Course number and name:	**CS 07652: Cryptographic Algorithms**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Ganesh Baliga
Text book, title, author, and year:	William Stallings, *Cryptography and Network Security*, Pearson publishing.

Specific course information

Catalog description: This graduate course examines the advanced topics in the field of cryptography. The course will introduce students to a wide range of topics ranging from mathematical foundations to designing cryptographic algorithms. The topics covered in the course will include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA cryptosystem, ElGamal cryptosystem, elliptic curve cryptosystem, integrity, authentication, cryptographic hash functions, digital signatures, entity authentication, key management, Kerberos, and others.

Prerequisites: CS 07540 Advanced Design and Analysis of Algorithms[1]

Type of Course: ☐ Required ☒ Elective ☐ Selected Elective

Specific goals for the course:

1. Understand fundamental mathematics needed for the study of cryptography and cryptanalysis.

2. Understand state of the art cryptographic techniques for asymmetric and symmetric data encryption and decryption, hashing, digital signatures and digital certificates.

3. Apply the concepts described above to ensure confidentiality, integrity, authenticity and non-repudiation.

Required List of Topics to be covered:

1. Computer security concepts: Confidentiality, integrity, authentication, non-repudiation
2. Mathematics prerequisites
    a. Algorithmic efficiency
    b. Modular arithmetic
    c. GCD and the extended Euclidean algorithm

[1] This course is in the process of being converted to a 600 level course. This pre requisite is part of that conversion.

    d. Prime numbers
        i. Fermat's little theorem
        ii. Euler's totient theorem
        iii. Miller Rabin primality test
    e. Discrete logarithms
    f. Birthday paradox
3. Classical symmetric ciphers
    a. Caesar, Hill and Playfair ciphers
    b. Vigenère cipher
    c. Transposition
4. Basic cryptanalysis techniques
5. Random number generation
    a. True random number generators
    b. Pseudo random number generators
        i. Linear congruential generator
        ii. Blum, Blum and Shub generator
6. Modern symmetric ciphers
    a. Stream and Block ciphers
    b. Linear Feedback Shift registers
    c. Feistel networks
    d. S-Boxes
    e. DES and AES
    f. Block cipher operation modes
7. Asymmetric ciphers
    a. Public key cryptography
    b. Diffie Hellman
    c. RSA
    d. ElGamal
    e. Elliptic curve cryptography
8. Data integrity and Privacy
    a. Hash functions SHA, MD5
    b. MAC/HMAC
    c. Digital signatures
9. Attacks
    a. Birthday attack
    b. Man-in-the-middle attack
    c. Meet-in-the-middle attack
10. Transport layer security
    a. Certificate Authorities
    b. Digital certificates
    c. Key management
    d. TLS
11. Additional topics:
    a. Steganography
    b. Cryptocurrency