INSTRUCTOR: Professor B. Gupta

Office: Faner 3044
Office Hours: MWF 1 p.m. – 3 p.m.
Telephone: 453-7194
Email: bidyut@cs.siu.edu
TA: TBA


Prerequisites: CS 220 and MATH 221, or consent from the instructor

Course Outline:

Symmetric Ciphers:
Classical encryption techniques: substitution and transportation techniques.
Block Cipher Techniques
Data Encryption Technique (DES)
Advanced Encryption Standard (AES)
RC4

(Number theory and field theory required to understand AES and RSA techniques will be taught in the class.)

Asymmetric Ciphers:
Principles of Public-Key Cryptosystems
RSA algorithm
Diffie-Hellman Key Exchange algorithm

Cryptographic Hash Functions:
MD5
SHA-1
SHA-512

Message Authentication Codes:
HMAC

RSA and Digital Signature
DSA and Digital Signature
**GRADING:**

- There will be three exams. The exams together will have 60% of the total points. *Distribution of points in the exams will be notified later. Third exam will be held according to University’s final schedule.*

- Three labs will have 30% of the total points. *Distribution of points in the labs will be notified later.*

- Homework has 10% of the total points.

*** Note: *These percentages are tentative. There may be significant changes.*

Grade A ≥ 90%
Grade B ≥ 80% and < 90%
Grade C ≥ 70% and < 80%
Grade D ≥ 60% and < 70%