

Branch Name:	Information and Communication Technology
Program Code:	ET208
Course Name:	Information Security Practical (Elective-III)
Course Code:	2ET2080302P
Pre-requisite Course:	Computer Networks

Course Objective:

1. Students will be able to understand basic cryptographic algorithms, message and web authentication and security issues.
2. Ability to identify information system requirements for both of them such as client and server.
3. Ability to understand the current legal issues towards information security.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

LAB/Practical

- 1 Implement Brute-Force Attack (Exhaustive Key Analysis on Caesar Cipher)
- 2 Write a program to implement the Substitution ciphers.
- 3 Write a program to implement the Transposition ciphers.
- 4 Perform various encryption-decryption methods using freeware encryption tool (cryptool).
- 5 Perform the encryption operation for given information using S-DES.
- 6 Implementation of RSA algorithm.
- 7 Implementation of simple stenographic technique.
- 8 Implementation of block ciphers (Blowfish) using library (API)
- 9 To generate a digital certificate.
- 10 Capture and analyze the network traffic using wireshark tool.
- 11 To generate SHA-1 Hash code for given message/file.
- 12 To implement SSL/TLS.
- 13 To demonstrate any advance cryptography.
- 14 Open Experiment (Student have to identify the problem from Research papers from reputed Journals & Conferences and try to implement it-if possible)