GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER III

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS-324** Course Title: **Information Security Foundations**
2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **3**
7. Category of Course: **DSE**
8. Pre-requisite: **Fundamental of Computers (TCS 101), Programming for problem solving (TCS 201)**

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Explain symmetric and asymmetric key cryptosystems. CO2: Know the working of cryptography techniques. CO3: Analyze the different types of cryptosystems. CO4: Use cryptographic techniques to implement information security protocols. CO5: Apply cryptographic techniques in different applications. CO6: Develop symmetric and asymmetric key cryptosystems.

10. **Details of the Course:**

Sl. No.	Contents	Contact Hours
1	**Unit 1:** **Introduction to information security** What is information security, why we need information security, the zero trust model, overview of ethical hacking Protection against- unauthorized modification, unauthorized deletion and unauthorized access, different types of user authentication techniques, access control techniques Pillars of information security - confidentiality, availability and integrity Steps to fix a cybercrime - Identify cyber threats, analyze and evaluatethreat, treatment Type of hackers - white hat, grey hat, black hat Penetration testing and its phases - reconnaissance, scanning, gaining access, maintaining access, covering tracks. SSL and Transport layer security.	10
2	**Unit 2:** **Basics of cryptography** What is cryptography, what is confidentiality, data integrity, authentication, and nonrepudiation, applications of cryptography - chip based payment cards, digital currencies, computer passwords, digital communications, plaintext, cipher-text, cipher - characteristics of a good cipher, encryption, decryption, Key - significance of key length, symmetric and asymmetric key cryptography, cryptanalysis, OSI security architecture- security attacks, security services, security mechanisms	10
3	**Unit 3:** **Mathematics applied in information security** Concept of divisibility, prime numbers, importance of prime numbers in cryptography, euclid theorem for GCD, extended euclidean algorithm, modular arithmetic, random number generators, deterministic and nondeterministic random number generators, XOR, bit shifts, euler's totient theorem, chinese remainder theorem.	8

4	**Unit 4:** **Symmetric key cryptosystem** Secret Key (symmetric) cryptography - stream and block ciphers, additive and multiplicative ciphers, rail fence technique, playfair cipher, hill cipher, vernam cipher, Vigenère Cipher, RC4 algorithm, DES, 2DES, 2-3DES, 3DES, AES, block cipher modes of operations.	10
5	**Unit 5:** **Asymmetric key cryptosystem, digital signature, and message integrity** RSA, Diffie Hellman key exchange protocol, Elliptic curve cryptography (ECC), ElGamal encryption system. DSS algorithm, RSADS algorithm, ECDSA algorithm, Message integrity, hash functions, MAC functions, HMAC	8
	Total	**46**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
William Stallings	Cryptography and Network Security: Principles and Practice	8th	Pearson Publication, India	2020

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies	Security in Computing”, 5th Edition	**5th**	Prentice Hall, India	**2015**
William Stallings	Network Security Essentials: Applications and Standards	**6th**	Prentice Hall, India	**2016**

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS324.1	Explain symmetric and asymmetric key cryptosystems.	2											1	1	2	1
TCS324.2	Know the working of cryptography techniques.		2	1		1							1	2	1	1
TCS324.3	Analyze the different types of cryptosystems.		2	1		1							1	2	1	1
TCS324.4	Use cryptographic techniques to implement information security protocols.	2			1	2							1	1	2	1
TCS324.5	Apply cryptographic techniques in different applications.		2	1									1	2	1	1
TCS324.6	Develop symmetric and asymmetric key cryptosystems.	2	1									1	2	1	1	1
TCS 324		2.00	1.75	1.00	1.00	1.33	-	-	-	-	-	1.00	1.17	1.50	1.33	1.00

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER IV

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 493** Course Title: **Introduction to cryptography and PKC**
2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **IV**
7. Category of Course: **DSE**
8. Pre-requisite: TCS 332 Fundamental of Information Security and Blockchain.

9. **Course Outcome:**	After completion of the course the students will be able to**:** **CO1** Explain symmetric and asymmetric key cryptosystems. **CO2**: Know the working of cryptography techniques. **CO3**: Analyze the different types of cryptosystems. **CO4:** Use cryptographic techniques to implement information security protocols. **CO5:** Apply cryptographic techniques in different applications. **CO6:** Develop symmetric and asymmetric key cryptosystems.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	**Unit-I** **Basics of cryptography** What is cryptography, what is confidentiality, data integrity, authentication,and nonrepudiation, applications of cryptography - chip based payment cards, digital currencies, computer	10

	passwords, digital communications, plaintext, cipher-text, cipher - characteristics of a good cipher, encryption, decryption, Key - significance of key length, symmetric and asymmetric key cryptography, cryptanalysis, OSI security architecture- security attacks, security services, security mechanisms	
2.	**Unit-II** **Mathematics for cryptography** Concept of divisibility, prime numbers, importance of prime numbers in cryptography, euclid theorem for GCD, extended euclidean algorithm, modular arithmetic, random number generators, deterministic and nondeterministic random number generators, XOR, bit shifts, euler's totient theorem, chinese remainder theorem	8
3.	**Unit-III** **Symmetric key cryptosystem** Secret Key (symmetric) cryptography - stream and block ciphers, additive and multiplicative ciphers, rail fence technique, playfair cipher, hill cipher, vernam cipher, Vigenère Cipher, RC4 algorithm, DES, 2DES, 2-3DES, 3DES, AES, block cipher modes of op	10
4.	**Unit-IV** **Asymmetric key cryptosystem** RSA, Diffie Hellman key exchange protocol, Elliptic curve cryptography(ECC), ElGamal encryption system	8
5.	**Unit-V** **Digital signature and message integrity mechanisms** DSS algorithm, RSADS algorithm, ECDSA algorithm, Message integrity, hash functions, MAC functions, HMAC, secure electronic transaction, useof ECDSA in blockchain implementation	10
	TOTAL	**46**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
William Stallings	Cryptography and Network Security: Principles and Practice	**7th**	Pearson publication, India	2016

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
Charles P. PFleeger, Shari Lawrence Pfleeger, Jonathan Margulies	Security in Computing	**5th**	Prentice Hall, India	**2018**
Roger Wottenhofer	Distributed Ledger Technology, The science of Blockchain	**2nd**	Invested Forest Publishing	**2017**

