COURSE INSTRUCTOR NAME:Dr.C.N.Ravi ACADEMIC YEAR:2024-25

SUBJECT NAME:CRYPTOGRAPHY AND NETWORK SECURITY SECTION:B&D

EMAIL-ID:cnravi@cmrec.ac.in

CLASS ROOM NO:B214&216

CONTACT NO: 99410 07874

SEM START DATE AND END DATE: 8-7-24 TO 9-11-24

CONTENTS OF COURSE FILE

1. **Department vision & mission**
2. **List of PEOs, POs, PSOs**
3. **List of Cos (Action verbs as per blooms with BTL)**
4. **Syllabus copy and suggested or reference books**
5. **Individual Time Table**
6. **Session plan/ lesson plan**
7. **Session execution log**
8. **Lecture notes(handwritten or softcopy printout-5 units)**
9. **Assignment Questions with (original or Xerox of mid 1 and mid 2 assignmentsamples)**
10. **Mid exam question papers with(Xerox of mid 1 and mid 2 script samples)**
11. **Scheme of evaluation**
12. **Mapping of Cos with Pos and PSOs**
13. **COs, POs, PSOs Justification**
14. **Attainment of Cos, Pos and PSOs (Excel sheet)**
15. **Previous year question papers**
16. **Power point presentations (PPTs)**
17. **Innovative Teaching method**
18. **References (Textbook/Websites/Journals)**

HOD

A

Course File Report

On

"Cryptography and Network Security"

Submitted by

Dr. C.N.Ravi
Associate Professor

In the department of
Computer Science & Engineering

CMR ENGINEERING COLLEGE

(Approved by AICTE-NewDelhi, Affiliated to J.N.T.U, Hyderabad)
Kandlakoya(v),Medchal Road,Hyderabad-501 401,Telangana State, India .Website: www.cmrec.ac.in
(2024-25)

1. DEPARTMENT VISION & MISSION

Vision:

To produce globally competent and industry-ready graduates in Computer Science & Engineering by imparting quality education with the know-how of cutting-edge technology and holistic personality.

Mission:

1. To offer high-quality education in Computer Science & Engineering in order to build core competence for the graduates by laying a solid foundation in Applied Mathematics and program frameworkwith a focus on concept building.
2. The department promotes excellence in teaching, research, and collaborative activities to prepare graduates for a professional career or higher studies.
3. Creating an intellectual environment for developing logical skills and problem-solving strategies, thus developing, an able and proficient computer engineer to compete in the current global scenario.

2. LIST OF PEOs, POs AND PSOs

2.1 Program Educational Objectives (PEO):

PEO 1: Excel in professional career and higher education by acquiring knowledge of mathematical computing and engineering principles.
PEO 2: To provide an intellectual environment for analyzing and designing computing systems for technical needs.
PEO 3: Exhibit professionalism to adapt current trends using lifelong learning with legal and ethical responsibilities.
PEO 4: To produce responsible graduates with effective communication skills and multidisciplinary practices to serve society and preserve the environment.

2.2. Program Outcomes (POs):

Engineering Graduates will be able to satisfy these NBA graduate attributes:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first

principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

8. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

9. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

10. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

11. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

2.3 Program Specific Outcomes (PSOs):

PSO1: Professional Skills and Foundations of Software development: Ability to analyze, design and develop applications by adopting the dynamic nature of Software developments.
PSO2: Applications of Computing and Research Ability: Ability to use knowledge in cutting edge technologies in identifying research gaps and to render solutions with innovative ideas.

3. LIST OF CO's (ACTION VERBS AS PER BLOOM'S TAXONOMY)

COURSE OUTCOMES:

COURSE NAME: CRYPTOGRAPHY & NETWORK SECURITY	
CO1	**Define** the basic components of security systems and cryptographic concepts & techniques [remembering]
CO2	**Illustrate** the basic cryptographic algorithms, message, web authentication and security issues [understanding]
CO3	**Apply** crystographic hash function and message authentication codes, key management and distribution key [Apply]
CO4	**Analyze** transport-level security[SSH] and wireless network security [ieee 802.11 & ieee 802.11] [Analyzing]
CO5	**Explain** mail security and ip security and case studies on cryptography & security evaluation.[Understanding]

4. SYLLABUS COPY

III Year B.Tech. CSE-I Sem (R22 – Professional Elective)

1. CS511PE - CRYPTOGRAPHY AND NETWORK SECURITY SYLLABUS

UNIT – I UNIT – I

Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security

Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

UNIT – II

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

UNIT – III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure

UNIT – IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH)

Wireless Network Security: Wireless Security, Mobile Device Security, IEEE 802.11,Wireless LAN, IEEE 802.11i Wireless LAN Security

UNIT – V

E-Mail Security: Pretty Good Privacy, S/MIME IP Security: IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange

Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

TEXT BOOKS:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition

2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition

REFERENCE BOOKS:

1. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.

2. Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition

3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.

4. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH

5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning

6. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

5.Session Plan

Sl. No.	Topics	No. Of Periods	Text / Reference book	Teaching aids BB/LCD
UNIT-I (Attacks on Computers and Computer Security)				
1	Introduction to Network Security The need of security, security approaches, principles of security	L2	T1 R1	BB
2	Security Attacks (Interruption, Interception, Modification and Fabrication),	L3	T1 R1	LCD/BB
3	Security Services	L4	T1 R1	LCD/BB
4	Security Mechanisms.	L5	T1 R1 T1	LCD/BB
5	A model for Internetwork security, Introduction,plain text and cipher text	L6	T1	LCD/BB
6	Substitution techniques	L9	R1 R1	LCD/BB
7	Transpositition techniques	L11	R1 R1	LCD/BB
8	Encryption&Decryption Symmetric&asymetric key cryptography ,stegnography	L13	R1 T1 T1	LCD/BB

9	Keyrange&key size	L14	T1	
10	Possible types of attacks	L15	T1	LCD/BB
UNIT-II(Symmetric key ciphers)				
11	Block Cipher principles	L17	T1 T1	LCD/BB
12	Algorithms(DES,AES,Blowfish),	L19	T1 T1 T1	LCD/BB
13	Differential and linear Cryptanalysis,Block cipher modes of operation	L21	T1 T1	LCD/BB
14	Stream ciphe rs,RC4	L24	T1 T1	LCD/BB
15	Location and placement of encryption function	L26	T1 T1	LCD/BB
16	Key distribution Asymmetic key Ciphers	L27	T1	
17	Principlesofpubliceycryptosystems,Algorithms(RSA,Diffie-**Hellman**,ECC),Key Distribution	L31	T1 T1 R2 R2	LCD/BB
UNIT-III(Message Authentication Algorithms and Hash Functions)				
18	Authentication requirements	L32	R2	LCD/BB
19	functions,Message authentication codes	L33	R2	LCD/BB
20	Hash functions	L35	R2 R2	LCD/BB
21	Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme	L36	T2	LCD/BB
22	Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption	L37	T2	LCD/BB
23	Distribution of Public Keys	L39	T2 T2	LCD/BB
24	Kerberos, X.509 Authentication Service	L41	T2 T2	LCD/BB
25	Public – Key Infrastructure	L43	T2 R2 T1 R1 T1 R1	LCD/BB
UNIT-IV(Transport-level Security **)**				
26	Web security considerations,			
27	Secure Socket Layer, and Transport Layer Security			

28	HTTPS, Secure Shell (SSH)	L47	T1	LCD/BB
29	Wireless Network Security: Wireless Security	L48	R1	LCD
30	Mobile Device Security, IEEE 802.11 Wireless LAN	L52	R1 R1 R1 R1	LCD/BB
31	IEEE 802.11i Wireless LAN Security	L53	T1	LCD/BB
32	Wireless LAN Security	L54	T1	LCD
UNIT-V(**E-mail security)**				
33	E-Mail Security: Pretty Good Privacy	L56	T1 T1	LCD/BB
34	S/MIME IP Security: IP Security overview	L57	T1	LCD/BB
35	IP Security architecture	L58	T1	LCD/BB
36	Authentication Header, Encapsulating security payload	L61	T1 T1	LCD/BB
37	Combining security associations, Internet Key Exchange	L63	T1 T1	
38	Case Studies on Cryptography and security: Secure Multiparty Calculation	L64	T1	LCD/BB
39	Virtual Elections, Single sign On	L65	T1	LCD/BB
40	Secure Inter-branch Payment Transactions	L66	T1	LCD/BB
41	Cross site Scripting Vulnerability.	L67	T1	LCD/BB

