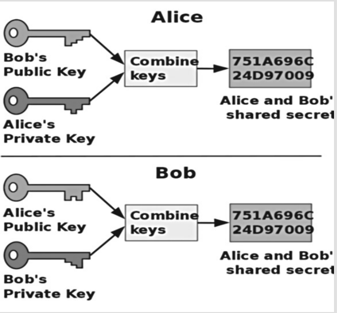

source
https://en.wikipedia.org/

19CS311 CRYPTOGRAPHY AND NETWORK SECURITY

Hours Per Week :

L	T	P	C
3	-	-	3

Total Hours :

L	T	P	CS	WA/RA	SSH	SA	S	BS
45	-	-	5	5	30	20	5	5

PREREQUISITE COURSE: Computer Networks.

COURSE DESCRIPTION AND OBJECTIVES:

This course focuses on the modern concepts of network security using various cryptographic algorithms and underlying network security applications. It enables to understand various symmetric and asymmetric cryptographic techniques. It focuses on security implementation in practical applications such as e-mail functioning, web security and secure electronic transactions protocol and system security.

COURSE OUTCOMES:

Upon completion of the course, the student will be able to achieve the following outcomes:

COs	Course Outcomes	POs
1	Apply cryptographic techniques in various security service solutions effectively in everyday professional and social contexts.	1
2	Analyse various network security essentials, classical and modern encryption techniques, the network security model, principles of symmetric and asymmetric cryptosystems, protocols and its usage in network, web and system security.	2
3	Design of cryptographic mechanisms using the algorithms for providing the needed services.	3, 6
4	Investigate various network security and system security scenarios for real time applications.	4, 6

SKILLS:

- ✓ *Design various security services for appropriate applications.*
- ✓ *Identifying the appropriate firewall, password management and anti-virus models for specific applications.*

UNIT– I **L- 7**

INTRODUCTION TO NETWORK SECURITY: Security attacks, Security services, Security mechanisms, A model for network security.

CLASSICAL ENCRYPTION TECHNIQUES: Symmetric cipher model, Substitution techniques, Transposition techniques, Rotor machines and steganography.

UNIT – II **L- 9**

BLOCK CIPHERS AND DATA ENCRYPTION STANDARD: Block cipher principles, Data encryption standard, Strength of DES, Differential and linear cryptanalysis, Block cipher design principles.

ADVANCED ENCRYPTION STANDARD: Evaluation criteria of AES, AES cipher, More on symmetric ciphers, Multiple encryption and triple DES, Block cipher modes of operation, RC4.

UNIT – III **L- 11**

PUBLIC-KEY ENCRYPTION AND HASH FUNCITONS: Principles of public key cryptosystems, RSA algorithm, Key management.

MESSAGE AUTHENTICATION AND HASH FUNCTIONS: Authentication requirements, Authentication functions, Message authentication, Hash functions, Security of hash functions and MACs.

DIGITAL SIGNATURES: Authentication protocols and digital signature standard.

UNIT – IV **L- 9**

NETWORK SECURITY APPLICATIONS: Kerberos, X.509 authentication service, Public key infrastructure, Pretty good privacy, S/MIME.

IP SECURITY OVERVIEW: IP security architecture, Authentication header, Encapsulating security payload, Combining security associations and key management.

UNIT – V **L- 9**

WEB SECURITY: Secure socket layer and transport layer security, Secure electronic transaction.

SYSTEM SECURITY: Intruders, Intrusion detection, Password management, Malicious software, Firewalls and trusted systems.

TEXT BOOK:

1. William Stallings, “Cryptography and Network security”, 4th edition, Pearson Education, 2010.

REFERENCE BOOKS:

1. William Stallings “Network Security Essentials Applications and Standards”, 2nd edition, Pearson Education, 2009.
2. Eric Malwald, “Fundamentals of Network Security”, 4th edition, Pearson Education, 2010.
3. Buchmann, “Introduction to Cryptography”, 2nd edition, Pearson Education, 2009.