

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES**

**COURSE HANDOUT**

**Part A: Content Design**

|  |  |
| --- | --- |
| **Course Title** | Network Security |
| **Course No(s)** | CSI ZG513 / ES ZG513 / SS ZG513 |
| **Credit Units** | 4 (1: Class Room Hours; 2: Students Preparation; 1: Lab Work/Case Studies)  *(1 credit unit translates to approximately 32 hours)* |
| **Course Author** | SANJAY SAHAY |
| **Version No** |  |
| **Date** |  |

**Course Objectives:**

|  |  |
| --- | --- |
| **No** | **Course Objective** |
| **CO1** | Information security is an important area of information technology and this course on Network Security help audience to understand the three important security goals in the networks - Confidentiality, Integrity and Availability and cryptographic techniques to implement these security goals. |
| **CO2** | The course provides a top down approach to explore the security implementations in different network layers - application, transport and network. |
| **CO3** | The course provides a necessary review of mathematical concepts to implement different cryptographic techniques to achieve the network security goals and then provides a deeper dive to the field of cryptography - symmetric and asymmetric key cryptography and methods to implement them. |
| **CO4** | The course consolidates and sums up the learning taking few case studies and examples from latest trends and industry deployments. |

**Text Book(s):**

|  |  |
| --- | --- |
| T1 | Stallings William: Cryptography and Network Security - Principles and Practice, Pearson India, 6th Edition, 2014. |

**Reference Books & other resources:**

|  |  |
| --- | --- |
| R1 | Christof Paar and Jaan Pelzl, Understanding Cryptography: A Textbook for Student and Practitioner, Springer, 1st Edition, 2010 |
| R2 | Forouzan B A, Mukhopadhyay [Debdeep](http://www.flipkart.com/author/debdeep-mukhopadhyay): Cryptography and Network Security, McGraw Hill, 2nd Edition, 2010. |
| R3 | [Schneier](http://www.flipkart.com/author/bruice-schneier) Bruice: [Applied Cryptography: Protocols, Algorithms and Source Code In C](http://www.flipkart.com/applied-cryptography-protocols-algorithms-source-code-c-english-2nd/p/itme52hypcdtgawg?pid=9788126513680&ref=L%3A5350302959759475515&srno=p_1&query=applied+cryptography&otracker=from-search), Wiley India, 2nd Edition, Reprint - 2013. |
| R4 | Kurose James F and Keith W. Ross: Computer Networking: A Top-Down Approach, Pearson India, 5th Edition, 2012. |

**Content Structure**

**M1: Introduction**

|  |  |
| --- | --- |
| Type | Description |
| RL1.1 | RL1.1.1 = Introduction - Information Security Objectives  RL1.1.2 = Standardization in Information Security & OSI Security Architecture |
| RL1.2 | RL1.2.1 = Security Attacks  RL1.2.2 = Security Mechanisms  RL1.2.3 = Security Services |
| RL1.3 | RL1.3.1 = Reference Model for Network Security  RL1.3.2 = Techniques to Implement Network Security - An Introduction |

**M2: Security at the Application Layer**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL2.1 | RL2.1.1 = Overview - Layered Architecture in the service model and Networking Layers  RL2.1.2 = Security at the application layers - objectives, issues and need. |
| RL2.2 | RL2.2.1 = E-Mail System Architecture |
| RL2.3 | RL2.3.1 = Introduction to PGP  RL2.3.2 = Integrity services through PGP  RL2.3.3 = Confidentiality services through PGP  RL2.3.4 = Brief discussion on the Cryptographic Algorithms used in PGP |
| RL2.4 | RL2.4.1 = Introduction to MIME and MIME Headers |
| RL2.5 | RL2.5.1 = Introduction to S/MIME  RL2.5.2 = Security Services through S/MIME  RL2.5.3 = Brief discussion on the Certificates and Cryptographic Algorithms in S/MIME |

