Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Third Year Bachelor of Engineering (Computer Engineering)

(In Effect From Academic Year 2019-20)

Subject Code: CE603-N	**Subject Title:** Cryptography and Network Security
Pre-requisite	

Teaching Scheme (Credits and Hours)

Teaching scheme				Total Credit	Evaluation Scheme					
L	T	P	Total		Theory		Mid Sem Exam	CIA	Pract.	Total
Hrs	Hrs	Hrs	Hrs		Hrs	Marks	Marks	Marks	Marks	Marks
03	00	02	05	04	03	70	30	20	30	150

The course is intended to familiarize the student to the domain of information and network security. After introducing the basics of cryptography and security along with the essential mathematical background, the course aims to elaborate the understanding of various cryptographic primitives such as symmetric/asymmetric key encryption, hash, MAC, key management, digital signature etc. Together with the various attacks, the course also includes few modern security protocols. At the end, the course concludes with brief introduction about latest and forthcoming trends in the sphere of security.

Course Objective: This course aims to

- Explain the significance of security in digital communication in today's world
- Teach the mathematical background needed to understand modern cryptography
- Study various cryptographic mechanisms to implement security aspects
- Educate recent security protocols

Outline of the Course:

Sr. No	Title of the Unit	Minimum Hours
1	Introduction	4
2	Symmetric Encryption	6
3	Mathematical Background	7
4	Asymmetric Encryption	7
5	Hash/MAC	6
6	Cryptanalysis	4
7	Security Protocols	7
8	Advanced Topics	7

Total hours (Theory): 48
Total hours (Lab): 32
Total hours: 80

Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Third Year Bachelor of Engineering (Computer Engineering)

(In Effect From Academic Year 2019-20)

Detailed Syllabus

No	Topic	Lecture (Hrs)	Weightage (%)
1	Introduction to cryptography and classical cryptosystem, Security attacks and vulnerabilities, Block cipher, Stream Cipher, Steganography.	4	8
2	Symmetric Encryption: Fiestal Structure. Block Cipher Design Principles. Data Encryption Standard (DES), Triple DES, Modes of Operation. Advanced Encryption Standard (AES)	6	12
3	Mathematical background: Abstract algebra, Number Theory, Modular Arithmetic, Euclidean and Extended Euclidean algorithm, Prime numbers, Fermat and Euler's Theorem. Chinese reminder theorem.	7	15
4	Asymmetric Encryption: Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange, RSA Cryptosystem, ECC.	7	15
5	Hash/MAC: Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security Of Hash Functions And MACs, MD5-Message Digest Algorithm, SHA-Secure Hash Algorithm, Digital Signatures, Digital Signature Standard (DSS).	6	12
6	Cryptanalysis, Time-Memory Trade-off Attack, Differential and Linear Cryptanalysis, Side-channel attack.	4	8
7	Security Protocols: IPSec, SSL, TLS, SET, PGP, SMIME. X.509 Digital Certificates and Kerberos.	7	15
8	Introduction to Advance Topics (*Definitions and basic understanding only*): Identity-based Encryption (IBE), Attribute-based Encryption (ABE). Introduction to Quantum Cryptography, Blockchain, Bitcoin and Cryptocurrency.	7	15
	Total	48	100

Instructional Method and Pedagogy:

- At the start of course, significance of the course, content delivery pattern, and other required details regarding subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, smart boards etc.
- Attendance is compulsory in lecture and laboratory which will be reflected in Continuous Internal Assessment (CIA) component in the examination scheme of the course.
- Internal / Mid-semester examinations shall be conducted for theoretical evaluation.
- Assignments based on the course content will be given to the students and will be evaluated at regular interval evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures. Experiments shall be performed in the laboratory related to course contents.

Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Third Year Bachelor of Engineering (Computer Engineering)

(In Effect From Academic Year 2019-20)

Learning Outcome:

On successful completion of this course, the student should be able to:

- Explain the significance of information security in digital era
- Indentify various threats and vulnerabilities in networking
- Apply various modern algorithms to achieve various security aspects

e-Resources:

- https://nptel.ac.in/courses/106105162/
- http://williamstallings.com/Cryptography/
- http://williamstallings.com/NetworkSecurity/
- https://www.coursera.org/learn/crypto

Reference Books:

1. Cryptography And Network Security Principles And Practice Fourth Edition, William Stallings, Pearson Education
2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall PTR
3. Network Security Essentials: Applications and Standards, by William Stallings, Prentice Hall.
4. Information Security Principles and Practice By Mark Stamp, Willy India Edition
5. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw Hill
6. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press.
7. Cryptography & Network Security, Atul Kahate, McGraw Hill
8. Cryptography & Network Security, V.K. Jain, Khanna Publishing House
9. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India

List of experiments:

No	Name of Experiment
1	Implement the Caesar cipher with variable key
2	Implement the brute-force (exhaustive key search) attack on Caesar cipher
3	Implement simple transposition technique
4	Implement simple permutation technique
5	Implement the rail fence cipher with variable fence
6	Implement 6 x 6 Playfair cipher
7	Implement n x n Hill Cipher
8	Implement Vigenere Cipher
9	Implement the auto-key cipher
10	Implement the vernam cipher
11	Implement the One Time Pad (OTP) cipher
12	Implement the cryptanalysis using frequency analysis
13	Implement Euclidean Algorithm & Advanced Euclidean Algorithm
14	Implement Deffie-Hellman algorithm for key exchange with small number
15	Implement RSA algorithm with small number
16	Study various encryption/decryption tools available online (E.g. www.cryptool.org)