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS493.1	Explain symmetric and asymmetric key cryptosystems.	2						1	2	1	2			2	1	1
TCS493.2	Know the working of cryptography techniques.	2	3		1								2	2	2	3
TCS493.3	Analyze the different types of cryptosystems.	2			1									1	2	3
TCS493.4	Use cryptographic techniques to implement information security protocols.	1	1										1	2	1	1
TCS493.5	Apply cryptographic techniques in different applications.			3		3							2	3	2	2
TCS493.6	Develop symmetric and asymmetric key cryptosystems.			2		3							2	3	2	2
TCS442		1.75	2.00	2.50	1.00	3.00	-	1.00	2.00	1.00	2.00	-	1.75	2.17	1.80	2.00

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER IV

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS426** Course Title: **Information Security and Risk Management**

2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**

3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **3**

6. Semester: **IV**

7. Category of Course: **DSE**

8. Pre-requisite: (TCS **Information Security foundations and programming**

9. **Course Outcome:**	After completion of the course the students will be able to**:** **CO1:** Information Security and Risk Management **CO2**: Information Security and Risk Management **CO3**: Analyze the different types of information security risk management techniques. **CO4:** Use information security risk management techniques to implement informationsystems. **CO5** Apply information security risk management techniques in different applications. **CO6:** Develop information security risk management techniques.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
Unit-I	**Overview of information security and cryptography** What is information security, why we need information security, zero trust model Protection against- unauthorised modification, unauthorised deletion and unauthorised access, different types of user authentication techniques, access control techniques Pillars of information security - confidentiality, availability and integrity What is cryptography, what is confidentiality, data integrity, authentication, and nonrepudiation, applications of cryptography, network security model, plaintext, ciphertext, cipher - characteristics of a good cipher, encryption, decryption, Key - significance of key length, symmetric and asymmetric key cryptography, cryptanalysis, OSI security architecture- security attacks, security services, security mechanisms	**10**
Unit-II	**Risk management and analysis** Overview of risk management, risk identification, identifying the assets, threats and vulnerabilities, risk control strategies, selection of a risk control strategy, planning for risk analysis, performing risk analysis and assessment	8
Unit-III	**Information security planning and implementations** Information security policy, standards and practices, information security blueprint, security education, training and awareness program, project management for information security, technical topics of implementation, nontechnical aspects of implementation	8
Unit-IV	**Disaster recovery and risk monitoring** What is disaster in information security, disaster recovery planning, disaster recovery plan, risk monitoring, requirement of risk monitoring, various phases of risk monitoring	8
Unit-V	**Vulnerabilities and security assessment** What is vulnerability, sources of vulnerabilities, vulnerability assessment, system security policy, building a security policy, security requirement specification, threat identification, threat	8

	models (Dolev Yao model and CK adversary model), threat analysis, vulnerability identification and assessment, security certification, security monitoring and auditing	
	TOTAL	46

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
William Stallings	Cryptography and Network Security: Principles and Practice	**8th**	Pearson publication,India	**2020**
Michael E. Whitman and Herbert J. Mattord	Principles of Information Security, (2e), Thomson Learning	2nd	Cengage Learning, United States	2007
NIIT	Introduction to Information Security Risk Management	2nd	PHI Learning,India	2004
Joseph Migga Kizza	A Guide to Computer Network Security, Springer	3rd	Verlag London Limited, United Kingdom	2013

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies	Security in Computing	5th	Prentice Hall,India	1989

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS426.1	Information Security and Risk Management	1	2		3								2	3	2	1
TCS426.2	Information Security and Risk Management	2		3									1	3	1	3
TCS426.3	Analyze the different types of information security risk management techniques.	2	1	1									2	2	1	1
TCS426.4	Use information security risk management techniques to implement information systems.	1	2	2	2					1	1		1	3	1	2
TCS426.5	Apply information security risk management techniques in different applications.	2	2	3		2		1		2		2		2	2	3
TCS426.6	Develop information security risk management techniques.	1	2	3									3	1	1	2
TCS 426		1.50	1.80	2.40	2.50	2.00	-	1.00	-	1.50	1.00	2.00	1.80	2.33	1.40	1.80

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER V

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS597** Course Title: **Computer System Security**

2. Contact Hours: **L:** **0** **T**: **1** **P**: **2**

3. Examination Duration (Hrs): **Theory** **0** **Practical** **3**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **1**

6. Semester: **V**

7. Category of Course: **DSE**

8. Pre-requisite: TCS-492 Fundamental of Cyber Security

9. **Course Outcome:**	After completion of the course, the students will be able to: CO1: Explain different security threats and attacks. CO2: Know the working of different attacks and security protocols. CO3: Analyze the different security protocols. CO4: Use programming to implement security protocols. CO5: Use programming to implement security protocols. CO6: Develop system security protocols

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	**Introduction to System security:** Control hijacking attacks buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques program analysis (static, concolic and dynamic analysis), Privileges, access	10

	control, and Operating System Security, Exploitation techniques, and Fuzzing	
2	**Software security:** Vulnerabilities, Attacks, and Countermeasures: Privileged programs (Set-UID programs) and vulnerabilities & Privilege Separation, Buffer Overflow vulnerability and defences, Return-to-libc attack, Race, Condition vulnerability and attack, Dirty COW attack, Format String vulnerability and attack, Shellshock attack, Heartbleed attack Interactivity, Annotation, and Arrangement;	10
3	**Web Security:** Same origin Policy, Cross site scripting attack, Cross site request forgery attack, Sql Injection attack, Clickjacking attack, Content Security Policies (CSP) in web, Web Tracking, Session Management and User Authentication, Session Integrity, Https, SSL/TLS, Threat Modelling	10
4	**Smartphone Security**: Android vs. ioS security model, threat models, information tracking, rootkits, Access control in Android operating system, Rooting android devices, Repackaging attacks, Attacks on apps, Whole- disk encryption, hardware protection, Viruses, spywares, and keyloggers and malware detection	9
5	**Hardware and system security**: Meltdown Attack, spectre attack, Authentication and password, Access control concept, Access control list, Capability, Sandboxing, Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks. Issues in Critical Infrastructure and SCADA Security.	6
	Total	**45**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
Charles P Pfleeger and Shari Lawrence Pfleeger	Security in Computing	5th	Pearson/Addison-Wesley, American	2011
Principles and Practice, Book by William Stallings	Cryptography and Network Security	7th	Pearson/Addison-Wesley, American	1998