**M3: Security at the Transport Layer**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL3.1 | RL3.1.1 = Web Security - threats, challenges and solutions. |
| RL3.2 | RL3.2.1 = Secure Socket Layer (SSL): Introduction  RL3.2.2 = Secure Socket Layer (SSL): Handshake Protocol  RL3.2.3 = Secure Socket Layer (SSL): Change Cipher Spec Protocol  RL3.2.4 = Secure Socket Layer (SSL): Alert Protocol  RL3.2.5 = Secure Socket Layer (SSL): Record Protocol |
| RL3.3 | RL3.3.1 = Secure Shell (SSH) Protocol for Secure Remote Login |

**M4: Security at the Network Layer**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL4.1 | RL4.1.1 = Security Challenges at the Network Layer  RL4.1.2 = IP Security (IPSec) Overview |
| RL4.2 | RL4.2.1 = IP Security - Different Variations  RL4.2.2 = IP Security Architecture  RL4.2.3 = Security Policy - IP Security Packer Processing |

**M5: Classical Encryption Techniques**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL5.1 | RL5.1.1 = Classical Encryption Techniques - Introduction  RL5.1.2 = Cryptanalytic Attacks and Security Criteria |
| RL5.2 | RL5.2.1 = Caesar Cipher - A classical substitution encryption technique  RL5.2.4 = Playfair Cipher  RL5.2.5 = Polyalphabetic Ciphers - Vigenère Cipher  RL5.2.6 = Vernam and One Time Pad Ciphers  RL5.2.7 = Comparison of Classical Substitution Encryption Techniques |
| RL5.3 | RL5.3.1 = Transposition Encryption Technique |

**M6: Mathematics for Symmetric Key Cryptography**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL6.1 | RL6.1.1 = Basic Number Theory  RL6.1.2 = GCD and Euclidean's Theorem  RL6.1.3 = Matrix Mathematics |

**M7: Block Ciphering Techniques**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL7.1 | RL7.1.1 = Block Ciphering  RL7.1.2 = Shannon's Confusion and Diffusion Theory  RL7.1.3 = Feistel Cipher Structure |
| RL7.2 | RL7.2.1 = Data Encryption Standard (DES) |

**M8: Pseudo Random Number (PRN) Generation and Stream Ciphering**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL8.1 | RL8.1.1 = Pseudo Random Number Generation (PRN) |
| RL8.2 | RL8.2.1 = Introduction to Stream Ciphering  RL8.2.2 = Example of Stream Ciphering - RC4 |
| RL8.3 | RL8.3.1 = True Random Number Generation |

**M9: Mathematics for Asymmetric Key Cryptography**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL9.1 | RL9.1.1 = Fermat's Theorem  RL9.1.2 = Euler's Theorem  RL9.1.3 = Primitive Roots |

**M10: Asymmetric (Public) Key Cryptography**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL10.1 | RL10.1.1 = Reference Model for Asymmetric (Public) Key Cryptography |
| RL10.2 | RL10.2.1 = Public Key Cryptosystems - RSA  RL10.2.2 = Public Key Cryptosystems - ElGamal and  RL10.2.3 = Diffie-Hellman Key Exchange Algorithm |

**M11: Data Integrity**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL11.1 | RL11.1.1 = Hash Functions and Properties |
| RL11.2 | RL11.2.1 = Secure Hash Algorithms (SHA)  RL11.2.3 = Message Authentication Codes (MAC) |

**M12: Mutual Trust - Key Management**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL12.1 | RL12.1.1 = Distribution of Symmetric Key |
| RL12.2 | RL12.2.1 = Distribution of Asymmetric (Public) Keys  RL12.2.2 = Basic Concept of Public Key Certificates  RL12.2.3 = X.509 Certificate Structure |

**M13: User Authentication and Digital Signatures**

|  |  |
| --- | --- |
| Type | Description/Plan/Reference |
| RL13.1 | RL13.1.1 = Problem Statement of User Authentication  RL13.1.2 = Kerberos-4.0 with details |
| RL13.2 | RL13.2.1 = Basic Concept of Digital Signatures with one algorithm example |

