

CO3:

Identifying the various hashing functions and analyse it.

CO4:

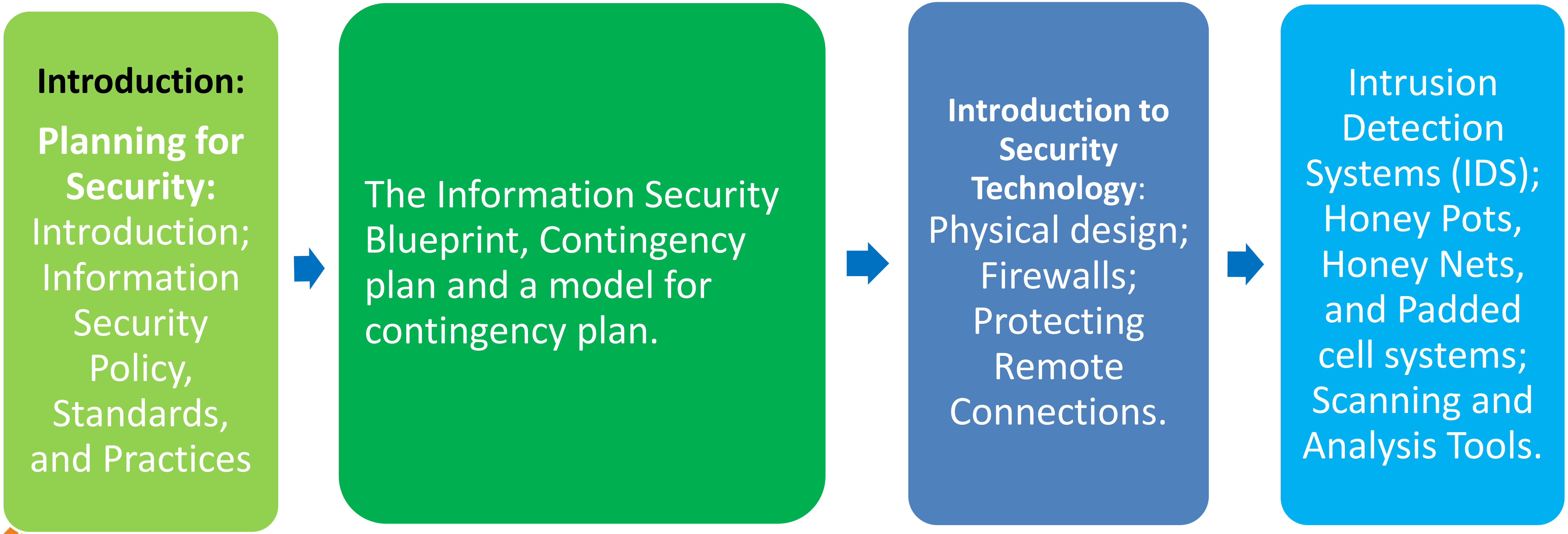
Interpret and analyse the different types of network issues.

Introduction Class

Course Contents

COURSE CONTENTS

UNIT – 1:



Introduction:

Planning for Security: Introduction; Information Security Policy, Standards, and Practices

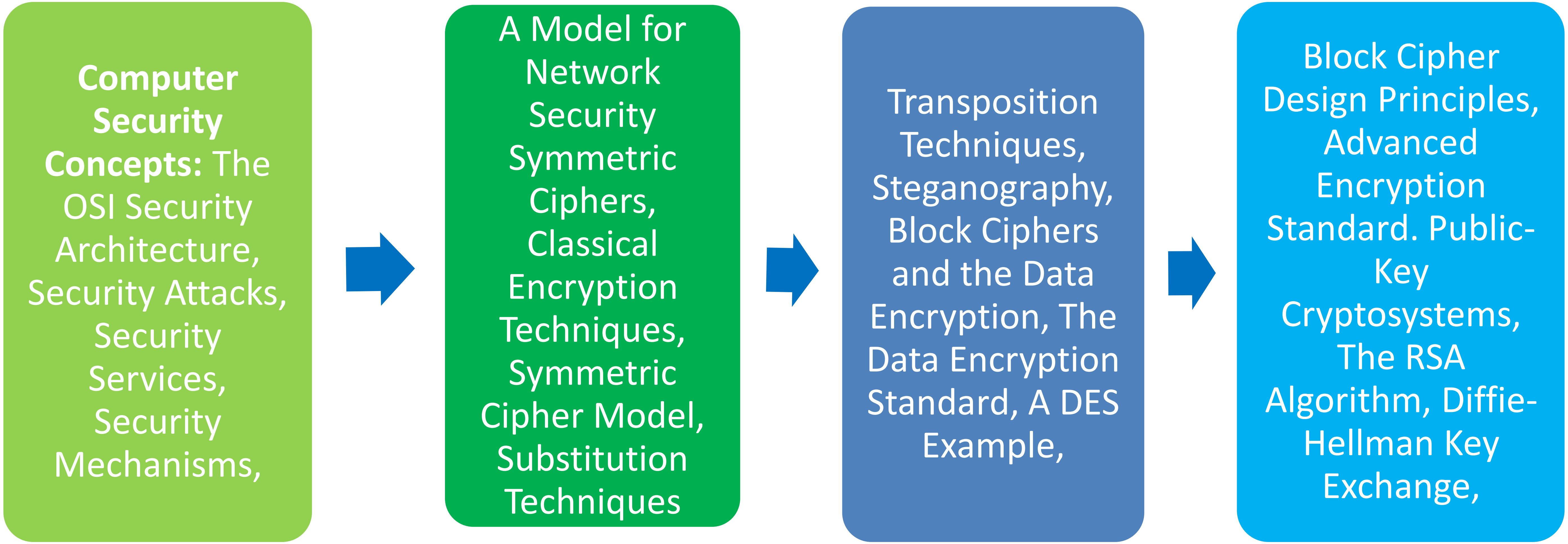
The Information Security Blueprint, Contingency plan and a model for contingency plan.

