NETWORK AND INFORMATION SECURITY **Course Code : 316317**

Programme Name/s	**: Cloud Computing and Big Data/ Computer Technology/ Computer Engineering/ Computer Science & Engineering/ Computer Hardware & Maintenance/ Computer Science**
Programme Code	**: BD/ CM/ CO/ CW/ HA/ SE**
Semester	**: Sixth**
Course Title	**: NETWORK AND INFORMATION SECURITY**
Course Code	**: 316317**

I. RATIONALE

Network information security is to protect sensitive data and systems within a network from unauthorized access, modification, or disruption by implementing security measures. Students learn confidentiality, integrity, and availability of information, ensuring the smooth operation of critical business functions and minimizing potential damage from cyber threats and also able to implement various computer security policies.

II. INDUSTRY / EMPLOYER EXPECTED OUTCOME

The aim of this course is to help the students to attain the following Industry Identified Outcomes through various teaching learning experiences: Implement policies and guidelines to maintain data security and privacy during data transmission.

III. COURSE LEVEL LEARNING OUTCOMES (COS)

Students will be able to achieve & demonstrate the following COs on completion of course based learning

- CO1 - Identify types of Cyber attacks and threats.
- CO2 - Apply multi-factor user authentication and access control.
- CO3 - Implement encryption/decryption techniques.
- CO4 - Use tools and techniques to prevent cyber attacks.
- CO5 - Apply security on Network and Database.

IV. TEACHING-LEARNING & ASSESSMENT SCHEME

Course Code	Course Title	Abbr	Course Category/s	Learning Scheme					Credits	Assessment Scheme											
				Actual Contact Hrs./Week			SLH	NLH		Paper Duration	Theory				Based on LL & TL				Based on SL		Total Marks
															Practical						
				CL	TL	LL					FA-TH	SA-TH	Total		FA-PR		SA-PR		SLA		
											Max	Max	Max	Min	Max	Min	Max	Min	Max	Min	
316317	NETWORK AND INFORMATION SECURITY	NIS	DSE	3	-	2	1	6	3	3	30	70	100	40	25	10	25#	10	25	10	175

Total IKS Hrs for Sem. : 0 Hrs
Abbreviations: CL- ClassRoom Learning , TL- Tutorial Learning, LL-Laboratory Learning, SLH-Self Learning Hours, NLH-Notional Learning Hours, FA - Formative Assessment, SA -Summative assessment, IKS - Indian Knowledge System, SLA - Self Learning Assessment
Legends: @ Internal Assessment, # External Assessment, *# On Line Examination , @$ Internal Online Examination
Note :

1. FA-TH represents average of two class tests of 30 marks each conducted during the semester.
2. If candidate is not securing minimum passing marks in FA-PR of any course then the candidate shall be declared as "Detained" in that semester.
3. If candidate is not securing minimum passing marks in SLA of any course then the candidate shall be declared as fail and will have to repeat and resubmit SLA work.
4. Notional Learning hours for the semester are (CL+LL+TL+SL)hrs.* 15 Weeks
5. 1 credit is equivalent to 30 Notional hrs.
6. * Self learning hours shall not be reflected in the Time Table.
7. * Self learning includes micro project / assignment / other activities.

V. THEORY LEARNING OUTCOMES AND ALIGNED COURSE CONTENT

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
1	TLO 1.1 Explain the need of information security. TLO 1.2 State criteria for information classification. TLO 1.3 Identify various types of attacks. TLO 1.4 Enlist types of Malware. TLO 1.5 Explain importance of Operating system updates. TLO 1.6 Establish relationship between threat, vulnerability, risks with suitable example.	**Unit - I Introduction to Computer and Information Security** 1.1 Foundations of computer security: Definition and Need of Computer Security, Security Basics: Confidentiality, Integrity, Availability, Accountability, Authentication, Non - repudiation and Reliability 1.2 Information Security Overview: Introduction to information, need and importance of information security, Information classification, Criteria for information classification 1.3 Type of Attacks: Active and Passive attacks, Masquerade Attack, Denial of Service, Backdoors and Trapdoors, Sniffing, phishing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Social Engineering 1.4 Types of Malwares: Virus, Worms, Trojan horse, Spyware, Adware, Ransom ware, Logic Bombs, Rootkits, Key loggers 1.5 Operating system updates: HotFix, Patch, Service Pack 1.6 Threat to security: Introduction to assets, vulnerability, threats, risks, relation between threat, vulnerability, risks	Lecture Using Chalk-Board Presentations