**Learning Outcomes:**

|  |  |
| --- | --- |
| **No** | **Learning Outcomes** |
| **LO1** | Knowledge to visualize the security goals clearly in the networks. |
| **LO2** | Knowledge of mathematical background and different cryptographic techniques to provides security in the networks. |
| **LO3** | Ability to compare merits and demerits of different Cryptographic techniques and take decisions while securing a network. |
| **LO4** | Ability to analyze a network for security flaws and fool proofing. |

**Part B: Contact Session Plan**

|  |  |
| --- | --- |
| **Academic Term** | Second Semester 2018-2019 |
| **Course Title** | Network Security |
| **Course No** | CSI ZG513 / ES ZG513 / SS ZG513 |
| **Lead Instructor** | Sanjay Sahay |

## Glossary of Terms

1. Contact Hour (CH) stands for a hour long live session with students conducted either in a physical classroom or enabled through technology. In this model of instruction, instructor led sessions will be for 22 CH.
   1. Pre CH = Self Learning done prior to a given contact hour
   2. During CH = Content to be discussed during the contact hour by the course instructor
   3. Post CH = Self Learning done post the contact hour
2. Contact Hour (CS) stands for a two-hour long live session with students conducted either in a physical classroom or enabled through technology. In this model of instruction, instructor led sessions will be for 11 CS.
   1. Pre CS = Self Learning done prior to a given contact session
   2. During CS = Content to be discussed during the contact session by the course instructor
   3. Post CS = Self Learning done post the contact session
3. RL stands for Recorded Lecture or Recorded Lesson. It is presented to the student through an online portal. A given RL unfolds as a sequences of video segments interleaved with exercises
4. SS stands for Self-Study to be done as a study of relevant sections from textbooks and reference books. It could also include study of external resources.
5. LE stands for Lab Exercises
6. HW stands for Home Work.
7. M stands for module. Module is a standalone quantum of designed content. A typical course is delivered using a string of modules. M2 means module 2.

## Teaching Methodology (Flipped Learning Model)

The pedagogy for this course is centered around flipped learning model in which the traditional class-room instruction is replaced with recorded lectures to be watched at home as per the student’s convenience and the erstwhile home-working or tutorials become the focus of classroom contact sessions. Students are expected to finish the home works on time.

## Contact Session Plan

* Each Module (M#) covers an independent topic and module may encompass more than one Recorded Lecture (RL).
* Contact Sessions **(2hrs each week)** are scheduled alternate weeks after the student watches all Recorded Lectures (RLs) of the specified Modules (listed below) during the previous week
* In the flipped learning model, Contact Sessions are meant for in-classroom discussions on cases, tutorials/exercises or responding to student’s questions/clarification--- may encompass more than one Module/RLs/CS topic.
* Contact Session topics listed in course structure (numbered CSx.y) may cover several RLs; and as per the pace of instructor/students’ learning, the instructor may take up more than one CS topic during each of the below sessions.

## Detailed Structure

**Introductory Video/Document:** *<< Introducing the faculty, overview of the course, structure and organization of topics, guidance for navigating the content, and expectations from students>>*

* Each of the sub-modules of **Recorded Lectures** (RLx.y ) shall delivered via **30 – 60mins videos** followed by:
* **Contact session** (CSx.y) of 2Hr each for illustrating the concepts discussed in the videos with exercises, tutorials and discussion on case-problems (wherever appropriate); contact sessions (CS) may cover more than one recorded-lecture (RL) videos.

