Syllabus

Computer and Network Security

Subject Code: ECE-803 L T P: 2 1 0 Credits: 03

I. Introduction

1. Need for Security
2. Security Attacks
3. Services and Mechanisms
4. Network Security
5. Model

II. Symmetric Ciphers

1. Substitution &Transposition Techniques
2. Block Cipher
3. DES
4. Triple DES
5. Stream Ciphers
6. RC4

III. Public Key Cryptography

1. Need and Principles of Public Key Cryptosystems
2. RSA Algorithm
3. Key Distribution and Management
4. Diffie-Hellman Key Exchange
5. Digital Signatures

IV. Authentication

1. Authentication Requirements
2. Message Authentication Codes
3. Hashes
4. MD5 & SHA
5. User Authentication: Password, Certificate based & Biometric Authentication
6. Kerberos

V. Network Security

1. Firewalls
2. IP Security
3. VPN
4. Intrusion Detection
5. Web Security
6. SSL
7. TLS

Text Books:

1.	“Cryptography & Network Security”, PHI	William Stalling
2.	“Cryptography & Network Security”, Mc Graw Hill	Atul Kahate
3.	“Cryptography & Network Security”, PHI 4	Forouzan

Additional References:

1.	"Modern Cryptography, Theory & Practice", Pearson Education.	Wenbo Mao
2.	"An Introduction to Mathematical Cryptography", Springer.	Hoffstein, Pipher, Silvermman.
3.	"The Design of Rijndael", Springer.	J. Daemen, V. Rijmen.
4.	"Algorithmic Cryptanalysis", CRC Press.	A. Joux
5.	"Number Theory", Tata Mc Graw Hill.	S. G. Telang
6.	"Protocols for Authentication and Key Establishment", Springer.	C. Boyd, A. Mathuria.
7.	"Computer Security", Pearson Education.	Matt Bishop
8.	“Understanding Cryptography”, Springer-Verlag Berlin Heidelberg	Christof Paar, Jan Pelzl

Virtual Laboratories

1.	Vlabs, “Cryptography Lab”	http://cse29-iiith.vlabs.ac.in/

Course Outcomes:

COs	
CO1	Develop Concept of Security needed in Communication of data through computers and networks along with Various Possible Attacks
CO2	Understand Various Encryption mechanisms for secure transmission of data and management of key required for required for encryption
CO3	Understand authentication requirements and study various authentication mechanisms
CO4	Understand network security concepts and study different Web security mechanisms.

Module No.	Lectures	Videos NPTEL	Additional Videos- MIT	Additional Materials
I-INTRODUCTION	1. Need for Security 2. Security Attacks 3. Services and Mechanisms 4. Network Security 5. Model	https://nptel.ac.in/courses/106105031/ "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"-Videos and PDF	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm "Computer Systems Security by Nickolai Zeldovich & James Mickens, MIT"	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm "Network and Computer Security by Prof Ronald Rivest, MIT"
II-SYMMETRIC CIPHERS	6. Substitution &Transposition Techniques 7. Block Cipher 8. DES 9. Triple DES 10. Stream Ciphers 11. RC4	https://nptel.ac.in/courses/106105031/ "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"	https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/v "Introduction to Cryptography by Christof Paar, MIT"	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm "Network and Computer Security by Prof Ronald Rivest, MIT"
III-PUBLIC KEY CYPTOGRAPHY	12. Need and Principles of Public Key Cryptosystems 13. RSA Algorithm 14. Key Distribution and Management 15. Diffie-Hellman Key Exchange 16. Digital Signatures	https://nptel.ac.in/courses/106105031/ "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"	https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/v "Introduction to Cryptography by Christof Paar, MIT"	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm "Network and Computer Security by Prof Ronald Rivest, MIT"
IV-AUTHENTICATION	17. Authentication Requirements 18. Message Authentication Codes(MAC) 19. Hashes 20. MD5 & SHA 21. User Authentication: Password, Certificate based & Biometric Authentication 22. Kerberos	https://nptel.ac.in/courses/106105031/ "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"	https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/v "Introduction to Cryptography by Christof Paar, MIT"	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm "Network and Computer Security by Prof Ronald Rivest, MIT"
V-NETWORK SECURITY	23. Firewalls 24. IP Security 25. VPN 26. Intrusion Detection 27. Web Security 28. SSL 29. TLS	https://nptel.ac.in/courses/106105031/ "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"	https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm "Computer Systems Security by Nickolai Zeldovich & James Mickens, MIT"	https://www.edx.org/course/network-security-2 "An eDx Course on Network Security"

Links to Reading Material (Use your institute mail IDS to access the Google Drive)

https://drive.google.com/open?id=1somShxnVKGgep6pLcvRFfm_KMyrsG0DC

https://drive.google.com/open?id=1xd3RSBl6iEGW2AiZ4lgbb9TdgpfpizP5

https://books.google.co.in/books?id=Kokjwdf0E7QC&printsec=copyright&source=gbs_pub_info_r#v=onepage&q&f=false