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
W. Stallings	Network Security Essentials	6th	Prentice Hall, India	2017
Ch. P. Pfleeger, S. L. Pfleeger	*Security in Computing*	4th	Prentice Hall, India	2006

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS597.1	Explain different security threats and attacks.		2		3								1	2	1	1
TCS597.2	Know the working of different attacks and security protocols.	2			1								1	1	2	3
TCS597.3	Analyze the different security protocols.	1	2		3								2	3	2	1
TCS597.4	Use programming to implement security protocols.		1	1	2								2	2	2	1
TCS597.5	Use programming to implement security protocols.	1			2								2	2	1	1
TCS597.6	Develop system security protocols			3	3								3	3	2	1
TCS 542		1.33	1.67	2.00	2.33	-	-	-	-	-	-	-	1.83	2.17	1.67	1.33

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER V

Name of Department: - Computer Science and Engineering

1. Subject Code: **PCS597** Course Title: **Computer System Security Lab**
2. Contact Hours: **L:** **0** **T**: **1** **P**: **2**
3. Examination Duration (Hrs): **Theory** **0** **Practical** **3**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **V**
7. Category of Course: **DSC**
8. Pre-requisite:

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Explain different security threats and attacks CO2: Know the working of different attacks and security protocols CO3: Analyse the different security protocols CO4: Use programming to implement security protocols CO5: Apply security mechanisms to secure various applications CO6:Develop system security protocols

10. **Details of the Course:**

SI. No.	**Contents**	**Contact Hours**
1.	Practical demonstration of buffer overflow vulnerability and attack. Also write down the solutions available to mitigate the buffer overflow attack.	2
2.	Practical demonstration of race condition and vulnerability and attack. What are possible solutions for race condition vulnerability.	2
3.	Practical demonstration of dirty cow vulnerability and attack.	2

4.	Installation and demonstration of burp suite tool.	2
5.	Installation and demonstration of metasploit tool.	2
6.	Practical demonstration of XSS using burp suite tool.	2
7.	Practical demonstration of CSRF vulnerability and attack. What are the possible solutions for CSRF?	2
8.	Practical demonstration of SQL injection vulnerability and attack. What are the possible solutions for SQLi?	2
9.	Installation and demonstration of wireshark tool.	2
10.	Practical demonstration of HTTPs using the wireshark tool.	2
11.	Practical demonstration of ICMP using the wireshark tool.	2
12.	Case study of hardware security and attacks like Stuxnet and hardware trojan.	2
13.	Case study of side channel attack.	2
	Total	26

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Charles P Pfleeger and Shari Lawrence Pfleeger	Security in Computing	5th	Pearson/Addison-Wesley, American	2011
Principles and Practice, Book by William Stallings	Cryptography and Network Security	7th	Pearson/Addison-Wesley, American	1998

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
W. Stallings	Network Security Essentials	6th	Prentice Hall, India	2017
Ch. P. Pfleeger, S. L. Pfleeger	*Security in Computing*	4th	Prentice Hall, India	2006

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
PCS597.1	Explain different security threats and attacks		2	1									1	2	1	1
PCS597.2	Know the working of different attacks and security protocols	2	1		1								1	2	1	1
PCS597.3	Analyse the different security protocols		2		1								1	2	1	1
PCS597.4	Use programming to implement security protocols	2			1									1	2	3
PCS597.5	Apply security mechanisms to secure various applications	1			1	3								1	2	3
PCS597.6	Develop system security protocols		1	3									1	3	1	1
TCS 597		1.67	1.50	2.00	1.00	3.00	-	-	-	-	-	-	1.00	1.83	1.33	1.67

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER V

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS592** Course Title: **Block chain Technology and its application**

2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**

3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **3**

6. Semester: **V**

7. Category of Course: **DSE**

8. Pre-requisite: **TCS 302 Data Structure with C, TCS 332 Fundamental of Information security and Block Chain**

9. **Course Outcome:**	After completion of the course the students will be able to**:** **CO1:** Explain blockchain technology and its immutable property. **CO2:** Know the working of distributed ledger. **CO3:** Analyze the different consensus protocols. **CO4:** Use Ethereum to implement Blockchain. **CO5:** Apply blockchain techniques in different applications. **CO6:**Develop blockchain based frameworks to secure a communication environment

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	Introduction to blockchain- Overview of blockchain, structure of a block, block header, block identifiers: block header hash and block height, genesis block, linking of blocks, merkle trees, and use of merkle root in payment verification	10

2	Application of cryptography to blockchain- Overview of ECDSA, DSA and RSADS, use of hash functions to chain blocks, use of digital signatures to sign transactions	9
3	Distributed ledger- Introduction to distributed systems, fault tolerance and paxos, byzantine agreement, authenticated agreement, eventual consistency & bitcoin consistency- availability and partitions, bitcoin, smart contracts, weak consistency, distributed storage, consistent hashing mechanism	8
4	**Blockchain mining and consensus-**Overview of various consensus algorithms, decentralized consensus, independent verification of transactions, mining nodes, aggregating transactions into blocks, constructing the block header, successfully mining of block, validating a new block, assembling and selecting chains of blocks, consensus attacks**,** DoS attack on blockchain, changing the consensus rules, soft fork signaling with block version	10
5	Ethereum- Differences between ethereum and bitcoin, block format, mining algorithm, proof-of-stake (PoS) algorithm, account management, contracts and transactions, decentralized applications using ethereum proof-of-stake (PoS) algorithm, contracts, and transactions. Applications of blockchain technology- Blockchain in banking and marketing, smart contracts, blockchain of Internet of Things, blockchain in healthcare, Future Research directions of blockchain technology	8
	Total	**45**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
George Icahn	Blockchain: the complete guide to understanding blockchain technology	4th	Prentice Hall, American	2020
Antony lewis	The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them	5th	McGraw Hill Education, American	2018