## Course Contents

**Contact Hour 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-1 |  |
| During CH | CH-1 | * Network Security and OSI Security Architecture * Review of Attacks, Mechanisms and Services, Network Security Model |  |
| Post-CH |  | Uses of Wireshark |  |
| Lab Reference |  |  |  |

**Contact Hour 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-1 |  |
| During CH | CH-2 | * Network Security Model * Techniques to Implement Network Security |  |
| Post-CH |  | Uses of Wireshark |  |
| Lab Reference |  |  |  |

**Contact Hour 3**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-5 |  |
| During CH | CH-3 | * Cryptography, Classical Encryption * Breaking the Cryptosystem |  |
| Post-CH |  | Review the Simple attack to break the cryptosystem |  |
| Lab Reference |  |  |  |

**Contact Hour 4**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-6 |  |
| During CH | CH-4 | * Modular Arithmetic, Groups and Rings * One example each in classical substitutive and transposition ciphering. |  |
| Post-CH |  | Caesar/Affine Cipher –Worksheet and Lab Program |  |
| Lab Reference |  |  |  |

**Contact Hour 5**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-8 |  |
| During CH | CH-5 | * Random numbers, its types and usage. * TRNG, PRNG, CSPRNG * Review of BBS |  |
| Post-CH |  | Find out more on Intel processors that include True RNG |  |
| Lab Reference |  |  |  |

**Contact Hour 6**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-8 |  |
| During CH | CH-6 | * Stream Ciphering * RC4 algorithm * Basic Number Theory |  |
| Post-CH |  | Stream Cipher - RC4 Lab Program – Worksheet. |  |
| Lab Reference |  |  |  |

**Contact Hour 7**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-6 |  |
| During CH | CH-7 | * Extended Euclidean Algorithm * Galois Field |  |
| Post-CH |  | Relevance of Extended Euclidean Algorithm |  |
| Lab Reference |  |  |  |

**Contact Hour 8**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-6 |  |
| During CH | CH-8 | * Polynomial Arithmetic * Block Ciphers |  |
| Post-CH |  | Example of Polynomial Arithmetic |  |
| Lab Reference |  |  |  |

**Contact Hour 9**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-7 |  |
| During CH | CH-9 | * Confusion and Diffusion Theory * AES and its importance in security |  |
| Post-CH |  | Understand the algebra of AES e.g. finding inverse etc. |  |
| Lab Reference |  |  |  |

**Contact Hour 10**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  |  |  |
| During CH | CH-10 | * Efficient implementation of AES. * Modes of Operation and its applications * Multiple Encryption and Meet-in-the Middle Attack |  |
| Post-CH |  | Implementation of AES |  |
| Lab Reference |  |  |  |

**Contact Hour 11: Review**

**Contact Hour 12**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  |  |  |
| During CH | CH-12 | * SHA-1 and SHA-3 * HMAC and CBC-MAC and its Security |  |
| Post-CH |  | Modes of Operations Implementation |  |
| Lab Reference |  |  |  |

**Contact Hour 13**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-11 |  |
| During CH | CH-13 | * Model of Asymmetric Key Cryptography * Factorization and other methods for Public Key Cryptography |  |
| Post-CH |  | CBC-MAC implementation |  |
| Lab Reference |  |  |  |

**Contact Hour 14**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-9, 10 |  |
| During CH | CH-14 | * RSA and OAEP * Diffe-Hellman Key Exchange and its * Security Aspects |  |
| Post-CH |  | Generation of Large Prime Numbers |  |
| Lab Reference |  |  |  |

**Contact Hour 15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-9, 10 |  |
| During CH | CH-15 | * Distribution of Symmetric and Asymmetric Key * Digital Signature: DSA |  |
| Post-CH |  | RSA Lab Programs |  |
| Lab Reference |  |  |  |

**Contact Hour 16**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-12, 13 |  |
| During CH | CH-16 | * X.509 Certificate * Man-in-the Middle Attack |  |
| Post-CH |  | Check a digital certificate while accessing a secure website and compare its structure with X.509 standard |  |
| Lab Reference |  |  |  |

**Contact Hour 17**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-12, 13 |  |
| During CH | CH-17 | * User/Entity Authentication * Kerberos |  |
| Post-CH |  | Authentication with Digital Certificate |  |
| Lab Reference |  |  |  |