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
2	TLO 2.1 Apply different types of authentication methods. TLO 2.2 Apply various methods to prevent password from attacks. TLO 2.3 Illustrate the given biometric patterns. TLO 2.4 Explain the purpose of authorization. TLO 2.5 Compare DAC, MAC, RBAC and ABAC on the basis of given parameters.	**Unit - II User Authentication and Access Control** 2.1 Identification and Authentication methods: Electronic user authentication, user name and password, multi-factor authentication, token-based authentic 2.2 Password attacks: Guessing password, Piggybacking, Shoulder surfing, Dumpster diving 2.3 Biometrics: Finger prints, Hand prints, Retina scan patterns, Voice patterns, Face recognition, Signature and Writing patterns, Keystrokes 2.4 Authorization: Introduction to authorization, goals of authorization 2.5 Access controls: Definition, Authentication mechanism, Access control principles, Access rights and permission Access control policies: Discretionary access control (DAC), Mandatory access control (MAC), Role-based access control(RBAC),Attribute-based access control (ABAC)	Lecture Using Chalk-Board Presentations Video Demonstrations
3	TLO 3.1 Explain the process of encryption and decryption. TLO 3.2 Compare symmetric and asymmetric cryptography on the basis of given parameters. TLO 3.3 Use the substitution techniques on given text. TLO 3.4 Apply the transposition techniques on given text. TLO 3.5 Explain the concept of steganography.	**Unit - III Cryptography** 3.1 Introduction: Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption 3.2 Symmetric and Asymmetric cryptography : Introduction, working, key management, asymmetric cryptography -public key distribution 3.3 Substitution techniques : Caesar cipher, Play fair cipher, Vigenere cipher, Vernam cipher(One-timepad) 3.4 Transposition techniques: Railfence technique, Simple columnar technique 3.5 Steganography: Overview of steganography	Lecture Using Chalk-Board Presentations Video Demonstrations

Sr.No	Theory Learning Outcomes (TLO's)aligned to CO's.	Learning content mapped with Theory Learning Outcomes (TLO's) and CO's.	Suggested Learning Pedagogies.
4	TLO 4.1 Differentiate between hardware and software firewalls. TLO 4.2 Explain various firewall policies. TLO 4.3 Compare DES, AES and RSA algorithms with the given parameters. TLO 4.4 Apply Diffie-Hellman key exchange algorithm on the given text. TLO 4.5 Calculate hash value for given text using hash function algorithm. TLO 4.6 Explain working of Digital Signature.	**Unit - IV Firewall and Encryption Algorithms** 4.1 Firewall: Need of firewall, Types of firewalls: Packet filters, Stateful packet filters, Application gateways, Circuit gateways 4.2 Firewall policies, Configuration, Limitations, Demilitarized zone (DMZ) 4.3 DES (Data Encryption Standard) algorithm, AES (Advanced Encryption Standard) algorithm, RSA (Rivest-Shamir-Adleman) algorithm 4.4 Diffie-Hellman key exchange algorithm, Man-in- middle attack 4.5 Hash Function: Introduction, Features of Hash Functions, MD5 (Message Digest Method 5) and SHA(secure hashing algorithm) algorithm 4.6 Digital Signature: Introduction and working of digital signature, Digital Certificate	Lecture Using Chalk-Board Presentations Video Demonstrations Flipped Classroom
5	TLO 5.1 Compare Network Based and Host-Based IDS. TLO 5.2 Use Kerberos and IP Security Protocols on network security. TLO 5.3 Explain given protocol used for E-mail security. TLO 5.4 Explain need of database security. TLO 5.5 Explain cloud security.	**Unit - V Network and Database Security** 5.1 Intrusion Detection System(IDS):Network-based IDS, Host-based IDS, Honeypots 5.2 Kerberos: Working, Authentication Server (AS), Ticket Granting Service (TGS), Service Server (SS), IP Security: Overview, Authentication Header (AH), Encapsulating Security Payload (ESP) protocols, Transport and tunnel modes 5.3 E-mail security: Simple mail transfer protocol (SMTP), Pretty good privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME), Privacy Enhance Mail (PEM) 5.4 Database Security: Need for database security, SQL injection attack, database encryption 5.5 Cloud security: Essential characteristics, service model, deployment model, cloud specific security threats	Lecture Using Chalk-Board Presentations Video Demonstrations

VI. LABORATORY LEARNING OUTCOME AND ALIGNED PRACTICAL / TUTORIAL EXPERIENCES.

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 1.1 Install Antivirus software on system. LLO 1.2 Apply privacy and security settings to protect operating system.	1	* i.Install and configure Antivirus software on system (Licensed copy) ii. Use privacy and security settings on operating system	2	CO1

