Course Name	**CRYPTOGRAPHY**	**Course Code**	**COMP 525**		
Credit Hours	3	**Contact Hours**	Lec	Lab	Total
			2	2	4
Offered as	□ University Requirement □ College Requirement ☒ Program Requirement ☒ Core □ Elective □ ITEC ☒ COMP □ CNET				
Level	9	**Prerequisite**	COMP 323		

Course Description:

This course provides an insight of functioning and analysis of various cryptographic algorithms and protocols and their applications. The course covers the following topics: Principles of cryptography, classical ciphers and general cryptanalysis, Symmetric primitives: Modern encryption methods and secure hashing, Public key cryptography: Key exchange, asymmetric encryption and digital signatures, Advanced applications: protocols, key management and special cryptographic services, Throughout the course, commonly used encryption schemes and other services that can be provided by modern cryptography will be discussed.

Upon completion, the student will be able to:

- Explain the concepts and technical terms related to cryptography and cryptanalysis.
- Describe the concepts of message authentication and hash functions to be used in cryptographic applications such as digital signature.
- Explain the differences between the various cryptographic schemes such as symmetric encryption, asymmetric encryption, authentication, key distribution and key management.
- Analyze the security of some simple cryptographic schemes.
- Demonstrate the implementation of simple cryptographic schemes.

Assessment Methods	**Exam-1** ☒	**10%**	**Exam-2** ☒	**10%**	**Assignments** ☒	**10%**
	Mini Project ☒	**10%**	**Lab Exam** ☒	**20%**	**Final Exam** ☒	**40%**

Text Book:

- Stallings, William. “Cryptography and network security: Principles and practice”, Pearson, 7th Edition, ISBN-13: 978-0134444284, 2016.

References:

- Paar, Christof, Pelzl, Jan, “Understanding Cryptography”, 2nd Edition, Springer, ISBN-13: 978-3642041006, 2010.
- Menezes, van Oorschot and Vanstone, “Handbook of Applied Cryptography”, 5th Edition, CRC Press, ISBN: 978-8189836122, 2001.