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Andreas M. Antonopoulos	Mastering Bitcoin: unlocking digital cryptocurrencies	2nd	O'Reilly,United Kingdom	2017
Roger Wattenhofer	Distributed Ledger Technology, The science of the Blockchain	2nd	Inverted Forest Publishing, United State	2017

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS592.1	Explain blockchain technology and its immutable property.	2											1	2	1	1
TCS592.2	Know the working of distributed ledger.		2	1									1	2	1	1
TCS592.3	Analyze the different consensus protocols.	2		3									1	3	1	3
TCS592.4	Use Ethereum to implement Blockchain.		2	1									1	2	1	1
TCS592.5	Apply blockchain techniques in different applications.	2		3					3				1	3	1	3
TCS592.6	Develop blockchain based frameworks to secure a communication environment		2	1									1	2	1	1
TCS592		2.00	2.00	1.80	-	-	-	-	3.00	-	-	-	1.00	2.33	1.00	1.67

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VI

Name of Department: - Computer Science and Engineering

1. Subject Code: **PCS 679** Course Title: **Network and System security**
2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory** **3** **Practical** **0**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **1**
6. Semester: **VI**
7. Category of Course: **DSC**
8. Pre-requisite: (**TCS 591**) **Computer System Security**

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Understand the basics of computer security CO2: Elaborate the cryptographic techniques. CO3: Discuss the transport layer security CO4: Find the pros and cons of various key distribution methods CO5: Analyze the wireless Network security CO6: Find the level of system security

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	**Unit 1:** **Introduction** Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Models for network security, standards.	**9**
2	**Unit 2:** **Cryptography**	**9**

	Symmetric Encryption and Message Confidentiality Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Random and Pseudorandom Numbers, Stream Ciphers and RC4, Cipher Block Modes of Operation. **Public-Key Cryptography and Message Authentication 61** Approaches to Message Authentication, Secure Hash Functions, Message Authentication Codes, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures	
3	**Unit 3:** **Network security Application - I** **Key Distribution and User Authentication** Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption, X.509 Certificates, Public-Key Infrastructure, Federated Identity Management **Transport-Level Security** Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell (SSH)	**10**
4	**Unit 4:** **Network security Application - II** **Wireless Network Security** IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security, Wireless Application Protocol Overview, Wireless Transport Layer Security, WAP End-to-End Security **Electronic Mail Security** Pretty Good Privacy, S/MIME, DomainKeys Identified Mail, **IP Security** IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic Suites	**8**
5	**Unit 5:** **System Security** **Intruders** Intruders, Intrusion Detection, Password Management, **Malicious Software** Types of Malicious Software, Viruses, Virus Countermeasures, Worms, Distributed Denial of Service Attacks. **Firewalls** The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations,	**10**

	Legal and Ethical Aspects Cybercrime and Computer Crime, Intellectual Property, Privacy, Ethical Issues	
	Total	**46**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
W. Stallings	Network Security Essentials	6th	Prentice Hall, India	2017
Ch. P. Pfleeger, S. L. Pfleeger	*Security in Computing*	4th	Prentice Hall, India	2006

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
Charles P Pfleeger and Shari Lawrence Pfleeger	Security in Computing	5th	Pearson/Addison-Wesley, American	2011
Principles and Practice, Book by William Stallings	Cryptography and Network Security	7th	Pearson/Addison-Wesley, American	1998

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS697.1	Understand the basics of computer security	2	1		1								1	2	1	1
TCS697.2	Elaborate the cryptographic techniques.	1	2										1	2	2	1
TCS697.3	Discuss the transport layer security	1	2											2	1	1
TCS697.4	Find the pros and cons of various key distribution methods		1	1									1	1	1	1
TCS697.5	Analyze the wireless Network security		2			2							1	2	1	1
TCS697.6	Find the level of system security		2			2							1	2	1	1
PCS 697		1.33	1.67	1.00	1.00	2.00	-	-	-	-	-	-	1.00	1.83	1.17	1.00

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VI

Name of Department: - Computer Science and Engineering

1. Subject Code: **PCS 697** Course Title: **Network and System Security Lab**
2. Contact Hours: **L: 0** **T**: **1** **P**: **2**
3. Examination Duration (Hrs): **Theory** **0** **Practical** **3**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **VI**
7. Category of Course: **DSC**
8. Pre-requisite: **Java Programming Language (TCS 408), Database Management System (TCS 503)**

9. **Course Outcome:**	After completion of the course the students will be able to: CO1: Explain different threats and attacks on network and system. CO2: Know the working of different cryptographic schemes. CO3: Analyze the security of networks and systems. CO4: Use programming to implement various security algorithms. CO5: Apply security mechanisms to secure networks and systems. CO6: Develop Networks and System Security Protocols.

10. **Details of the Course:**

Sl. No.	Contents	Contact Hours

1	Write down a program for the encryption and decryption procedure of affine cipher scheme.	3
2	Write down a program for the encryption and decryption procedure of hill cipher scheme.	3
3	Write down a program for the encryption and decryption procedure of rail fence technique.	3
4	Write down a program for the encryption and decryption procedure of RSA algorithm.	3
5	Write down a program for the signature generation and verification procedures of RSADS algorithm.	3
6	Write down a program for the signature generation and verification procedures of DSA algorithm.	3
7	Design and implement a secure communication system, in which you have to use symmetric key cryptography for the bulk data encryption. Use the RSA algorithm for the encryption of shared secret key. Use RSADS algorithm for the signature generation and verification. Further use SHA256 algorithm for the calculation of the message digest value.	3
8	Use sample data of network anomalies and attacks, i.e., NSL-KDD and predict about the various possibilities of attacks. You have to try this exercise with the different machine learning algorithms.	3
9	Implement a simple security protocol that does encryption/ decryption using a public key cryptographic algorithm through the scyther tool.	3
10	Implement the following problem using the scyther tool: (i) Sender and receiver use symmetric key cryptography for the bulk data secure exchange. (ii) Use the RSA algorithm for the encryption of shared secret keys. (iv) Use RSADS algorithm for signature generation and verification. (v) Further use SHA256 algorithm for the calculation of the message digest value. (vi) Use various random secret values, pseudo identities and timestamp values to get protection against the MITM attack, impersonation attack and replay attack.	3
	Total	**30**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
W. Stallings	Network Security Essentials	6th	Prentice Hall, American	2003

