## **CYBR 470: Cryptography (3 credits)**

This course focuses on the study of techniques for secure communication in the presence of adversaries. The course covers topics such as classical ciphers, modern symmetric and asymmetric key cryptographic systems, cryptographic protocols, and cryptanalysis. The course is designed to provide students with an understanding of the principles and techniques for designing and analyzing secure communication systems. *(Prerequisite: MATH 203)*

**Course Learning Outcomes:**

By the end of the course, students will be able to:

A1. Demonstrate a critical understanding of core concepts and theories related to classical and modern cryptographic techniques.

A2. Apply cryptographic protocols and their design principles to ensure secure communication.

B1. Identify potential vulnerabilities through conducting critical cryptanalysis and deciphering of cryptographic systems.

B2. Design secure communication systems that apply cryptographic principles to address real-world security challenges.

B3. Communicate cryptographic concepts and principles effectively, both in written and verbal forms, to various stakeholders.

C1. Operate as a cryptography specialist, making ethical decisions and considering the broader impacts of cryptographic systems in variable contexts.

**Course Learning Materials:**

* W. Stallings, "Cryptography and Network Security: Principles and Practice," 7th ed., Pearson, 2017.
* B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," 2nd ed., Wiley, 1996.
* J. Katz and Y. Lindell, "Introduction to Modern Cryptography," 3rd ed., CRC Press, 2014.

**Course Content:**

1. Introduction to cryptography
2. Classical ciphers and their cryptanalysis
3. Modern symmetric key cryptographic systems
4. Public key cryptography and digital signatures
5. Cryptographic protocols for secure communication
6. Cryptanalysis techniques
7. Cryptography and its applications in cybersecurity.