FACULTY OF COMPUTER SCIENCE

Master of Computer Application (Sem-IV)

In Effect from Academic Year 2016-17

Subject Code : 1CS2010409	**Subject Title: INFORMATION SECURITY**
Pre-requisite :	Knowledge of Security

Course Objective:

The objectives of the course are to:

- Identify and list various security related terms
- State the importance and identify where they are needed for security processes like authentication, access control, cryptography
- Differentiate between malicious and non-malicious coding
- Identify a countermeasure for a given problem

Teaching Scheme (Hours per week)				**Evaluation Scheme (Marks)**				
				Theory		**Practical**		
Lecture	**Tutorial**	**Practical**	**Credit**	**University Assessment**	**Continuous Assessment**	**University Assessment**	**Continuous Assessment**	**Total**
4	-	3	7	60	40	30	20	150

Subject Contents			
Sr. No	**Topic**	**Total Hours**	**Weight (%)**
1	**Security problem in computing** The meaning of Secure, Attacks, vulnerabilities, threats, control methods opportunities and motive, Security goals and vulnerabilities, Types of computer criminals from armature to career criminals, Defense methods	6	15
2	**Program security & Trusted OS** Secure Programs, Finding faults, unexpected behavior, Types of Flaws, Non malicious program errors, buffer overflow, incomplete mediation, time related errors, combination of non-malicious program flaws What is a trusted system, Military and commercial security policies, models of security, multilevel security?	9	25
3	**Database security and Threats in networks** Integrity requirements, Element integrity, auditability, access control, user authentication, Integrity, confidentiality, availability, Network vulnerabilities, who attacks networks, Reconnaissance, threats in transit, protocol flaws, integrity and confidentiality threats, website and other vulnerabilities, complex attacks	9	25
4	**Administrative Security** Security planning, members, commitment, incident response, business continuity, Risk analysis, organization security policies, characteristics of good policy, examples	8	20
5	**Privacy in computing & Protecting programs and data** Privacy concepts, computer related privacy problems, US and non US privacy policies, Identity theft, authentication and privacy Copy rights, patents, trade secrets, protection of computer objects.	7	15

Course Outcome:

At the end of this course, the student would be able

- To identify the security problem in computing.
- To understand the database security and Threats in networks.
- To choose the best security policies for administrative security.

- To overcome privacy in computing and protecting programs and data.
- To write programs to encrypt, authenticate, communicate securely, use secure hash function for message digest, implement trusted OS and network concepts and managing privacy.

List of References:

1. Security in computing, Charles P, Pfleeger, Shari Lawrence Pfleeger, 4th edition, PHI.
2. Information security fundamentals by Thomas R Peltier, Justine Peltier Johm Blackley, Special Indian Edition, Auerbach.

List of Experiments:

Note: The experiment list provided beneath is for reference only. The course teacher may Change/formulate it as per his/her methodology and requirement.

Sr.No	Practical Experiments
1.	**Part I : Programs related to Message Confidentiality:** 1.1 Implement a program which encrypts a given text message (from keyboard) or from a file. Decrypt the message and display the contents on screen. Observe the contents of plaintext and cipher-text. Also store the decrypted contents in another file. Implement the above program for DES. 3DES and AES. 1.2 Modify the above program 1 using DES to include a routine which intentionally corrupts the cipher text. Now, decrypt the corrupted cipher text and observe the contents of the plaintext and cipher-text. Do the original plaintext and the decrypted cipher-text agree? Repeat the program for 3DES and AES. 1.3 Implement the above program 1 and record the cipher-text generated. Now, using bitwise Operators, change just one bit of the plaintext and again encrypt it. Observe whether the generated cipher-text in second case is slightly different or significantly different from the first case. 1.4. Repeat all above program 1 to 4 for binary data like image file/audio file, etc.
2.	**Part II: Programs related to Message Integrity:** 2.1. Implement a program which applies MD5 on a given text message (from keyboard) or from a file. Display the contents on screen and also store the contents in another file. By observing the output, can you determine the size of MD5 code? Implement the above program for SHA-1 and SHA-512 also. 2.2. Implement the above program 1 for MD5 and record the message digest generated. Now, using bitwise operators, change just one bit of the above plaintext and again apply MD5 on it. Observe whether the generated message digest in second case is slightly different or significantly different from the first case. Repeat this program for SHA-1 and SHA-512. 2.3. Repeat all above program 1 to 2 for binary data like image file/audio file, etc.
3.	**Part III: Programs related to Message Integrity and Authentication:** 3.1. Implement a program which applies HMAC with MD5 on a given text message (from keyboard) or from a file. Display the contents on screen and also store the contents in another file. By observing the output, can you determine the size of this HMAC with MD5 code? Is the size same as using only MD5? Implement the above program for HMAC with SHA-1 and HMAC with SHA-512 also. 3.2. Implement the above program 1 for MD5 and record the message digest generated. Now, using bitwise operators, change just one bit of the above plaintext and again apply MD5 on it. Observe whether the generated message digest in second case is slightly different or significantly different from the first case. Repeat this program for SHA-1 and SHA-512. 3.3. Repeat all above program 1 to 2 for binary data like image file/audio file, etc.