Suggested List of Assignments:

1. Design a lexical analyzer for a subset of C language using Lex tool.
2. Design a hand-coded lexical analyzer for a subset of C language, draw the transition diagrams and then implement the lexical analyzer in C language.
3. Design a scientific calculator using Lex & Yacc or PLY or ANTLR tools.
4. Write a code for finding FIRST & FOLLOW of a grammar.
5. Design a SQL parser / html parser.
6. Implement a SLR parser for a given grammar.
7. Implement a static semantics analyzer.
8. Implement an intermediate code generator in three-address code form represented in quadruples.
9. Implement different optimization techniques on intermediate code.

(CT-22003) Cryptography and Network Security

Teaching Scheme	**Examination Scheme**
Lectures: 3 Hrs/ Week	Assignment/Quizzes : 40 marks End Semester Exam: 60 marks

Course Outcomes

Students will be able to:

1. Explain the concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, and digital signatures
2. Apply concepts of finite mathematics and number theory.
3. Demonstrate the understanding of common network vulnerabilities and attacks, defence mechanisms against network attacks, and cryptographic protection mechanisms.
4. Detect possible threats to different defence mechanisms and different ways to protect against these threats

Course Contents

Introduction: Cryptography and modern cryptography, Need of security, Security services, Basic network security terminology, Security attacks, Classical cryptosystems and their cryptanalysis, Operational model of network security

[4 Hrs]

Mathematical Foundations: Prime Number, relatively prime numbers, Modular Arithmetic, Fermat's and Euler's Theorem, The Euclidean and Extended Euclidean Algorithms, The Chinese Remainder Theorem, Discrete logarithms

[6 Hrs]

Symmetric Key Ciphers: Symmetric Key Ciphers, Feistel Networks, Modern Block Ciphers, Modes of Operation, Cryptanalysis of Symmetric Key Ciphers: Linear Cryptanalysis, Differential Cryptanalysis

[8 Hrs]

Asymmetric Cryptography: RSA, Key Distribution and Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography, hash functions: The Merkle Damgard Construction, Message Digest algorithms: MD5, Secure Hash algorithm (SHA), Message Authentication Codes **[8 Hrs]**

Authentication and Web Security: Digital Signatures, Authentication Protocols, Kerberos, X.509 Digital Certificate Standard, Pretty Good Privacy, Secure Socket Layer, Secure Electronic Transaction. Zero knowledge proof

[8 Hrs]

Network Security: Intruders, Intrusion Detection, Password Management, Worms, viruses, Trojans, Virus Countermeasures, Vulnerabilities in TCP/IP model, Firewalls, Firewall Design Principles.

[6 Hrs]

Text Books

- "Cryptography and Information Security", V. K. Pachghare, 3rd edition, PHI Learning, ISBN: 978-93-89-347-10-4.
- "Network Security: Private Communication in a Public World", Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, ISBN 0-13-046019-2.

Reference Books

- "Cryptography and Network Security, Principles and Practices", William Stallings, Pearson Education, Fifth Edition, and ISBN: 0-13-60970-9.
- "Network Security the Complete Reference", Robert Bragge, Mark Rhodes, Heith Straggberg Tata McGraw Hill Publication, ISBN: 9780072226973.

(CT-22004) Cryptography and Network Security Laboratory

Teaching Scheme
Laboratory: 2 Hrs/ Week

Examination Scheme
Continuous evaluation: 50 Marks
Mini Project: 25 marks
End Semester Exam: 25 Marks

Course Outcomes

Students will be able to:

1. Analyze the optimal features and time required for an encryption technique.
2. Implement cryptographic algorithms in any programming language.
3. Demonstrate the ability to detect attacks on a system and tackle it.
4. Write a security application to protect a system from some attacks.

Suggested List of Assignments

1. 1. Study papers on a network security topic and write a study report
   a) Wireless Network Security,
   b) Key Exchange Protocols,
   c) Block chain.
2. 2. Implement any one classical encryption technique in any programming language.
3. 3. Design and implement a symmetric encryption algorithm based on Feistel structure.
4. 4. Demonstrate how Diffie-Hellman key exchange works with Man-In-The-Middle attack.
5. 5. Study different approaches for Anti-virus software and write one document.
   a) Examine files to look for viruses by means of a virus dictionary
   b) Identifying the suspicious behavior from any computer program which might indicate infection
6. 6. Study and demonstrate system hacking and write a report.
   a) How to crack a password?
   b) How to use Ophcrack / Crowbar / John the Ripper / Aircrack-ng to Crack Passwords
7. 7. Develop a mini project on
   a) a hack tool to break the security of a system.
   OR
   b) a tool to protect the system from the hack tool.

This is a suggested list. The instructor is expected to continuously update it.

Departmental Elective – II

(CT(DE)-22002) Cloud Computing and Big Data

Teaching Scheme	**Examination Scheme**
Lectures: 3 Hrs/ Week	Assignment/Quizzes : 40 marks
	End Semester Exam: 60 marks

Course Outcomes

Students will be able to:

1. Comprehend basic concepts of cloud computing and virtualization.
2. Identify various cloud-based solutions to meet a set of given requirements.
3. Visualize development of applications using kubernetes and container concepts.
4. Gain fundamentals of big data and big data processing frameworks.
5. Demonstrate applications of Apache framework for big data processing and analysis on cloud.

Course Contents

Introduction: History of Centralized and Distributed Computing - Overview of Distributed Computing, Cluster computing, Grid computing Distributed Computing and Enabling Technologies, Cloud Fundamentals: Cloud Definition, Evolution, Architecture, Applications, deployment models, and