Revision

Summarise what has been delivered
Specify requirements for preparation of the exam

Topic 1 - Introduction

- **Lecture Contents**
  - Introduction to the Course Unit
  - Introduction to Cybersecurity
- **Exam Requirements**
  - Introduction to Cybersecurity

Topic 2: Security Basics

- **Lecture Contents**
  - Cybersecurity Threats
  - Security Properties
  - Achieving Security
  - Security Models

- **Exam Requirements**
  - All of the above.

Topic 3: Symmetric-key Ciphers

- **Lecture Contents**
  - Symmetric-key ciphers and their applications
  - Block Ciphers (DES, 3DES, AES); Stream Ciphers; Block Ciphers vs Stream Ciphers
  - Use of Block Ciphers in Real World – Modes of Encryptions: ECB (Electronic Code Book) mode; CBC (Cipher Block Chaining) mode; CTR (Counter) mode
- **Exam Requirements**
  - Understand the properties/features, merits and limitations/weaknesses of different types of ciphers and different modes of encryptions
  - Be able to apply them appropriately

Topic 4: Public-key Ciphers

- **Lecture Contents**
  - RSA and DSA algorithms and their applications

- **Exam Requirements**
  - Understand the properties/features, merits and limitations of these two public-key ciphers
  - Be able to apply them appropriately

Topic 5: Cryptographic Checksums and Applications

- **Lecture Contents**
  - Cryptographic Hash Functions
  - Block Cipher based MAC (Message Authentication Code)
  - HMAC (hash function based MAC)
  - Authenticated Encryption, including CCM and GCM

- **Exam Requirements**
  - All of the above except for GCM

Topic 6: Secret Key Management

Lecture Contents

- Key Management Issues
- Symmetric Key Establishment
  - Symmetric Key Agreement: Diffie-Hellman (DH) algorithm/protocol
  - Symmetric Key Distribution: using symmetric key encryption; using public-key encryption

Exam Requirements

- All of the above
- Be able to design and analyse key establishment protocols

Topic 7: PKI

- **Lecture Contents**
  - Public Key Infrastructures (PKI) Overview
  - Digital Certificates
  - Certificate Revocation Lists (CRLs)
  - Certificate Hierarchies

- **Exam Requirements**
  - All of the above
  - Be able to apply PKI properly

Topic 8: Entity Authentication

- **Lecture Contents**
  - Password-based Authentication in General: Unix authN Solution
  - Challenge-Response (C-R) AuthN Protocols
  - Token-based Authentication
  - Enterprise-wide Authentication (SSO – Single Sign On)

- **Exam Requirements**
  - All of the above
  - Be able to design and analyse authentication protocols

Topic 9: VPNs (Virtual Private Networks)

- **Lecture Contents**
  - What is VPN
  - IPSec

- **Exam Requirements**
  - Understand the components of IPSec, the functions they each provide and how the functions are provided
  - Appreciate the design of IPSec and the security threats it is designed to thwart
  - Be able to design and analyse security protocols

Topic 10: Email Security

- **Lecture Contents**
  - PGP
  - S/MIME
- **Exam Requirements**
  - All of the above

Topic 11: Software Security

- **Lecture Contents**
  - Malware types and defence measures
  - Buffer overflow vulnerability and defence measures

- **Exam Requirements**
  - All of the above