|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Course Code** | CSU5309 | | | | | | |
| **Level** | 5 | | | | | | |
| **Course Title** | Information Security and Cryptography | | | | | | |
| **Credit value** | 3 | | | | | | |
| **Core/Optional** | Optional | | | | | | |
| **Prerequisites** | (EL/CR in 6 credits from L4 Computer Science courses)  (CSU5304)+(CSU5305) (EL/CR ) and EL/CR in 6 credits from L4 Computer Science courses | | | | | | |
| **Hourly breakdown** | **Theory** | | **Practical**  **hours** | **Independent Learning** | | **Assessments** | **Total hrs.** |
| 24 Sessions X 2  = **48 hrs.** | 6 DS x 3 hrs. = **18 hrs.** | **-** | * Sessions (24x 3)   = 72 hrs.   * Online = 10 hrs.   .  Total = **82 hrs.** | | * Continuous Assessments (CA) : **02 hrs.** | **150 hrs.** |
| **Course Aim/s.** | To gain an understanding of fundamental cryptographic concepts like encryption and signatures and use it to build and analyse security in computers, communications and networks. | | | | | | |
| **PLOs addressed by course** | **PLO1: Knowledge:** Explain the fundamental, principles and broader knowledge pertaining to the chosen science disciplines offered for the degree.  **PLO4: Individual Work, Team Work and Leadership**: Demonstrate the competency in working independently and in groups in addressing issues in multi-disciplinary environments and completing the tasks on time through collaborative learning while exhibiting leadership.  **PLO5: Creativity and Problem Solving:** Identify and analyze problems using quantitative and/or qualitative approaches using scientific methodology to provide valid conclusions.  **PLO8**: **Vision for Life:** Develop the capacity to project for future through identifying self-directed goals and continuously targeting towards them for self-improvement by undertaking further studies.  **PLO9: Lifelong Learning**: Develop the capacity to foresee new trends and their impacts and continuously update knowledge and develop skills willingly to meet those future challenges. | | | | | | |
| **Course Learning Outcomes (CLO)** | At the completion of this course student will be able to;  CLO1: Explain about computer security and security models with security system features. (PLO1, PLO5)  CLO2: Explain about threats and attacks to the systems. (PLO1, PLO5)  CLO3: Learn about network security and security systems with hardware security and devices (PLO1, PLO5)  CLO4: Explain about Cryptography , algorithms (PLO1, PLO5)  CLO5: Understand security applications, protocols, models and standards (PLO1, PLO5)  CLO6**:** Application of security over attacks and threats (PLO4, PLO8 , PLO9) | | | | | | |
| **Content**  **(Main topics, sub topics)** | Introduction to security, Features of security systems, Threats and attacks on security, Computer system security, Network security and Secure networks, Secure computer systems, Introduction to cryptography, Digital signatures, Program level security, OS security principles, exploitations, Security devices: Firewalls, IDS, IPS, etc., Secure designs, Client and server security, Secure applications, Secure Protocols, Kerberos, VPN, L2TP, PPTP, IPSec, SSL, HTTPS, Security standards, Information security models, Access control theories and techniques, Cryptography and related concepts, theories, standards, and methods, Key exchange, digital certificate systems and protocols, Application security, attacks and counter measures | | | | | | |
| **Teaching Learning methods (TL)** | Self-learning/independent learning of self - study (IL)   * Learning the course contents in course materials in print and web-based materials (SS) * Additional reading materials/ recommended reading (RE)   Contact sessions   * Day schools (discussion sessions) (Non-compulsory) | | | | | | |
| **Assessment strategy** | Overall Continuous Assessment Mark (OCAM): 40% | | | | Final Assessment: 60 % | | |
| Details: Continuous Assessment I (CA I) : **01 hr.**  Continuous Assessment II (CA II) : **01 hr.**    OCAM computation:  OCAM= 60% of best CA I/CA II+ 40% of other CA I/CA II | | | | Final Evaluation  Theory: **02 hrs.** | | |
| **Recommended**  **Readings:** | 1. Burnett S, Paine S. 2004. *RSA Security’s guide to Cryptography*. California, USA : McGraw Hill 2. Conklin A, White B G , Cothren C, Williams D, Davis R L. 2004 . *Principles of Computer Security*. 3. California, USA : McGraw Hill 4. Gill P S . 2011. *Cryptography and Network Security*. Delhi, India : MacMillon 5. Gaelli W, Longley D, Shain M. 1994. *Information Security Handbook*. London, UK : MacMillon | | | | | | |