M1 : Lecture Method/BB	**M4 : Presentation /PPT/LCD**	**M7 : Assignment**
M2 : Demo Method	**M5 : Lab/Practical**	**M8 : Industry Visit**
M3 : Guest Lecture	**M6 : Tutorial**	**M9 : Project Based**

6. SESSION EXECUTION LOG:

SLNO	UNIT	SCHEDULED DATE	COMPLETED DATE	REMARKS
1	Unit-1	29-07-2024	21-08-2024	COMPLETED
2	Unit-2	26-08-2024	10-09-2024	COMPLETED
3	Unit-3	16-09-2024	07-10-2024	COMPLETED
4	Unit-4	16-10-2024	06-11-2024	COMPLETED
5	Unit-5	07-11-2024	22-11-2024	COMPLETED

7.Lecutre Notes

Attached

Assignment Questions along with Sample assignment scripts

Assignment Questions - II

1. a. Explain the model of network security [**CO-1**]
   b. Explain Knapsack Algorithm with example. [**CO-1**]
2. Explain RC5 Algorithm with example. [**CO-1**]
3. Write the ElGamal Algorithm. Further to Encrypt the message M=8, on primitive root= 2 of prime= 11. [**CO-2**]
4. Briefly discuss about the concept of Diffie Hellman Key Exchange algorithm. [**CO-2**]
5. Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key d.Let the message be x=24. Perform the encryption and decryption using R.S.A algorithm **[CO-2]**

Assignment Questions – II

1a) Explain Message Authentication Requirements and what are the attacks related to message communication. **(CO-3)**

b) Discuss the different servers used in Kerberos in detail. Explain the role of each one. **(CO-3)**
c) Describe signing and verification in Digital Signature Algorithm. What are two levels of functionality that comprise a message authentication or digital signature mechanism? **(CO-3)**

2a) Is it possible in SSL for the receiver to recorder SSL record blocks that arrive out of order? If so, explain how it can be done. If not, why not? **(CO-4)**
b) Discuss the IEEE 802.11i Wireless LAN Security. **(CO-4)**

3a) What protocols comprise SSL? What is the difference between an SSL connection and an SSL session? (CO-4)
b) Explain about SSL Handshake protocol. **(CO-4)**

4a) Briefly discuss about the scenario of IP security and its Policy. **(CO-5)**
b) Explain IP security architecture and also explain basic combinations of security associations with a neat diagram. **(CO-5)**

5a) List and explain the PGP services and explain how PGP message generation is done with a neat diagram. **(CO-5)**
b) Discuss about the S/MIME in detail. **(CO-5)**
c) .Explain secure interbranch payment transactions in detail**. (CO-5)**

INNOVATIVE ASSIGNMENTS

- Mind Mapping on Security
- Research Paper report on Cryptography
- Write Code for any Current Algorithms.
- Poster Presentation on Phishing Concept

9. Mid Exam Question paper along with sample answer scripts

MID-1

Part –A **Total = 30 Marks**
Answer all Questions: **Marks:**
2X5=10M

1. Write about steganography? (CO1)

2. Mention 5 Block cipher modes of operation.(CO1)
3. Explain (i)Fermat and Eluer's theorem with Example (CO2)
4. Describe about RC4 algorithm (CO2)
5. Define Diffusion & Confusion (CO2)

Part –B

Answer any 4 Questions: Marks: 4X5=20 M

1. Explain Playfair Cipher with **Plain text=Cryptography** and **Key=Network** (CO1)
2. Explain the model of network security? (CO1)
3. Explain in detail about Feistel cipher with diagram. (CO1)
4. How AES is used for encryption/decryption? Discuss with example. (CO1)
5. Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key Let the message be x=24. Perform the encryption and decryption using R.S.A algorithm (CO1)
6. Explain ECC - Diffie Hellman key Exchange with both keys in detail with an example(CO1)

MID-2

Part –A **Total = 30 Marks**

Answer all Questions: **Marks: 2X5=10M**

1. List the schemes for the distribution of public keys. (CO3)
2. What are the properties a digital signature should have . (CO3)
3. Give SSL record format (CO5)
4. What is security association (CO4)
5. Name any cryptographic keys used in PGP (CO5)