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
Ch. P. Pfleeger, S. L. Pfleeger	Security in Computing	4th	Prentice Hall, American	2006

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
PCS679.1	Explain different threats and attacks on network and system.	1		2								1	2	3	1	1
PCS679.2	Know the working of different cryptographic schemes.		2									2		2	1	1
PCS679.3	Analyze the security of networks and systems.		2										2	1	2	1
PCS679.4	Use programming to implement various security algorithms.	2			1									1	2	3
PCS679.5	.Apply security mechanisms to secure networks and systems.	2			1									1	1	3
PCS679.6	Develop Networks and System Security Protocols.			3		1							3	3	1	1
PCS 679		1.67	2.00	2.50	1.00	1.00	-	-	-	-	-	1.50	2.33	1.83	1.33	1.67

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VI

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 692** Course Title: **Block chain Platforms**
2. Contact Hours: **L: 3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **VI**
7. Category of Course: **DSE**
8. Pre-requisite: TCS 332 **Fundamental of Information Security and Blockchain,TCS 493 Introduction of Cryptography and PKC, TCS 592 Blockchain technology and its applications**

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Explain blockchain technology and its platforms. CO2: Know the working of blockchain platforms. CO3: Analyze the mechanism of various blockchain platforms. CO4:Use different blockchain platforms to implement blockchain. CO5: Apply security mechanism to secure the networks and system. And blockchain platforms in different applications. CO6: Develop blockchain platforms.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	Blockchain mining - types of blockchain, mechanism of blockchain, verification of transactions, mining nodes, aggregating transactions into blocks, constructing the block header, successfully mining of block, validating a new block, assembling and selecting chains of blocks, consensus attacks	6

2	Consensus algorithms: Details of following consensus algorithms, Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA) Proof-of-Importance (PoI), Proof-of-Capacity (PoC), Proof-of-Burn (PoB), Proof-of-Weight (PoWeight)	8
3	Advanced consensus algorithms: Details of following consensus algorithms, Delegated Proof-of-Stake (DPoS), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Simplified Byzantine Fault Tolerance (SBFT), Delegated Byzantine Fault Tolerance (DBFT)	10
4	Blockchain platforms: Ethereum, Hyperledger Fabric,Multichain,Hydrachain,Ripple,R3 Corda, BigChainDB,Open-chain	16
5	Applications of blockchain platforms: Applications of blockchain platforms in various domain, smart contract, smart cities, smart healthcare system	**6**
	Total	**46**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
George Icahn	Blockchain: the complete guide to understanding blockchain technology	4th	Prentice Hall, American	2020
Antony lewis	The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them	3rd	McGraw Hill Education, American	2020
Imran Bashir	Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained	2nd	Packt Publishing Limited, UK	2018

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
Andreas M. Antonopoulos	Mastering Bitcoin: unlocking digital cryptocurrencies	2nd	O'Reilly,United Kingdom	2017
Roger Wattenhofer	Distributed Ledger Technology, The science of the Blockchain	2nd	Inverted Forest Publishing,United State	2017
Antonopoulos, Andreas M. and Wood, Gavin	Mastering Ethereum	1st	O'Reilly,United Kingdom	2018

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS692.1	Explain blockchain technology and its platforms.	2											1	1	2	1
TCS692.2	Know the working of blockchain platforms.		3										2	3	1	1
TCS692.3	Analyze the mechanism of various blockchain platforms.	2			3								1	1	2	1
TCS692.4	Use different blockchain platforms to implement blockchain.	3											2	1	3	1
TCS692.5	Apply security mechanism to secure the networks and system. And blockchain platforms in different applications.	2	3	1									1	1	2	1
TCS692.6	Develop blockchain platforms.	3		2	3								2	1	3	1
TCS 692		2.40	3.00	1.50	3.00	-	-	-	-	-	-	-	1.50	1.33	2.17	1.00

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 791** Course Title: **Internet Security**

2. Contact Hours: **L: 3** **T**: **1** **P**: **0**

3. Examination Duration (Hrs): **Theory** **3** **Practical** **0**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **3**

6. Semester: **VII**

7. Category of Course: **DSC**

8. Pre-requisite: (**TCS 404) Computer Organization, (TCS 408) Java Programming Language**

9. **Course Outcome:**	After completion of the course, the students will be able to: CO1: Explain the architecture of the Internet. CO2: Know the working of Internet security mechanisms. CO3: Use cryptography to secure various applications. CO4: Analyze various network security mechanisms. CO5: Apply security mechanisms to protect online systems. CO6: Develop Internet security protocols.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	Unit 1: **Introduction and Overview:** Internet Architecture, How the Internet Works (high-leveloverview), IP address.	5
2	Unit 2:	10

	Internet SecurityMechanism: Denial-of-Service, Traceback, DoS Defence, Network Intrusion Detection Systems, Fundamental NIDS Issues,NIDS Evaluation, Scanning (NMAP, Nessus, NetTools, Smart Whois), Anonymity Tor browser	
3	Unit 3: **Cryptography Basics andApplications:** Secret Key encryption, DES, AES, One-way Hash functions, MD5, SHA-1 and SHA-2, collision attacks, Diffie-Hellman Key Exchange, Public-Key Encryption (RSA), Digital Signatures, Public-key Infrastructure (PKI).	10
4	**Unit 4:** **Network SecurityMechanisms:** Ip Tunneling and SSH Tunneling, Virtual Private Networks, Firewalls, Bypassing Firewalls, Transport Layer Security (TLS/SSL), TLS Programming, Packet Sniffer (Wireshark), Man in the middle attack	9
5	**Unit 5:** **Monitoring systems overnetwork**. Malware attacks, Virus, Worms, Trojans horse, ransomware, keylogger, spyware, bot, botnet, botnet detection, and intrusion detection techniques.	8
	Total	**42**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
William Stallings	Cryptography and Network Security	7th	McGraw Hill Education, American	2016
William Cheswick, Steven Bellovin, Aviel Rubin.	Firewalls and Internet Security: Repelling the Wily Hacker (Addison-Wesley Professional Computing Series)	2nd	Prentice Hall, American	2003

