Course Syllabus Part I
CIS 313 Cryptography

3 Credit Hours

Course Description
This course provides an introduction to the fundamental components of encryption. Topics include the history of cryptography, public key and private key systems, hashing, and digital signatures. Topics also include the development of the Advanced Encryption Standard, the use and functionality of Pretty Good Privacy, and the Secure Socket Layer.

Course Prerequisites
None

Course Objectives

Students who successfully complete this course should be able to:
1. Demonstrate an understanding of operations on binary numbering systems.
2. Distinguish between the mechanics of symmetric and asymmetric ciphers.
3. Describe conditions under which symmetric and asymmetric ciphers are implemented.
4. Demonstrate an understanding of the use of hashing routines to ensure integrity of data.
5. Identify applications of cryptographic techniques to ensure confidentiality of data in transit.
6. Explain common cryptographic system vulnerabilities.
7. Analyze emerging cryptographic capabilities and issues.

Grading Scale

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

Topic Outline

I. The use and manipulation of numbering systems
   a. Binary
   b. Decimal
   c. Hexadecimal
II. Symmetric cipher use in cryptography
   a. Historical symmetric key ciphers
   b. Modern symmetric key ciphers

i. Digital Encryption Standard (DES)
ii. 3DES
iii. Advanced Encryption Standard (AES)

III. Asymmetric cipher use in cryptography
a. Diffie-Hellman
b. RSA

IV. Cryptography use for integrity, authentication, and key management
a. Hashing routines
i. MD5
ii. Secure Hash Algorithm (SHA)
iii. Message Authentication Code (MAC)
b. Digital signatures

V. The use of cryptography in network security
a. Secure Socket Layer (SSL)
b. Transport Layer Security (TLS)
c. Pretty Good Privacy (PGP)
d. Secure/Multipurpose Internet Mail Extensions (S/MIME)
e. Internet Protocol Security (IPSEC)

VI. Attacking cryptographic systems
a. Use of cryptanalysis
i. Known plain-text attack
ii. Chosen plain-text attack
iii. Cipher text-only attack
iv. Related-key attack
b. Indirect attacks
i. Password
ii. Related Data
iii. Spyware
iv. Side-channel
c. Backdoors
i. Algorithms
ii. Implementation
iii. Key Management