Part –B

Answer any 4 Questions: Marks: 4X5=20

M

6. What are the requirements for message authentication (CO3)
7. Describe HMAC algorithm in detail (CO3)
8. Explain in detail about KDC.. (CO3)
9. What is Kerberos? Explain how it provides authenticated service. (CO4)
10. Write brief note on IP Security. (CO5)
11. Explain Secure Electronic transaction with neat diagram(CO5)

11.Mapping of Course outcomes andPOs and PSOs

COURSE CO-PO&PSO MATRIX	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	-	-	-	-	-	-	-	-	-	-	-	-
CO2	3	3	3	2	-	-	1	-	-	-	-	-	-
CO3	3	3	2	2	2	-	1	1	-	-	-	-	2
CO4	3	-	-	2	-	-	-	-	2	-	-	-	-
CO5	3	-	-	-	-	-	1	1	2	-	2	3	-
AVERAGE	**3**	**3**	**3**	**2**	**2**	**0**	**1**	**1**	**2**	**0**	**2**	**3**	**2**

12. **ATTAINMENT OF CO's, PO's AND PSO's (EXCEL SHEET)**:

AFTER RESULT

13.JUSTIFICATION

CO-PO Mapping Justification

CO 1: Define the basic components of security systems and cryptographic concepts & techniques [remembering]

	Justification
PO1	**Correlated with PO1 strongly b**ecause the students able to know the basic components of Security and various Cryptographic techniques. So, overall the correlation of CO1 to PO1 is good.

CO 2: Illustrate the basic cryptographic algorithms, message, web authentication and security issues [understanding]

	Justification
PO1	**Correlated with PO1 strongly** because the Students will able to identify different problems and they can analyze. So, overall the correlation of CO2 to PO1 is good.
PO2	**Correlated with PO2 strongly** because Students will able to analyze the complexity of the problems. So, overall the correlation of CO2 to PO2 is good.
PO3	**Correlated with PO3 strongly** because Students will be able to design the solutions to overcome the attacks. So, overall the correlation of CO2 to PO3 is good.
PO4	**Correlated with PO4 moderately** Students will be able to conduct interpretation of data and provide proper conclusions. So, overall the correlation of CO2 to PO4 is moderate.
PO7	**Correlated with PO7 low** Students will be able to explain the encryption and decryption techniques easily. So, overall the correlation of CO2 to PO8 is low.

CO 3: Apply cryptographic hash function and message authentication codes, key management and distribution key [Applying]

	Justification
PO1	**Correlated with PO1 strongly** because Students will be able to apply the knowledge of basic mathematics while using algorithms. So, overall the correlation of CO3 to PO1 is good.
PO2	**Correlated with PO2 strongly** because Students will be able to design the solutions for different authentication mechanisms. So, overall the correlation of CO3 to PO2 is good.
PO3	**Correlated with PO3 moderately** because Students will be able to design the solutions to overcome the attacks. So, overall the correlation of CO3 to PO3 is moderate.
PO4	**Correlated with PO4 moderately** because Students will be able to conduct interpretation of data and provide proper conclusions. So, overall the correlation of CO3 to PO4 is moderate.
PO5	**Correlated with PO5 moderately** because Students will be able to learn the modern tools which are used to overcome the attacks. So, overall the correlation of CO3 to PO8 is moderate.
PO7	**Correlated with PO7 is Low** because students will be able to apply the ethical principles and commit the norms of the enginnering practice. So, overall the correlation of CO3 to PO8 is low.
PO8	**Correlated with PO8 is Low** Students will be able to communicate as an individual if any attack occurs. So, overall the correlation of CO1 to PO8 is low.
PSO2	**Correlated with PO8 is moderate** Students will be able to do research on key management.

CO 4: Analyze transport-level security(SSH) and wireless network security (ieee 802.11) [Analyzing]

	Justification
PO1	**Correlated with PO1 strongly** because Students will be able to apply the mathematical knowledge on the different attacks. So, overall the correlation of CO4 to PO1 is good.
PO4	**Correlated with PO4 moderate** because Students will be able to conduct interpretation of data and provide proper conclusions. So, overall the correlation of CO4 to PO4 is moderate.
PO9	**Correlated with PO9 moderate** because Students will be able to make effective presentations on the recent attack. So, overall the correlation of CO4 to PO10 is moderate.