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
William Stallings	Network Security Essentials: Applications and Standards	4th	Prentice Hall, American	2011

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS791.1	Explain the architecture of the Internet.		1	3					1			1	1	2	3	1
TCS791.2	Know the working of Internet security mechanisms.		1		2	3					1		1	2	1	1
TCS791.3	Use cryptography to secure various applications.	2		1	1						1		2	3	2	1
TCS791.4	Analyze various network security mechanisms.	2	3		1								2	2	2	3
TCS791.5	Apply security mechanisms to protect online systems.	1	3			3							2	1	1	3
TCS791.6	Develop Internet security protocols.			3	1	1							3	3	1	1
TCS 791		1.67	2.00	2.33	1.25	2.33	-	-	1.00	-	1.00	1.00	1.83	2.17	1.67	1.67

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 788** Course Title: **Information Security and Audit Monitoring**
2. Contact Hours: **L: 3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory 4** **Practical 0**
4. Relative Weight: **CIE 25** **MSE 25** **ESE 50**
5. Credits: **3**
6. Semester: **VII**
7. Category of Course: **DSE**
8. Pre-requisite: **TCS 492 Fundamental of Cyber Security**

9. **Course Outcome:**	After completion of the course the students will be able to**:** **CO1**: Explain information security audit. **CO2**: Know the working of information security audit and monitoring. **CO3**: Analyze the various mechanisms of information security audit. **CO4**: Use information security audit and monitoring to prevent the information securityattacks. **CO5**: Apply information security audit and monitoring in various applications. **CO6**: Develop strategies for information security audit and monitoring.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	**Unit-1** **Overview** What is information security (IS), evaluation of information security, CIA triad, Components of IS, control in IT environment, components of information security management system (ISMS), framework for the development of ISMS, need of information security, threats to information security, risk to information	10

	systems, cybercrimes and attacks, information security policy, security life cycle	
2	**Unit-2** **Risk management and analysis** Overview of risk management, risk identification, identifying the assets, threats and vulnerabilities, risk control strategies, selection of a risk control strategy, planning for risk analysis, performing risk analysis and assessment	8
3	**Unit-3** Security principles, types of information security policies, structure and framework of compressive security policy, policy infrastructure, policy design life cycle and design processes, PDCA model, security policy standards and practices - BS7799, ISO/IEC 17799, ISO 27001. Auditing tools such as ISO 27001 ISMS TOOL KIT, NGS AUDITOR, Windows password auditor, ISO IES 27002 2005 IS AUDIT TOOL	12
4	**Unit-4** **Domains of IT security** Authentication and access control, physical access, Internet access, e-mail, digital signature, outsourcing, software development and acquisition, hardware acquisition, security organization structure.	8
5	**Unit-5** **Auditing and controls** Auditing concepts, information security audit (ISA) need, concept, standards, performance, steps, techniques, methodologies, around and through computer, controls-concept objectives, types, risk, input, process, validation, output, logical access, physical access database, network, environment, BCP, evidence collection, evaluation and reporting methodologies	8
	Total	**46**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
Michael E. Whitman and Herbert J. Mattord	Principles of Information Security	2nd	Thomson Learning, United States	2007
Angel R. Otero	Information Technology Control and Audit	2nd	CRC Press, United States	2018

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
William Stallings	Network Security Essentials: Applications and Standards	6th	Prentice Hall,America	2016

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS788.1	Explain information security audit.	1		2	1	2				1		2	1	1	1	2
TCS788.2	Know the working of information security audit and monitoring.				1					2	2	2	2	3	1	1
TCS788.3	Analyze the various mechanisms of information security audit.	1	3		1	1				1			1	3	2	1
TCS788.4	Use information security audit and monitoring to prevent the information securityattacks.			3		3							1	2	2	1
TCS788.5	Apply information security audit and monitoring in various applications.	1			1	3				1	1	1	2	2	2	1
TCS788.6	Develop strategies for information security audit and monitoring.		3								2	2	3	1	1	1
TCS 788		1.00	3.00	2.50	1.00	2.25	-	-	-	1.25	1.67	1.75	1.67	2.00	1.50	1.17

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 793** Course Title: **Cloud Security**

2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**

3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **3**

6. Semester: **VI**

7. Category of Course: **DSE**

8. Pre-requisite: **TCS351 Fundamental of Cloud Computing and Bigdata**

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Understanding the need of cloud security, cloud security reference models and standards. CO2: Understand security & privacy concepts and various cloud security issues. CO3: Identify threat model and attacks in cloud environment. CO4: Understand advanced security concepts. CO5: Understand and analyze intrusion detection techniques. CO6: Implement some intrusion detection tools.

10. **Details of the Course:**

Sl. No.	Contents	Contact Hours
1	**Unit 1:** **Introduction to Cloud Security** What is Cloud Security?, Motivation for Cloud Security, Reference models and Standards for Security Management, Information Technology Infrastructure Library (ITIL), ISO 27001/27002, CSA Cloud Reference Model with security boundaries, NIST Standards	08

	and Guidelines for Cloud Security, NIST Cloud Computing Security Reference Architecture.	
2	**Unit 2:** **Cloud Security & Privacy: Concepts and Issues** Security Concepts: Confidentiality, Integrity, Authentication, NonRepudiation, Availability, Access control, Defense in depth, Least privilege, Authorization, Cryptography, Auditing, Accountability) , Privacy : What is Privacy ,Key privacy concerns in Cloud ,Security Management in Cloud , Security aspects at different layers Cloud Security Issues: A Brief Discussion - Application-level, Network-level, Virtualization-level (i.e. Multi-Tenancy), Data Storage-level, Hardware-level, Identity Access Management level, Auditing, Governance and Regulatory Compliance, Cloud and CSP Migration, SLA and Trust level issues etc.)	08
3	**Unit 3:** **Threat Model and Virtualization System-Specific Attacks** Threat Model and Virtualization System-Specific Attacks Threat Model and Attack Taxonomy, Virtualization-specific Attacks: VM Escape, Cross-VM Side Channel Attack, Guest hopping, Guest DoS, VM Malware Injection, VM migration attack, VMM DoS, VMM Hyperjacking, VMM Malware Injection, VMM Backdoor	10
4	**Unit 4:** **Advanced Security Concepts** Securing the Cloud , The security boundary ,Security service boundary Security mapping , Securing Data , Brokered cloud storage access , Establishing Identity and Presence ,Identity protocol standards , Windows Azure identity standards , Identity and Access Management: Why IAM, IAM Challenges, Definitions, Architecture &Practice	10
5	**Unit 5:** **Cloud Security Defensive Approaches** Evolution of Cloud-Intrusion Detection System (IDS), Deployment of IDS in Cloud, Intrusion Detection Techniques in Cloud, Brief Discussion on Virtual Machine Introspection and Hypervisor Introspection Techniques	08
	Total	44

