RKUNIVERSITY

SYLLABUS

Course Title	**Cryptography&Network Security**
Course Code	CE704
Course Credit	Theory : 03
	Practical : 01
	Tutorial : 00
	Credits : 04

Course Learning Outcomes

On the completion of the course, students will be able to:

- **Understand**basic security concepts and applications.
- **Understand** and **apply** classical and modern encryption techniques to provide security.
- **Understand**basic web security principles**.**
- **Identify** and**investigate**system threats**.**
- **Understand** and **apply** various authentication applications for security.
- **Understand** basicprinciples of wireless network security.
- **Understand** howauthentication is implemented in wireless system.
- **Understand** and **implement** important network security tools and mechanisms**.**

Sr. No.	**Name of chapter & details.**	**Hours Allotted**
	Section – I	
1	**Introduction:** Security Attacks, Security services, Security Mechanisms, A Model for Network Security, Substitution Techniques, Transposition Techniques.	**05**
2	**Modern Encryption:** Symmetric Cipher Model, Block ciphers vs Stream ciphers, Overview of Cipher Algorithm Modes: ECB, CBC, CFB, OFB, CTR, Simple DES, Analysis of simple DES, Advanced Encryption Standard,	**08**
3	**Public Key Cryptography:** Principles of Asymmetric key Cryptography, RSA Algorithm, Key Management, Elliptic Curve Cryptography, Diffie-Hellman key Exchange, Digital Signature.	**08**
4	**Web Security:** Web Security Requirement, SSL, Secure Electronic Transaction	**03**

	Section – II	
5	**Systems Threats, Risks and Firewall:** Viruses and related threats, Specific attacks: Sniffing and spoofing, Phishing, Pharming, Key Logger, Firewall: Introduction, Types of Firewall, Firewall configurations.	05
6	**Authentication Applications:** Kerberos, X.509 Authentication Service, Public-Key Infrastructure	08
7	**IP Security E-mail Security:** IP Security Overview, Architecture, Authentication Header, Encapsulation Security payload, Combining Security Association, Key Management, Pretty Good Privacy.	07
8	**Wireless Network Security:** Wired Equivalent Privacy (WEP), Vulnerabilities of IEEE.11 Security, WPA1 and WPA2 : PSK Authentication, TKIP Encryption and AES-CCMP Encryption	04

Instructional Method and Pedagogy

- Lectures will be conducted using Multimedia software, and black-board.
- Various simulators will be used inside the class-room.
- Assessment will be done to monitor continuous student progress
- Computer network security tools will be used to understand various concepts of computer networks & security.

Reference Books

- William Stallings, Cryptography and Network Security, Pearson, 4th edition.
- Mark Ciampa,Security + Guide to Network Security Fundamentals,Cengage Learning, 4th edition.
- AtulKahate, Cryptography and Network Security, Tata MacGrew Hill, 3rd Edition
- B. Forouzan, Cryptography and Network Security, Tata MacGrew Hill, 2nd Edition
- D. Denning, Cryptography and Data Security, Addison-Wesley, 2nd edition.
- S Bueert and Stephen Paine, RSA securities official Guide to cryptography, McGraw-Hill, 1st edition.
- Uyless Black, Internet Security Protocols,Pearson Education, 2nd edition.
- W.R. Cheswick, S.M. Bellovin, Firewalls and Internet Security, Addison Wesley, 1998, 2nd edition.

Additional Resources

- NPTEL video lectures of Cryptography and Network Security course of Computer Science and Engineering by Dr. DebdeepMukhopadhyay, IIT Kharagpur.
- NPTEL video lectures of Computer Security and Cryptography – I course of Computer Science and Engineering by Prof. Bernard Menezes, IIT Bombay.

List of Experiments

Tutorial-1

1. **Develop** an application to implement Caesar cipher**.**
   Guidelines to convert Plain Text to Cipher Text
   - You have to take variable length string as plaintext and integer value between 1 to 25 as key.
   - Cipher text will be generated by taking one character of plain text at a time by using following formula:
   - C = (p + k) mod (26) where c=cipher text and p=plain text.
   - Students need to develop the same using C programming language.
2. **Implement** an application to implement Single columnar cipher.
   Guidelines to convert Plain Text to Cipher Text
   - You have to take variable length string as plaintext and order of columns as key.
   - Plain text will be arranged in matrix of m * n. where m=length(Plain Text)/length(column) and n=length(column)
   - Matrix will be read in order of the column as given per key.
   - Students need to implement the same using C programming language.

Tutorial-2

1. **Develop** an application to implement mono alphabetic cipher.
   Guidelines to convert Plain Text to Cipher Text

   - You have to take variable length string as plaintext and random key of exact 26 alphabets long.
   - Take one character from plain text and search index of it from “abcdefghijklmnopqrstuvwxyz”.
   - Locate the character in key which is there on the above found index.
   - Replace that character with newly found character.
   - Students need to develop the same using C programming language.

2. **Develop** an application to implement Rail fence cipher.
   Guidelines to convert Plain Text to Cipher Text

   - You have to take variable length string as plaintext.
   - Make matrix of 2 rows and (length (plaintext)/2) columns.
   - Put each and every alternate character of plain text in matrix
   - Read the matrix row wise to generate cipher text.

- Students need to develop the same using C programming language.

Tutorial -3

Implement an application to implement Play Fair Cipher.

Guidelines to convert Plain Text to Cipher Text

- You have to take variable length string as plaintext and variable length key.
- Make 5 * 5 MATRIX FROM THE KEY using :
  - fill in letters of key (without duplicates)
  - fill rest of matrix with other letters
- Make pair of two letters of plain text. if a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx lo on"
- Follow the encryption rules and generate the cipher text:
  - if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. “ar" encrypts as "RM"
  - if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. “mu" encrypts to "CM"
  - otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “hs" encrypts to "BP", and “ea" to "IM" or "JM" (as desired)
- Students need to develop the same using C programming language.

Tutorial-4

Implement anapplication to implement Diffie Hellman Key Exchange algorithm.

Guidelines to Generate keys using Diffie Hellman

You have to select two large prime numbers that are integer first. Now you have to assume two users Alice and Bob and calculate the value of A and B from A and B calculate the value of K1 and K2.

Tutorial-5

Find algorithms for checking largest prime numbers and use this algorithm to develop an application to implement RSA algorithm.

Guidelines to convert Plain Text to Cipher Text

In your answer you have to implement logic to search largest prime numbers. You have to search or develop logic for checking largest prime numbers. You will be using this logic to develop the program for RSA algorithm.

Tutorial 6

Perform an experiment to demonstrate how to sniff for network traffic.

Guidelines

Inside this lab you will download any packet sniffing tool. Download that tool and install the tool and try to capture the packets using the tool. Analyse the packet and note the analysis of the packet that you have captured.

Tutorial-7

Analyze and demonstrate one Security Tools or Esthetical Hacking tool.

Guidelines

In your answer you have to select one esthetical hacking or security tool that you have not selected in previous tutorials. You have to download the tool and install the tool. You have to identify the purpose of the tool and try to use the tool. Prepare a presentation or demonstration of the tool and give the demonstration of the tool that you have selected.