

## **CSCI 5322 – CRYPTOGRAPHY AND NETWORK SECURITY**

**CREDIT HOURS:** 3

**PREREQUISITES:** Graduate Student status; may not be enrolled in undergraduate courses.

### **CATALOG DESCRIPTION**

Coverage of symmetric and asymmetric cryptography algorithms and their real-world implementation. Analysis of weaknesses and strengths in different cryptographic methods; and understanding the impact they have had on modern communication protocols and network traffic.

### **PURPOSE OF COURSE**

Study the theory behind cryptographic mechanisms, and how they are implemented. Study block and stream ciphers using symmetric keys. Study asymmetric key generation and encryption; and studying the different mechanisms in implementation of public key cryptography. Gain practical experience in using these methods to secure communication across networks.

### **EDUCATIONAL OBJECTIVES**

Upon successful completion of the course, students should be able to:

1. Understand the difference between symmetric and asymmetric cryptography.
2. Generate encryption keys.
3. Recognize different security protocols placed on network traffic.
4. Understand the importance of digital signatures and how they are produced and verified.
5. Describe the types of safety and security risks associated with network infrastructures.
6. Deploy appropriate countermeasures, such as layers, access controls, privileges, intrusion detection, encryption, and coding checklists.

### **COURSE CALENDAR**

This course meets for a minimum of 37.5 lecture contact hours during the semester. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory/programming assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments

or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

<b>CONTENT</b>	<b>Hours</b>
Introduction to Cryptography .....	9
Overview and course introduction	
History of ciphers and semantic security	
Introduction to mathematical ciphers	
Symmetric Cryptography .....	11
Block ciphers	
Stream ciphers	
Key maintenance	
Message integrity	
Known plaintext attacks	
Hashing and collisions	
Asymmetric Cryptography.....	11
Public key infrastructure	
Key generation with RSA	
Different key exchange protocols	
Digital Signatures	
Modern public key problems	
Network Security.....	11
Protocols	
Secure signatures	
Authentication	
Identification	
Key exchange	
Multi party communication	
Exams (plus final) .....	3
	<b>TOTAL 45</b>

## REFERENCES

Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography, 2023

David Wong, Real-World Cryptography. Manning , 2021

Christof Paar and Jan Pelzl, Understanding Cryptography, Springer, 2010