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Barrie Sisisky	Cloud Computing Bible	1st	Wiley Publishing	2011
Tim Mather, Subra, Shahed Latif	Cloud Security and Privacy	1st	O'Reilly,United Kingdom	2009
Raj Kumar Buyya,Vecchiola&Selvi	Mastering Cloud Computing	2nd	McGraw Hill Education, American	2013
Vic (J.R.) Winkler	Securing the Cloud	1st	Prentice Hall, American	2011

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
William Stallings	Network Security Essentials: Applications and Standards	6th	Prentice Hall,America	2016

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS793.1	Understanding the need of cloud security, cloud security reference models and standards.	2											2	1	1	1
TCS793.2	Understand security & privacy concepts and various cloud security issues.				2						1			1	1	3
TCS793.3	Identify threat model and attacks in cloud environment.				2									1	2	1
TCS793.4	Understand advanced security concepts.		2		1				2		1		2	1	1	1
TCS793.5	Understand and analyze intrusion detection techniques.		3	1	1	1							1	3	1	2
TCS793.6	Implement some intrusion detection tools.	3	1	1					1				1	1	1	2
TCS793																

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VIII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 893** Course Title: **Privacy and Security in Online social media**
2. Contact Hours: **L: 3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory 4** **Practical 0**
4. Relative Weight: **CIE 25** **MSE 25** **ESE 50**
5. Credits: **3**
6. Semester: **VI**
7. Category of Course: **DSE**
8. Pre-requisite: TCS 693 Full Stack Web Development

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Understand the security and privacy concerns in Online social media. CO2: Develop Secure Web Applications CO3: Understand the Architecture of Web and working with social media APIs. CO4: Perform social media analysis and visualization using various tools and techniques. CO5: Know the various cases and data protection laws. CO6: Analyze the security parameters in social media.

10. **Details of the Course:**

Sl. No.	Contents	Contact Hours
1	**Unit - I** **Understanding Working of Web and Related Technologies** Working with Linux and Python, Understanding Basics of FrontEnd and Backend Technologies (HTML, CSS, JavaScript, Node JS), Understanding the HTTP Methods, Client Server Architecture, Working of DNS, Introduction to Online Social Media (OSM) - Pros and Cons, Introduction to Social Media APIs - Twitter, Facebook	**12**
2	**Unit – II** **Understanding Privacy and Security Concerns in Web** Misinformation on Social Media - Past Examples, Privacy and Social Media, Policing and Social Media, E-Crime and Social Media Social Media Attacks-Phishing, Reconnaissance, Fake Profiles, Social Engineering, Fake News, Profile Compromise Website Security and Threats - Cross-Site Scripting (XSS), SQL injection, Cross-Site Request Forgery (CSRF), Denial of Service (DoS), Clickjacking	**10**
3	**Unit – III** **Online Social Media and Security** How to keep your account secure (Facebook, Google, Twitter, LinkedIn, Instagram) - Two factor Authentication, Creating Strong Passwords Use Social Media for Awareness, Understand the pattern of Fake News on Social Media, Understanding Dark Web and its Role in Security, Anonymous Web Browsing, Proxy Servers	**10**
4	Unit – IV Learning Social Media Analysis on Publicly Available Twitter Data - Creating Twitter Developer Account, Download Twitter Data using API, Social Media Analysis using NLTK, Geo-Location Analysis, Gephi Network Visualization	**10**
5	**Unit – V** Case Studies - Facebook and Cambridge Analytica and The Misuse private data of 50 million Facebook users Data Protection Law - Need of Data Protection Laws, The General Data Protection Regulation (EU), Information Technology Act, 2000 (India)	**8**
	Total	**50**

Text Books:

Authors Name	Title	Edition	Publisher, Country	Year
Michael Cross	Social Media Security: Leveraging Social Networking While Mitigating Risk	1st	Pearson/Addison-Wesley, American	2017
William Stallings	Cryptography and Network Security	7th	McGraw Hill Education, American	2016

Reference Books:

Authors Name	Title	Edition	Publisher, Country	Year
William Cheswick, Steven Bellovin, Aviel Rubin.	Firewalls and Internet Security: Repelling the Wily Hacker (Addison-Wesley Professional Computing Series)	2nd	Prentice Hall, American	2003

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS893.1	Understand the security and privacy concerns in Online social media.	2		2		1							2	3	2	1
TCS893.2	Develop Secure Web Applications		2		1	1					1		1	2	1	1
TCS893.3	Understand the Architecture of Web and working with social media APIs.	1	1	2		1					2	1	2	2	1	1
TCS893.4	Perform social media analysis and visualization using various tools and techniques.	1	2	1		3					2	1	2	2	2	1
TCS893.5	Know the various cases and data protection laws.	1	3	1		3					1		2	3	2	1
TCS893.6	Analyze the security parameters in social media.	1	1	3	3					2	1	2	2	1	3	2
TCS893		1.20	1.80	1.80	2.00	1.80	-	-	-	2.00	1.40	1.33	1.83	2.17	1.83	1.17

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VIII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 894** Course Title: **E-Privacy: Privacy and Trust in Electronic Society**
2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**
3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**
4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**
5. Credits: **3**
6. Semester: **VIII**
7. Category of Course: **DSE**
8. Pre-requisite: TCS 332 Fundamentals of Information Security and Block Chain

9. **Course Outcome:**	After completion of the course the students will be able to**:** CO1: Explain e-privacy and trust. CO2: Know the working of e-privacy mechanisms. CO3: Analyze the various mechanisms of e-privacy. CO4: Use e-privacy and trust to maintain the privacy of an information system. CO5: Apply e-privacy in various applications. CO6: Develop strategies of e-privacy.