Introduction to Security Technology: Physical design; Firewalls; Protecting Remote Connections.

Intrusion Detection Systems (IDS); Honey Pots, Honey Nets, and Padded cell systems; Scanning and Analysis Tools.

COURSE CONTENTS

UNIT – 2:



Computer Security Concepts: The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms,

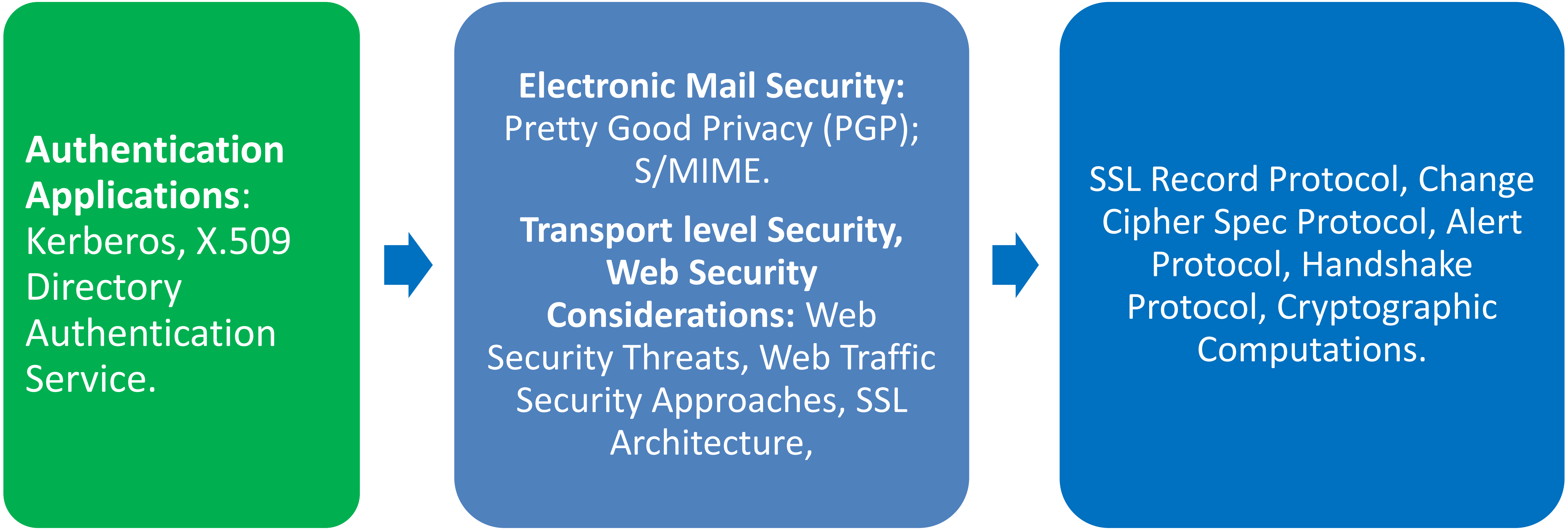
A Model for Network Security Symmetric Ciphers, Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques

Transposition Techniques, Steganography, Block Ciphers and the Data Encryption, The Data Encryption Standard, A DES Example,

Block Cipher Design Principles, Advanced Encryption Standard. Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange,

COURSE CONTENTS

UNIT – 3:



Authentication Applications: Kerberos, X.509 Directory Authentication Service.

