

Information Security					
Credit Hours:	2	Course Code:	COSC-2111	Prerequisites:	None
Course Learning Outcomes (CLOs):					
At the end of the course, the students will be able to:				Domain	BT Level*
1. <i>Explain key concepts of information security such as design principles, cryptography, risk management, and ethics</i>				C	1
2. <i>Discuss legal, ethical, and professional issues in information security</i>				C	2
3. <i>Apply various security and risk management tools for achieving information security and privacy</i>				C	3
4. <i>Identify appropriate techniques to tackle and solve problems in the discipline of information security</i>				C	3
* BT= Bloom’s Taxonomy, C=Cognitive Domain, P=Psychomotor Domain, A=Affective Domain					
#	SDG	Relevant CLOs			
1	SDG 4: Quality Education	CLO 4: Identify appropriate techniques to tackle and solve problems in the discipline of information security			
2	SDG 8: Decent Work and Economic Growth	CLO 2: Discuss legal, ethical, and professional issues in information security			
3	SDG 9: Industry, Innovation and Infrastructure	CLO 3: Apply various security and risk management tools for achieving information security and privacy			
Course Contents:					
Information security foundations, security design principles; security mechanisms, symmetric and asymmetric cryptography, encryption, hash functions, digital signatures, key management, authentication and access control; software security, vulnerabilities and protections, malware, database security; network security, firewalls, intrusion detection; security policies, policy formation and enforcement, risk assessment, cybercrime, law and ethics in information security, privacy and anonymity of data.					
Teaching Methodology:					
Lectures, Written Assignments, Practical labs, Semester Project, Presentations.					
Course Assessment:					
Mid Term Exams, Final Term Exams, Assignments, Quizzes, Project, Presentations, Practical Exam					
Text Books:					
1. Computer Security: Principles and Practice, 3 rd edition by William Stallings 2. Principles of Information Security, 6 th edition by M. Whitman and H. Mattord 3. Computer Security, 3 rd edition by Dieter Gollmann 4. Computer Security Fundamentals, 3 rd edition by William Easttom 5. Official (ISC)2 Guide to the CISSP CBK, 3 rd edition					
Reference Material:					

1. Computer Security: Principles and Practice, 3rd edition by William Stallings
2. Principles of Information Security, 6th edition by M. Whitman and H. Mattord
3. Computer Security, 3rd edition by Dieter Gollmann
4. Computer Security Fundamentals, 3rd edition by William Easttom
5. Official (ISC)2 Guide to the CISSP CBK, 3rd edition

Information Security - Lab

Credit Hours:	1	Course Code:	COSC-2211	Prerequisites:	None
----------------------	---	---------------------	-----------	-----------------------	------

Course Learning Outcomes (CLOs):

At the end of the course, the students will be able to:	Domain	BT Level*
1. Explain key concepts of information security such as design principles, cryptography, risk management, and ethics	C	1
2. Discuss legal, ethical, and professional issues in information security	C	2
3. Apply various security and risk management tools for achieving information security and privacy	C	3
4. Identify appropriate techniques to tackle and solve problems in the discipline of information security	C	3

* BT= Bloom's Taxonomy, C=Cognitive Domain, P=Psychomotor Domain, A=Affective Domain

#	SDG	Relevant CLOs
1	SDG 4: Quality Education	CLO 4: Identify appropriate techniques to tackle and solve problems in the discipline of information security
2	SDG 8: Decent Work and Economic Growth	CLO 2: Discuss legal, ethical, and professional issues in information security
3	SDG 9: Industry, Innovation and Infrastructure	CLO 3: Apply various security and risk management tools for achieving information security and privacy

Course Contents:

Perform Encryption / Decryption using Caesar cipher, play-fair system, Hill cipher Technique, transposition technique and Diffie-Helmen Key exchange, Implement AES, DES algorithm to implementation to encrypt and decrypt the data, Simple RSA algorithm to encrypt and decrypt the data, hashing in MD5, hashing in SHA1, hashing in SHA256, hashing in Whirlpool, encryption/hashing of different algorithm with salt function, Encryption/Decryption using different algorithm with hash function, creating digital signature.

Teaching Methodology:

Lectures, Written Assignments, Practical labs, Semester Project, Presentations.

Course Assessment:

Mid Term Exams, Final Term Exams, Assignments, Quizzes, Project, Presentations, Practical Exam

Text Books:

6. Computer Security: Principles and Practice, 3rd edition by William Stallings
7. Principles of Information Security, 6th edition by M. Whitman and H. Mattord

- | |
|--|
| <ol style="list-style-type: none">8. Computer Security, 3rd edition by Dieter Gollmann9. Computer Security Fundamentals, 3rd edition by William Easttom10. Official (ISC)2 Guide to the CISSP CBK, 3rd edition |
| Reference Material: |
| <ol style="list-style-type: none">11. Computer Security: Principles and Practice, 3rd edition by William Stallings12. Principles of Information Security, 6th edition by M. Whitman and H. Mattord13. Computer Security, 3rd edition by Dieter Gollmann14. Computer Security Fundamentals, 3rd edition by William Easttom15. Official (ISC)2 Guide to the CISSP CBK, 3rd edition |