CO 5: Explain mail security and ip security and case studies on cryptography & security evaluation.(Understanding)

	Justification
PO1	**Correlated with PO1 is Strongly** because Students will be able to generate passwords by applying the knowledge of mathematics. So, overall the correlation of CO5 to PO1 is good.
PO7	**Correlated with PO7 is Low** because students will be able to apply the ethical principles and commit the norms of the enginnering practice. So, overall the correlation of CO5 to PO8 is low.
PO8	**Correlated with PO8 is Low** because Students will be able to do any work effectively in any environment. So, overall the correlation of CO5 to PO9 is good.
PO9	**Correlated with PO9 is moderately** because Students will be able to write effective reports and make effective presentations. So, overall the correlation of CO5 to PO10 is good.
PO11	**Correlated with PO11 is moderately** because Students will be able to recognize the need for developing the methods to create passwords. So, overall the correlation of CO5 to PO12 is good.
PSO1	**Correlated with PSO1 is strongly** because Students are able to analyze, design and develop the applications by adopting the various developments. So, overall the correlation of CO5 to PSO1 is good.

13. UNIVERSITY QUESTION PAPERS/ QUESTION BANK

Code No.: DS621PE | R20 | H.T.No. | | | 8 | R | | | | |

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
III–B.TECH–II–Semester End Examinations (Regular) - May- 2023
CRYPTOGRAPHY AND NETWORK SECURITY (PE-2)
(CSD)

[Time: 3 Hours] **[Max. Marks: 70]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 20 marks. Answer all questions in Part A.
Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART-A **(20 Marks)**

1. a)	Define plain text and cipher text.	[2M]
b)	Write two principles of security.	[2M]
c)	Differences between stream cipher and block cipher.	[2M]
d)	Write principles of public key cryptosystems.	[2M]
e)	What is digital signature?	[2M]
f)	What is key size of SHA-512.	[2M]
g)	What is wireless security?	[2M]
h)	What are web security considerations?	[2M]
i)	How security maintained for e-mail?	[2M]
j)	What is PGP?	[2M]

PART-B **(50 Marks)**

2.	Discuss about types of security attacks and mechanisms.	[10M]
	OR	
3.	Illustrate different types of substitution techniques.	[10M]
4.	Explain DES algorithm and mention the strengths and weakness of it.	[10M]
	OR	
5.	Discuss RSA algorithm and Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and n=5.	[10M]
6.	Write about HMAC algorithm and its security.	[10M]
	OR	
7.	What is the motivation for Kerberos? Discuss Kerberos version 4.	[10M]
8.	Explain secure socket layer and transport layer security briefly.	[10M]
	OR	
9.	Discuss about IEEE 802.11 wireless LAN.	[10M]
10.	Explain the functionality of S/MIME.	[10M]
	OR	
11.	Discuss case study on "cross site scripting vulnerability".	[10M]

****

14. POWER POINT PRESENTATIONS (PPT's)

Cryptography and Network Security Chapter 1

Presented by
CH.RAVISHEKER
Asst.Proff
Dept. Of CSE

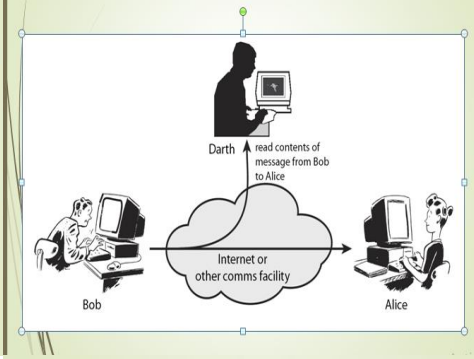
Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Aspects of Security

- consider 3 aspects of information security:
  - security attack
  - security mechanism
  - security service

Passive Attacks



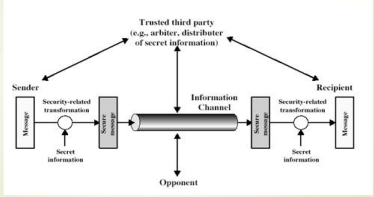
OSI Security Architecture

- ITU-T X.800 "Security Architecture for OSI"
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Security Service