NETWORK AND INFORMATION SECURITY **Course Code : 316317**

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs
LLO 2.1 Setup and recover password of computer system.	2	i. Set up single level authentication for computer system ii. Recover the password of computer system using any freeware password recovery tool (Example- John the ripper)	2	CO2
LLO 3.1 Grant read, write and execute permission on file and folder.	3	* i. Grant security to file, folder or application using access permissions and verify it ii. Grant access permission while sharing file and folder	2	CO2
LLO 4.1 Implement password authentication.	4	* Write a utility using C/Shell programming to create strong password authentication (Password should be more than 8 characters, and combination of digits, letters and special characters #, %, &, @)	2	CO2
LLO 5.1 Implement caesar cipher encryption technique.	5	* i. Write a C program to implement caesar cipher technique to perform encryption and decryption of text ii. Apply Caesar cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO3
LLO 6.1 Implement Vernam cipher encryption technique.	6	i. Implement Vernam cipher encryption technique to perform encryption of text using C programming language ii. Apply Vernam cipher technique to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO3
LLO 7.1 Implement railfence encryption technique.	7	Implement railfence encryption technique to perform encryption of text using C programming language	2	CO3
LLO 8.1 Implement simple columnar transposition technique.	8	Implement simple Columnar Transposition encryption technique to perform encryption of text using C programming language	2	CO3
LLO 9.1 Generate Hash Code.	9	* Create and verify Hash Code for given message using any Open-source tool (Example-Cryptool)	2	CO3
LLO 10.1 Implement Diffie-Hellman key exchange encryption technique.	10	i. Write a C program to implement Diffie-Hellman key exchange algorithm to perform encryption of text ii. Use Diffie-Hellman key exchange algorithm to perform encryption and decryption of text using any open-source tool (Example - Cryptool)	2	CO4
LLO 11.1 Implement steganography.	11	* Use Steganography to encode and decode the message using any open-source tool (Example-OpenStego)	2	CO4
LLO 12.1 Generate digital signature.	12	* Create and verify digital signature using any Open-source tool (Example-Cryptool)	2	CO4
LLO 13.1 Generate digital Certificate.	13	Create and verify digital Certificate using any Open-source tool (Example-Cryptool)	2	CO4
LLO 14.1 Configure firewall.	14	Configure firewall settings on any operating system	2	CO4
LLO 15.1 Implement email security.	15	* Send a test mail securely using any open-source tool (Example- Pretty Good Privacy with GnuPG)	2	CO5
LLO 16.1 Use of email tracker pro.	16	Find the origin of email using email tracker pro	2	CO5

Practical / Tutorial / Laboratory Learning Outcome (LLO)	Sr No	Laboratory Experiment / Practical Titles / Tutorial Titles	Number of hrs.	Relevant COs

Note : Out of above suggestive LLOs -

- '*' Marked Practicals (LLOs) Are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

VII. SUGGESTED MICRO PROJECT / ASSIGNMENT/ ACTIVITIES FOR SPECIFIC LEARNING / SKILLS DEVELOPMENT (SELF LEARNING)

Assignment

- Explain the role of digital signatures in verifying authenticity and integrity in a communication system.
- Describe the working of the RSA encryption algorithm showing generation of public and private key.
- Illustrate the use of cryptography in securing email communication.
- Encrypt the message "HELLO" using a Caesar Cipher with a shift of 3.
- Describe algorithms for symmetric and asymmetric cryptography.
- Explain the difference between active and passive security attacks. Provide examples of each.
- Compare and contrast DAC, MAC, and RBAC in terms of security, flexibility, and ease of use.
- Teachers shall give assignments covering all COs.

Micro project

- Implement communication system using steganography. Encrypt audio file and message using any cryptography technique.
- Implement communication system using steganography. Encrypt image and message using any cryptography technique.
- Implement Client/Server communication using cryptography tools in laboratory.
- User A wants to send message to user B securely on network.

i. Select any two techniques to encrypt message.
ii. Implement both the techniques.
iii. Evaluate result of implementation.
iv. Compare complexity of both techniques.
v. Prepare report.

- Prepare admin level report of company who wants to implement allocate fixed system to each employee for authentic access to maintain security.

i. Explain various single level authentication method available to access the system.
ii. Apply the weakness and security threats to this problem.
iii. Suggest multi factor authentication for given problem situation.
iv. Compare impact of single and multi-factor authentication on given situation.

- Create Digital Certificate for your department/personal communication.

Other

- Complete any course related to Network and Information Security on Infosys Springboard, NPTEL.

