Course Learning Outcomes

By the end of this course, a student should be able to:

- Compare basic ciphers
- Identify symmetric algorithms
- Identify asymmetric algorithms
- Explain hash algorithms
- Use current and applied algorithms
- Construct a sample Public Key Interchange

Course Outline

1. Historical ciphers and uses of encryption
   1.1 Ceasar
   1.2 Vigenere
   1.3 Enigma and Turing Machine
   1.4 DES
2. Foundational Cipher Concepts
   2.1 Substitution
   2.2 Transposition
   2.3 Mathematical Manipulation
   2.4 Keys
   2.5 Block versus Stream Ciphers
   2.6 Initialization Vectors
3. Symmetric Algorithms
   3.1 Strengths and Weaknesses
   3.2 Keys
   3.3 Modern Uses
   3.4 Current Algorithms
4. Asymmetric Algorithms
   4.1 Strengths and Weaknesses
   4.2 Keys
   4.3 Modern Uses
   4.4 Current Algorithms
5. Hashing Algorithms
   5.1 Strengths and Weaknesses
   5.2 Modern Uses
   5.3 Current Algorithms
6. Public Key Infrastructure
   6.1 Certificates
   6.2 Digital Signatures
   6.3 Non-Repudiation
   6.4 Certificate Authorities
6.5 Registration Authorities
6.6 Key Exchange

7. Cryptologic Attacks
   7.1 Plain Text
   7.2 Collision/Birthday
   7.3 Bit Flipping
   7.4 Brute Force
   7.5 Implementation Flaws