**Contact Hour 18**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-2 |  |
| During CH | CH-18 | * Review of PGP - Authentication and Confidentiality. * Review of MIME and S/MIME with a short review of SMTP. |  |
| Post-CH |  | S/MIME in MS-Outlook - worksheet |  |
| Lab Reference |  |  |  |

**Contact Hour 19**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-3 |  |
| During CH | CH-19 | * Review of SSL Protocols. * Review of SSH, its phases and its supported channel types. |  |
| Post-CH |  | SSL Protocol Analysis using Wireshark - worksheet. |  |
| Lab Reference |  |  |  |

**Contact Hour 20**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-3 |  |
| During CH | CH-20 | * Need for IPSec * Details of ESP and brief idea of AH. |  |
| Post-CH |  | SSH Channel Types - Experimentation using PuTTY and XMing - worksheet |  |
| Lab Reference |  |  |  |

**Contact Hour 21**

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Type** | **Description** | **Content Reference** |
| Pre-CH |  | Recorded Lectures for Module-4 |  |
| During CH | CH-21 | * SAD and SPD with inbound/outbound packet processing. * Discussion on the IPSec. |  |
| Post-CH |  | IPSec with Wireshark - Worksheet. |  |
| Lab Reference |  |  |  |

**Contact Hour 22: Review**

Refer Appendix for detailed Course Plan

**Evaluation Scheme**:

Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Name** | **Type** | **Duration** | **Weight** | **Day, Date, Session, Time** |
| EC-1 | Quiz-I/ Assignment-I | Online | - | 5% | February 14 to 28, 2019 |
| Quiz-II | Online | - | 5% | March 14 to 28, 2019 |
| Quiz-III | Online | - | 5% | April 14 to 28, 2019 |
| EC-2 | Mid-Semester Test | Closed Book | 2 hours | 35% | 08/03/2019 (FN)  10 AM – 12 Noon |
| EC-3 | Comprehensive Exam | Open Book | 3 hours | 50% | 03/05/2019 (FN)  9 AM – 12 Noon |

***Note*** *- Evaluation components can be tailored depending on the proposed model.*

## Important Information:

Syllabus for Mid-Semester Test (Closed Book): Topics in CS 1-5.

Syllabus for Comprehensive Exam (Open Book): All topics given in plan of study

Evaluation Guidelines:

1. For Closed Book tests: No books or reference material of any kind will be permitted. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
2. For Open Book exams: Use of prescribed and reference text books, in original (not photocopies) is permitted. Class notes/slides as reference material in filed or bound form is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
3. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam. The genuineness of the reason for absence in the Regular Exam shall be assessed prior to giving permission to appear for the Make-up Exam. Make-Up Test/Exam will be conducted only at selected exam centres on the dates to be announced later.

It shall be the responsibility of the individual student to be regular in maintaining the self-study schedule as given in the course handout, attend the lectures, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout.