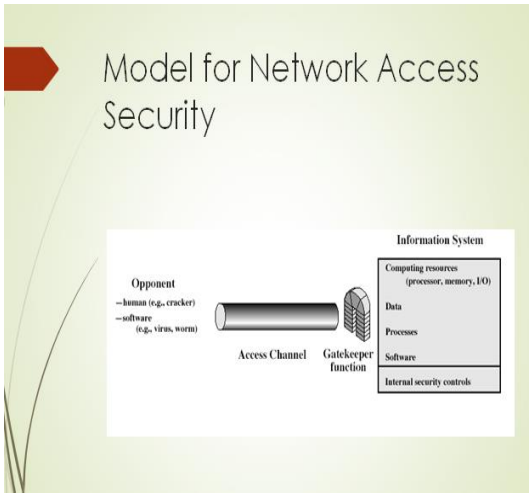
- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

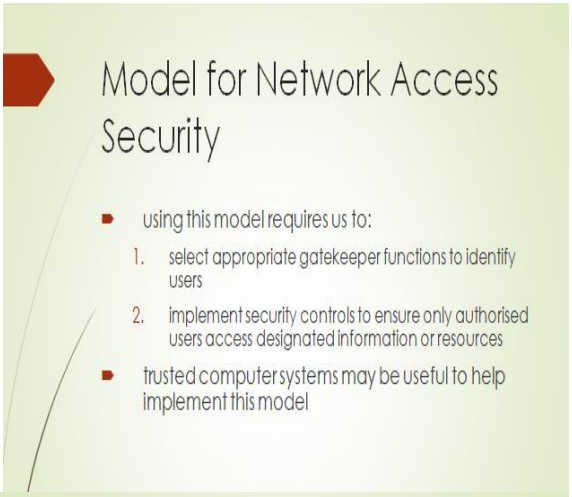
Model for Network Security

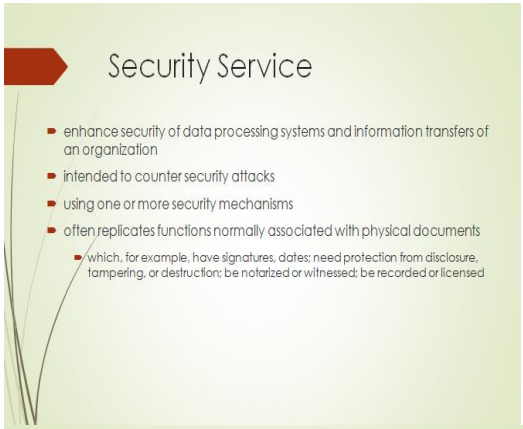


Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service







w15. WEBSITES/URL/E-RESOURCES:

TEXT BOOKS

1. Cryptography and Network Security: William Stallings, Pearson Education, 4th Edition
2. Cryptography and Network Security: Atul khanate, Mc Graw Hill, 2nd Edition

.

REFERENCE BOOKS

1. Cryptography and Network Security: CK Shyamala,N Harini, DrT R Padmanabhan, Wiley India, 1st Edition

2. Cryptography and Network Security:Forouzan Mukhopadhyay, MC Graw Hill, 2nd Edition
3. Information Security,Priniples and Practice: Mark Stamp, Wiley India
4. Priniples of Computer Security: WM Arthur Conklin, Greg White,TMH
5. Introduction to Network security: Neal Kranwez, CENGAGE Learning
6. Network Security and Cryptography: Bemard Menezes, CENGAGE Learning.

WEBSITES

- www.securities.edu
- www.soe.stanford.edu
- www.iitk.ac.in
- http://nptel.iitm.ac.in/courses.php?disciplineId=106
- www.cryptographytutorials.com
-

INTERNATIONAL

1. Mr.william St Dr.K.Vishnuvardhan, Dept. of CSE, JNTU Hyderabad,Dept. of CSE , United States.
2. Mr.Ryan Russell & Dan kaminsky, Information security and Hacking Dept. USA

NATIONAL

1. Prof. Mr.G.Govardhan, Dept. of CSE,IIT Kharagpur
2. Mr.K.Rayappa, Dept. of IT, Gulbarga, Karnataka

REGIONAL

1. Dr.K.Vishnuvardhan, Dept. of CSE,JNTU Hyderabad
2. Prof. R.Srinivas Dept. of CSE, HCU, Hyderabad

7. **JOURNALS:**

- Cryptologia
- Journal of Cryptology
- Journal of Cryptographic Engineerig
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security
- ACM Transactions on Information and System Security