IS-345 & 345L Secure Wireless Communications / Laboratory					
Credit Hours	3-1-4	**Prerequisites**	IS241		
Course Learning Outcomes:					
S No	**CLO**		**Domain**	**Taxonomy Level**	**PLO**
1.	Understand security threats in wireless communication		Cognitive	1	1
2.	Comprehend models, design principles, mechanisms and solutions used in wireless network security to obtain authentication and key transport protocols.		Cognitive	2	2
3.	Acquire practice and analytical skills in information security assessment of technology and methods for wireless communication		Cognitive	3	3
4.	Apply the techniques to analyze the learnt secure wireless issues in test networks		Psychomotor	4	4
Course Content:					
Fundamentals of wireless communications such as modulation schemes, channel access schemes and routing protocols etc. This course also provides an overview of existing and emerging wireless communications technologies along with different protocols and relevant security issues. It covers cellular communications, multiple access technologies, and various wireless networks, including past and future generation networks such as Wi-Fi, Zigbee, Blue tooth, AD-hoc wireless networks, 3G/4G cellular networks. Moreover, the course tackles major issues in wireless communication security such as authentication of wireless nodes and messages, access control, anti-jamming, data integrity, communications confidentiality, integrity of messages and protection against availability attacks etc.					
Teaching Methodology:					
Lectures, Written Assignments, Semester Project, Presentations					
Course Assessment:					
Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam					
Reference Materials:					
1. Chen, Zhang : Wireless network security: Theories and applications, 2013					

2. Frank Gustrau: RF and Microwave Engineering: Fundamentals of Wireless Communications, 1st Edition, 2012
3. Security and Cooperation in Wireless Networks, by Buttyan and Hubaux
4. Guide to Wireless Network Security, by Vacca

In addition there will be lecture notes and selected articles.

IS345L Secure Wireless Communications Laboratory Experiments
Practical handling, assessment/ vulnerability analysis of security of traditional wireless networks using USRP kits including GSM, CDMA/UMTS and LTE
Practical handling and security assessment of WiFi standards IEEE 802.11 a/b/g/n using Kali Linux, Arduino kits
Security assessment and vulnerability analysis of Bluetooth Technology
Wireless communication security deployment using Zigbee technologies
IoT security including Wireless Sensors, RFID, wearable devices etc using Arduino kits, RFID modules
Tools: **USRP Kits, RFIDs, Arduino and Raspberry Pi development boards, Zigbee/ Bluetooth modules etc**