Laboratory Manual

FOR

Cryptographic Protocols and Algorithms

(MIS 526)

MASTER OF TECHNOLOGY

[INFORMATION SECURITY MANAGEMENT]

REGULAR PROGRAMME

Offered by

Indira Gandhi Delhi Technical University for Women

(Established by Govt. of Delhi vide Act 09 of 2012)

(Formerly Indira Gandhi Institute of Technology)

Kashmere Gate Delhi-110006

Table of Contents

Objective

This laboratory course is intended for the students of second semester M.Tech (ISM) so as to enhance their programming skills in cryptographic algorithms. The lab exercises covers almost all techniques of symmetric and asymmetric cryptographic techniques, mathematical background, block ciphers and digital signature. These exercises will enhance their knowledge in the context of cryptography and make them learn how to implement the concepts learnt as theory in particular and will increase their curiosity to learn the encryption and decryption techniques in general.

Compiled by Ms. Charu Gupta, Assistant Prof. , Deptt of IT, IGDTUW.

Syllabus

Paper Code: MIS-502	L	P	C
Paper: Cryptographic Protocols and Algorithms	4	0	4

INSTRUCTIONS TO PAPER SETTERS:
Question No. 1 should be compulsory and cover the entire syllabus. This question should have objective or short answer type questions. It should be of 20 marks.
Apart from Question No. 1, rest of the paper shall consist of four units as per the syllabus. Every unit should have two questions. However, student may be asked to attempt only 1 question from each unit. Each question should be 10 marks

UNIT 1

Protocol Building Blocks, Communication Using Symmetric Cryptography, One Way Hash Functions, Communication using Public Key Cryptography , digital signatures, signature with encryption, Random and Pseudo random sequence generation.

(10 Hrs)

UNIT 2

Basic Protocols: key exchange, Authentication, Formal analysis of Authentication and Key exchange protocols, Multiple Key Public Key Cryptography, secret Splitting, Secret Sharing.

(10 Hrs)

UNIT 3

Intermediate Protocols: time stamping services, subliminal channels, Undeniable Digital signatures, Proxy signatures, group signatures, Bit Commitment, fair coin flips, metal poker, key escrow.

(10 Hrs)

UNIT 4

Advanced Protocols: Zero knowledge proofs, Zero knowledge proof for identity, blind signatures, identity based public key cryptography, Oblivious transfer, oblivious signatures, Simultaneous contact signing, Digital certified Mail, Esoteric protocols, secure elections.

(10 Hrs)

References:

1. Bruce Schneier, Applied Cryptography, 2nd edition, 1996, Wiley
2. Dong, Ling, Chen, Kefei, , Security Analysis Based on Trusted Freshness, 1st edition 2012, Springer
3. Bernard Menezes, “Network Security and Cryptography”, 2nd edition, 2011, Cenege Learning
4. J A Buchman, “ Introduction to Cryptography”, 2nd Edition, 2009, Springer

Guidelines

1. Students are allowed to work in groups of n (1≤n≤6) since some of the exercises are complex.
2. Any of the programming language can be used.
3. Every lab exercise should include objective, language used , details of protocol (background, history, drawbacks , etc.)
4. Both algorithm and properly commented program alongwith screenshots of output are to be written in files.
5. A proper explanation of the program is to be presented to the instructor as well as the class.
6. Every student is required to come prepared with the algorithmic steps of the lab exercise.
7. Study Material to be referenced from standard books, internet, published papers etc.
8. All references to be mentioned properly with each lab exercise.
9. Any student found indulged in malpractices, disobedience will be debarred from the lab without any warning for a part/whole semester.

List of Experiments

1. **Lab exercise 1 : -- Substitution Ciphers (Encryption)**
   Implement following ciphers to get encrypted output.
   - a) Caesar Cipher
   - b) General Caesar Cipher
   - c) Linear CaesarCipher
   - d) Solitaire
   - e) PlayFair
   - f) Hill Cipher
   - g) Vernam
   - h) Vignere
   - i) One Time Pad
   - j) Affine Cipher
2. **Lab exercise 2 : -- Substitution Ciphers (Decryption)** : Implement above ciphers to get decrypted output
3. **Lab exercise 3 : -- Transposition Ciphers (Encryption)**
   Implement following ciphers to get encrypted output.
   - a) Columnar Transposition
   - b) Rail Fence
   - c) Rail fence with different Permutations
4. **Lab exercise 4 : -- Transposition Ciphers (Decryption) :** Implement above ciphers to get decrypted output
5. **Lab exercise 5 : -- Mathematical Prelims :** Implement the following algorithms.
   - **a)** Legendre Symbol
   - **b)** Addition chaining
   - **c)** GCD of an array of n numbers
   - **d)** Jacobi Symbol
   - e) Solvay-Strassen
   - **f)** Rabin Miller Primality test
   - **g)** Extended Euclidean Algorithm
   - **h)** Chinese Remainder Algorithm
   - **i)** Lehmann Symbol
   - **j)** Discrete Log Algorithm
   - **k)** Euler Totient Function
6. **Lab exercise 6 : -- Asymmetric Ciphers (Encryption)**
7. **Lab exercise 7 : -- Asymmetric Ciphers (Decryption)**
8. **Lab exercise 8 : -- Hash Algorithms.**
9. **Lab exercise 9 : -- Block Ciphers (Encryption)**
10. **Lab exercise 10 : --Digital Signatures.**

-------The list of sub programs will be given in lab itself.

Compiled by Ms. Charu Gupta, Assistant Prof. , Deptt of IT, IGDTUW.

Rules to be followed

Do's

1. Strictly adhere to submission **deadline.**
2. **Both sides** of the paper to be used for print outs of lab files.
3. Standard font face and size to be used. (Times New Roman (14) for heading , 12 for text, `Courier(11) for code.`
4. Any sort of plagiarism is not accepted.
5. Every student to appear before viva-voce on the date scheduled for internal assessment.
6. Complete the lab work assigned in the lab timings only.
7. All references to be mentioned properly with each lab exercise.

Don'ts

1. Late submission – Marks will be deducted from internal assessment.
2. Plagiarism – is Unacceptable.
3. Malpractices, cheating**,** disobedience, misbehavior etc.-these activites are unacceptable and any student found indulged will be debarred from the lab without any warning for a part/whole semester.
4. Mobile Phone -- Use of mobile phone is strictly prohibited in the lab.

Evaluation Policy

1. Students will be evaluated on the basis of their performance in laboratory.
2. Each lab exercise will be evaluated on the following basis :

   a) Implementation

   b) Timely submission

   c) Presentation of code.

   d) Viva
3. Marks will be deducted from internal assessment for any delay, plagiarism, mis-conduct etc.