Course code	Course Name	L-T-P Credits	Year of Introduction
CS409	CRYPTOGRAPHY AND NETWORK SECURITY	3-0-0-3	2016

Course Objectives:

- To introduce fundamental concepts of symmetric and asymmetric cipher models.
- To introduce fundamental concepts of authentication.
- To introduce network security and web security protocols.

Syllabus:

Symmetric Cipher Models - Differential and linear Cryptanalysis- Block Cipher Design principles- Primitive operations- Key expansions- Inverse Cipher- Principles of Public key Cryptography Systems - Authentication functions- Message authentication codes- Hash functions- Digital signatures- Authentication protocols- Network security - Web Security - secure Socket Layer and Transport layer Security- Secure electronic transaction –Firewalls.

Expected Outcome:

The Students will be able to :

i. summarize different classical encryption techniques
ii. identify mathematical concepts for different cryptographic algorithms
iii. demonstrate cryptographic algorithms for encryption/key exchange
iv. summarize different authentication and digital signature schemes
v. identify security issues in network, transport and application layers and outline appropriate security protocols

Text Books:

1. Behrouz A. Forouzan, Cryptography and Network Security, Tata McGraw-Hill. 2010
2. William Stallings, Cryptography and Network Security, Pearson Education, 2014

References:

1. B. Schneier , Applied Cryptography, Protocols, Algorithms, and Source Code in C, 2 nd Edn, Wiley, 1995.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, PHI, 2002

Course Plan

Module	Contents	Hours	End Sem. Exam Marks
I	Symmetric Cipher Models- Substitution techniques- Transposition techniques- Rotor machines-Steganography. Simplified DES- Block Cipher principles- The Data Encryption Standard, Strength of DES- Differential and linear Cryptanalysis. Block Cipher Design principles- Block Cipher modes of operations.	7	15 %
II	IDEA: Primitive operations- Key expansions- One round, Odd round, Even Round- Inverse keys for decryption. AES: Basic Structure- Primitive operation- Inverse Cipher- Key Expansion, Rounds, Inverse Rounds. Stream Cipher –RC4.	7	15 %
FIRST INTERNAL EXAM			

III	Public key Cryptography: - Principles of Public key Cryptography Systems, Number theory- Fundamental Theorem of arithmetic, Fermat's Theorem, Euler's Theorem, Euler's Totient Function, Extended Euclid's Algorithm, Modular arithmetic. RSA algorithm- Key Management - Diffie-Hellman Key Exchange, Elliptic curve cryptography	7	15 %
IV	Authentication requirements- Authentication functions- Message authentication codes- Hash functions- SHA -1, MD5, Security of Hash functions and MACs- Authentication protocols-Digital signatures-Digital signature standards.	7	15 %
SECOND INTERNAL EXAM			
V	Network security: Electronic Mail Security: Pretty good privacy- S/MIME. IP Security: Architecture- authentication Header- Encapsulating Security payload- Combining Security associations- Key management.	7	20 %
VI	Web Security: Web Security considerations- secure Socket Layer and Transport layer Security- Secure electronic transaction. Firewalls-Packet filters- Application Level Gateway- Encrypted tunnels.	7	20 %
END SEMESTER EXAM			

Question Paper Pattern (End semester exam)

1. There will be ***FOUR*** parts in the question paper – **A, B, C, D**
2. **Part A**
   a. **Total marks : 40**
   b. ***TEN*** questions, each have **4 marks**, covering **all the SIX modules** (***THREE*** questions from **modules I & II**; ***THREE*** questions from **modules III & IV**; ***FOUR*** questions from **modules V & VI**). ***All*** questions have to be answered.
3. **Part B**
   a. **Total marks : 18**
   b. ***THREE*** questions, each having **9 marks**. One question is from **module I**; one question is from **module II**; one question ***uniformly*** covers **modules I & II**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
4. **Part C**
   a. **Total marks : 18**
   b. ***THREE*** questions, each having **9 marks**. One question is from **module III**; one question is from **module IV**; one question ***uniformly*** covers **modules III & IV**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
5. **Part D**
   a. **Total marks : 24**
   b. ***THREE*** questions, each having **12 marks**. One question is from **module V**; one question is from **module VI**; one question ***uniformly*** covers **modules V & VI**.
   c. ***Any TWO*** questions have to be answered.
   d. Each question can have ***maximum THREE*** subparts.
6. There will be ***AT LEAST* 60%** analytical/numerical questions in all possible combinations of question choices.