10. **Details of the Course:**

Sl. No.	**Contents**	**Contact Hours**
1	**Unit - I** **Overview** e-privacy, information security, CIA triad, vulnerability, threats, attacks, trust, computation of trust, privacy- an issue of global concern, technology and rising concern over privacy, a new theory of privacy	**12**
2	**Unit – II**	**8**

	Privacy theories and reconstructing Methods of conceptualizing, conceptions of privacy, feasibility of privacy conceptualizing, privacy- method, generality, variability and focus	
3	**Unit – III** **Value of privacy** Virtues and vices of privacy, theories of valuation of privacy, social value of privacy, privacy's pluralistic value	**8**
4	Unit – IV **Taxonomy of privacy** Information collection, information processing, information dissemination, invasion.	**8**
5	**Unit – V** **Privacy benefits and future** Nature of privacy problems, privacy and society, privacy and cultural difference, benefits of a pluralistic conception of privacy, future of privacy	**10**
	Total	**46**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Daniel J. Solove	Understanding Privacy	1st	Harvard university press, United States	2008
Peter Carey, Eduardo Ustaran	E-privacy and Online Data Protection	1st	Tottel publishing,United Kingdom	2002
Michael E. Whitman and Herbert J. Mattord	Principles of Information Security	2nd	Thomson Learning, United Kingdom	2007

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul de Hert,	Data Protection and Privacy: The Age of Intelligent Machines	1st	Hart Publishing, United Kingdom	2017

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS894.1	Explain e-privacy and trust.	2	2		1	1				1	1		2	2	2	1
TCS894.2	Know the working of e-privacy mechanisms.	2	2		1	1				1	1		2	2	2	1
TCS894.3	Analyze the various mechanisms of e-privacy.	1		3	1	3				1		1	2	3	2	2
TCS894.4	Use e-privacy and trust to maintain the privacy of an information system.	1	3	1		2						2	1	3	2	1
TCS894.5	Apply e-privacy in various applications.	1		1	2	2				2	2	2	1	2	1	1
TCS894.6	Develop strategies of e-privacy.	1	1	1		3								1	1	2
TCS894		1.33	2.00	1.50	1.25	2.00	-	-	-	1.25	1.33	1.67	1.60	2.17	1.67	1.33

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)

GRAPHIC ERA (DEEMED TO BE UNIVERSITY), DEHRADUN

SEMESTER VIII

Name of Department: - Computer Science and Engineering

1. Subject Code: **TCS 895** Course Title: **Crypto assets and crypto economy.**

2. Contact Hours: **L:** **3** **T**: **1** **P**: **0**

3. Examination Duration (Hrs): **Theory** **4** **Practical** **0**

4. Relative Weight: **CIE** **25** **MSE** **25** **ESE** **50**

5. Credits: **3**

6. Semester: **VIII**

7. Category of Course: **DSE**

8. Pre-requisite: TCS 332 Fundamentals of Information Security and Block Chain

9. **Course Outcome:**	After completion of the course the students will be able to**:** **CO1:** Explain fundamentals of crypto assets and crypto. **CO2:** Know the working mechanism of crypto assets. **CO3:** Analyze the different mechanism of crypto assets and crypto economy. **CO4:** Use blockchain mechanism to maintain crypto assets. **CO5:** Apply crypto assets in crypto economy applications. **CO6:** Develop policies of crypto economy.

10. **Details of the Course:**

Sl. No.	Contents	Contact Hours
1	**Unit 1:** Overview of distributed ledger technology: Details of blockchain, distributed ledger technology, its working mechanism and usability, security of crypto assets	6
2	**Unit 2:** **Overview of crypto assets:** Different types of crypto assets and their use, cryptocurrencies and non- currency assets-tokens and utility tokens, characteristics	8

	of cryptocurrencies- borderless, censorship-free, greater financial control, greater security, lower costs, greater accessibility **Working mechanism of crypto assets:** Mechanism of bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), ripple (XRP), zcash (ZEC), bitcoin cash, Ethereum classic, stellar lumen (XLM)	
3	**Unit 3:** **Overview of crypto economy:** Introduction to crypto economy, past, present, and future of crypto economy, the institutional economics of blockchain, the universal turing institution, the micro foundations of ledgers.	10
4	**Unit 4:** **Advanced topics of crypto economy:** Money, dequity, and the barter economy of the future, supply chains and identity, the V-form organization, and the future of the firm.	10
5	**Unit 5:** **Ethics and issues**: Ethics and issues in crypto economy, capitalism, policy in blockchain era, capitalism after Satoshi.	4
	Total	**46**

Text Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
Chris Berg, Sinclair Davidson, and Jason Potts	Understanding the Blockchain Economy- An Introduction to Institutional Crypto economics	1st	Edward Elgar Publishing,UK	2019
Imran Bashir,” Mastering Blockchain	Distributed Ledger Technology, decentralization, and smart contracts explained	2nd	Packt Publishing Limited, UK	2018

Reference Books:

Authors Name	**Title**	**Edition**	**Publisher, Country**	**Year**
George Icahn	the complete guide to understand the blockchain technology	1st	Prentice Hall, American	2020

Course Articulation Matrix

CO	Statement	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
TCS895.1	Explain fundamentals of crypto assets and crypto.	2	1	1					1					3	1	1
TCS895.2	Know the working mechanism of crypto assets.			2	3	2				2	2	1	2	1	2	3
TCS895.3	Analyze the different mechanism of crypto assets and crypto economy.	1	1	3		2			1		2		1	2	1	1
TCS895.4	Use blockchain mechanism to maintain crypto assets.		2		2	1			2	1	1	1		1	2	1
TCS895.5	Apply crypto assets in crypto economy applications.			3	1	2			1	1	1	1	2	1	3	1
TCS895.6	Develop policies of crypto economy.		2	2	3	3			1	2	1	1		2	2	3
TCS895		1.50	1.67	2.00	2.00	2.00	-	-	1.20	1.50	1.40	1.00	1.67	2.00	2.00	2.00

High correlation (3); Medium correlation (2); Low correlation (1), No correlation (-)