**Appendix**

**Course Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Contact Session** | **Pre-contact Session Preparation** | **Post Contact Session Homework** |
| 1 | CS-1 | Recorded Lectures for Module-1 | Uses of Wireshark |
| 2 | CS-2 | Recorded Lectures for Module-1 | Uses of Wireshark |
| 3 | CS-3 | Recorded Lectures for Module-5 | Review the Simple attack to break the cryptosystem |
| 4 | CS-4 | Recorded Lectures for Module-6 | Caesar/Affine Cipher –Worksheet and Lab Program |
| 5 | CS-5 | Recorded Lectures for Module-8 | Find out more on Intel processors that include True RNG |
| 6 | CS-6 | Recorded Lectures for Module-8 | Stream Cipher - RC4 Lab Program – Worksheet. |
| 7 | CS-7 | Recorded Lectures for Module-6 | Relevance of Extended Euclidean Algorithm |
| 8 | CS-8 | Recorded Lectures for Module-6 | Example of Polynomial Arithmetic |
| 9 | CS-9 | Recorded Lectures for Module-7 | Understand the algebra of AES e.g. finding inverse etc. |
| 10 | CS-10 | NA | Implementation of AES |
| 11 | CS-11 | Review Session before Mid-Semester Exams |  |
| 12 | CS-12 | NA | Modes of Operations Implementation |
| 13 | CS-13 | Recorded Lectures for Module-11 | CBC-MAC implementation |
| 14 | CS-14 | Recorded Lectures for Module-9, 10 | Generation of Large Prime Numbers |
| 15 | CS-15 | Recorded Lectures for Module-9, 10 | RSA Lab Programs |
| 16 | CS-16 | Recorded Lectures for Module-12, 13 | Check a digital certificate while accessing a secure website and compare its structure with X.509 standard |
| 17 | CS-17 | Recorded Lectures for Module-12, 13 | Authentication with Digital Certificate |
| 18 | CS-18 | Recorded Lectures for Module-2 | S/MIME in MS-Outlook - worksheet. |
| 19 | CS-19 | Recorded Lectures for Module-3 | SSL Protocol Analysis using Wireshark - worksheet. |
| 20 | CS-20 | Recorded Lectures for Module-3 | SSH Channel Types - Experimentation using PuTTY and XMing - worksheet. |
| 21 | CS-21 | Recorded Lectures for Module-4 | IPSec with Wireshark - Worksheet. |
| 22 | CS-10 | Review Session Before Comprehensive Exams |  |

**Contact Session Details:**

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Contact Session** | **Details need to be covered in the contact session** |
| 1 | CS-1 | * Network Security and OSI Security Architecture * Review of Attacks, Mechanisms and Services, Network Security Model |
| 2 | CS-2 | * Network Security Model * Techniques to Implement Network Security |
| 3 | CS-3 | * Cryptography, Classical Encryption * Breaking the Cryptosystem |
| 4 | CS-4 | * Modular Arithmetic, Groups and Rings * One example each in classical substitutive and transposition cipher. |
| 5 | CS-5 | * Random numbers, its types and usage. * TRNG, PRNG, CSPRNG * Review of BBS |
| 6 | CS-6 | * Stream Ciphering * RC4 algorithm * Basic Number Theory |
| 7 | CS-7 | * Extended Euclidean Algorithm * Galois Field |
| 8 | CS-8 | * Polynomial Arithmetic * Block Ciphers |
| 9 | CS-9 | * Confusion and Diffusion Theory * AES and its importance in security |
| 10 | CS-10 | * Efficient implementation of AES * Modes of Operation and its applications * Multiple Encryption and Meet-in-the Middle Attack |
| 11 | CS-11 | Recapitulation of the all the sessions / problem solving before mid-semester exam. |
| 12 | CS-12 | * SHA-1 and SHA-3 * HMAC and CBC-MAC and its Security |
| 13 | CS-13 | * Model of Asymmetric Key Cryptography * Factorization and other methods for Public Key Cryptography |
| 14 | CS-14 | * RSA and OAEP * Diffe-Hellman Key Exchange and its Security Aspects |
| 15 | CS-15 | * Distribution of Symmetric and Asymmetric Key * Digital Signature: DSA |
| 16 | CS-16 | * X.509 Certificate * Man-in-the Middle Attack |
| 17 | CS-17 | * User/Entity Authentication * Kerberos |
| 18 | CS-18 | * Review of PGP - Authentication and Confidentiality. * Review of MIME and S/MIME with a short review of SMTP. |
| 19 | CS-19 | * Review of SSL Protocols. * Review of SSH, its phases and its supported channel types. |
| 20 | CS-20 | * Need for IPSec * Details of ESP and brief idea of AH. |
| 21 | CS-21 | * SAD and SPD with inbound/outbound packet processing. * Discussion on the IPSec. |
| 22 | CS-22 | Recapitulation of the all the sessions/problem solving before comprehensive exam. |