Note :

- Above is just a suggestive list of microprojects and assignments; faculty must prepare their own bank of microprojects, assignments, and activities in a similar way.
- The faculty must allocate judicial mix of tasks, considering the weaknesses and / strengths of the student in acquiring the desired skills.
- If a microproject is assigned, it is expected to be completed as a group activity.
- SLA marks shall be awarded as per the continuous assessment record.
- For courses with no SLA component the list of suggestive microprojects / assignments/ activities are optional, faculty may encourage students to perform these tasks for enhanced learning experiences.
- If the course does not have associated SLA component, above suggestive listings is applicable to Tutorials and maybe considered for FA-PR evaluations.

VIII. LABORATORY EQUIPMENT / INSTRUMENTS / TOOLS / SOFTWARE REQUIRED

Sr.No	Equipment Name with Broad Specifications	Relevant LLO Number
1	Steganography Tools (Open-source tool)	11
2	E-mail Security Tool (Open-source tool)	15
3	Any freeware password recovery tool	2
4	Any compiler (TurboC/Online 'C' compiler)	4,5,6,7,8,10
5	Encryption and decryption tool (Open-source tool: Cryptool)	5,6,7,8,9,10,12,13
6	Antivirus software (Licensed copy)	All
7	Computer System (Any computer system with basic configuration)	All

IX. SUGGESTED WEIGHTAGE TO LEARNING EFFORTS & ASSESSMENT PURPOSE (Specification Table)

Sr.No	Unit	Unit Title	Aligned COs	Learning Hours	R-Level	U-Level	A-Level	Total Marks
1	I	Introduction to Computer and Information Security	CO1	8	4	6	2	12
2	II	User Authentication and Access Control	CO2	8	4	4	4	12
3	III	Cryptography	CO3	10	2	6	6	14
4	IV	Firewall and Encryption Algorithms	CO4	9	2	4	10	16
5	V	Network and Database Security	CO5	10	4	8	4	16
Grand Total				**45**	**16**	**28**	**26**	**70**

X. ASSESSMENT METHODOLOGIES/TOOLS

Formative assessment (Assessment for Learning)

- Continuous assessment based on process and product related performance indicators Each practical will be assessed considering

60% weightage to process
40% weightage to product
A continuous assessment based on term work

Summative Assessment (Assessment of Learning)

- End semester examination, Lab performance, Viva voce.

XI. SUGGESTED COS - POS MATRIX FORM

Course Outcomes (COs)	Programme Outcomes (POs)							Programme Specific Outcomes* (PSOs)		
	PO-1 Basic and Discipline Specific Knowledge	PO-2 Problem Analysis	PO-3 Design/ Development of Solutions	PO-4 Engineering Tools	PO-5 Engineering Practices for Society, Sustainability and Environment	PO-6 Project Management	PO-7 Life Long Learning	PSO-1	PSO-2	PSO-3
CO1	2	-	-	-	-	1	2			
CO2	2	1	1	1	2	2	2			
CO3	2	2	2	2	2	1	2			
CO4	2	2	2	2	2	1	2			
CO5	2	1	1	2	2	1	3			

Legends :- High:03, Medium:02,Low:01, No Mapping: -
*PSOs are to be formulated at institute level

XII. SUGGESTED LEARNING MATERIALS / BOOKS

Sr.No	Author	Title	Publisher with ISBN Number
1	William Stallings, Lawrie Brown	Computer Security Principles and Practice, Third Edition	Pearson. ISBN-13: 978-0-13-377392-7
2	Atul Kahate	Cryptography and Network security Third Edition	McGraw-Hill; Fourth edition ISBN-13:978- 9353163303
3	Mark Merkow,Jim Breithaupt	Information Security Principles and Practices	Pearson. ISBN 978-81-317-1288-7
4	V. K. Pachghare	Cryptography and Information Security	Prentice Hall India ISBN:978-81-203-5082-3
5	Dieter Gollmann	Computer Security	Wiley publication, New Delhi, ISBN: 978-0-470-74115-3

XIII . LEARNING WEBSITES & PORTALS

Sr.No	Link / Portal	Description
1	https://www.youtube.com/watch?v=NlpnJE0m-NU	Simulation of Intrusion Detection System in MANET using NetSim
2	https://archive.nptel.ac.in/courses/106/106/106106129/	NPTEL course on Introduction to Information Security
3	https://onlinecourses.swayam2.ac.in/cec22_cs15/preview	Swayam course onI nformation Technology
4	https://www.youtube.com/watch?v=T9c5ZpT2FV0	Firewall configuration
5	https://cse29-iiith.vlabs.ac.in/List%20of%20experiments.html	Virtual lab for cryptography
6	https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/	Types of Attacks

NETWORK AND INFORMATION SECURITY **Course Code : 316317**

Sr.No	Link / Portal	Description
7	https://brightsec.com/blog/sql-injection-attack/	SQL injection

Note :

- Teachers are requested to check the creative common license status/financial implications of the suggested online educational resources before use by the students