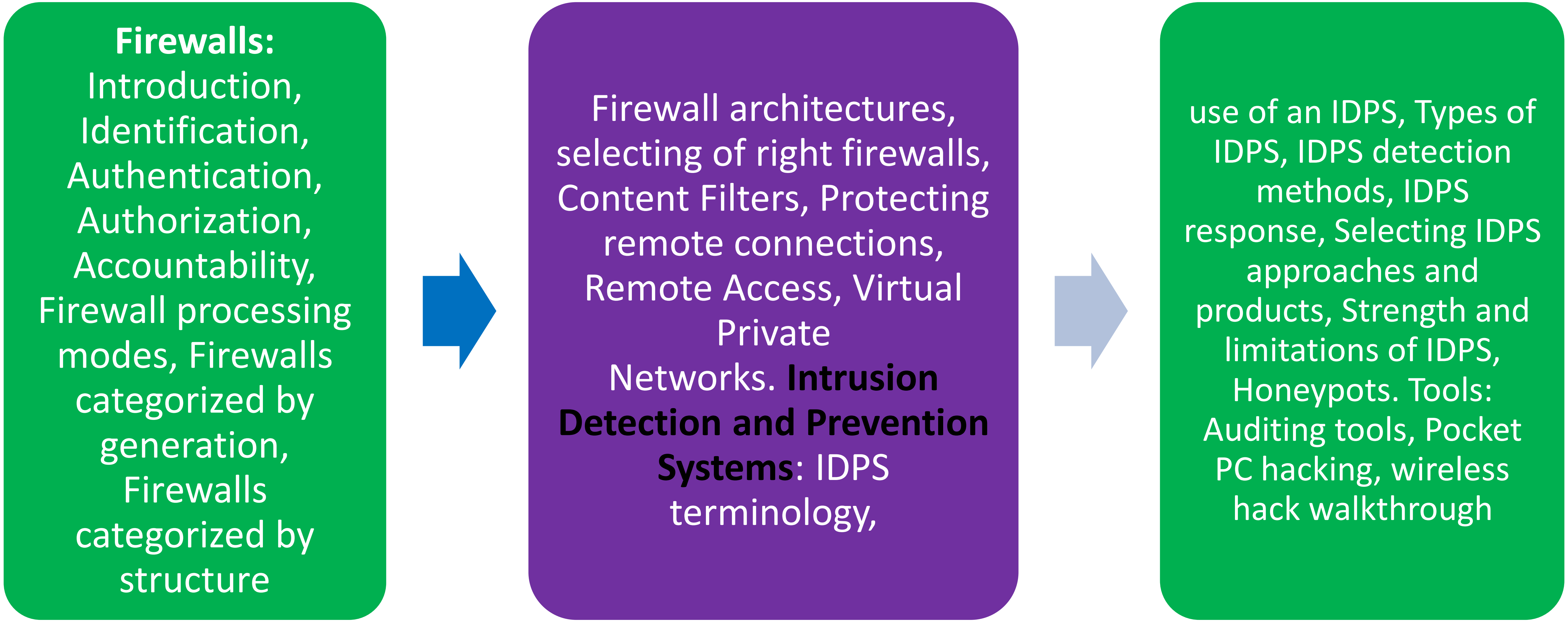
Electronic Mail Security: Pretty Good Privacy (PGP); S/MIME.

Transport level Security, Web Security Considerations: Web Security Threats, Web Traffic Security Approaches, SSL Architecture,

SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol, Cryptographic Computations.

COURSE CONTENTS

UNIT – 4:



Firewalls: Introduction, Identification, Authentication, Authorization, Accountability, Firewall processing modes, Firewalls categorized by generation, Firewalls categorized by structure

Firewall architectures, selecting of right firewalls, Content Filters, Protecting remote connections, Remote Access, Virtual Private Networks. **Intrusion Detection and Prevention Systems**: IDPS terminology,

use of an IDPS, Types of IDPS, IDPS detection methods, IDPS response, Selecting IDPS approaches and products, Strength and limitations of IDPS, Honeypots. Tools: Auditing tools, Pocket PC hacking, wireless hack walkthrough

Introduction Class

Learning Resources

LEARNING RESOURCES

Text books:

1. William Stallings, Cryptography and Network Security, Pearson Publications, 6th edition,20l4.

2. M. E. Whitman and Herbert J. Mattored, Principles of Information Security, Information Security Professional, 4thedition, 20l4.

TEXT BOOKS

Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill, 2007.

Joseph MiggaKizza, Guide to Computer Security, Springer Science & Media Inc., 3rd edition, 20l5

DISCUSSION

5 MINUTES