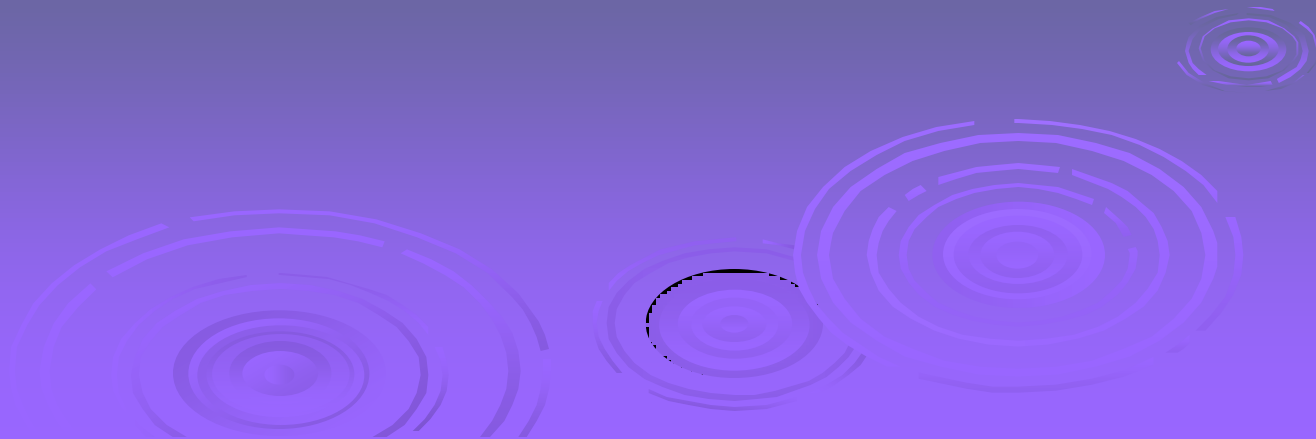


Cryptography and Network Security

Chapter 1



Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total
L	T	P	C	Theory Marks		Practical Marks			Marks
				ESE (E)	PA (M)	PA (V)		PA (I)	
						ESE			
4	0	2	6	70	30	20	10	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Sr. No.	Content	Total HRS	% Weightage
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	3	5%
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	10	25%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	4	5%
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	7	15%
5	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	4	10%

6	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	3	10%
7	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	4	8%
8	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure	4	7%
9	Remote user authentication with symmetric and asymmetric encryption, Kerberos	4	5%
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	5	10%

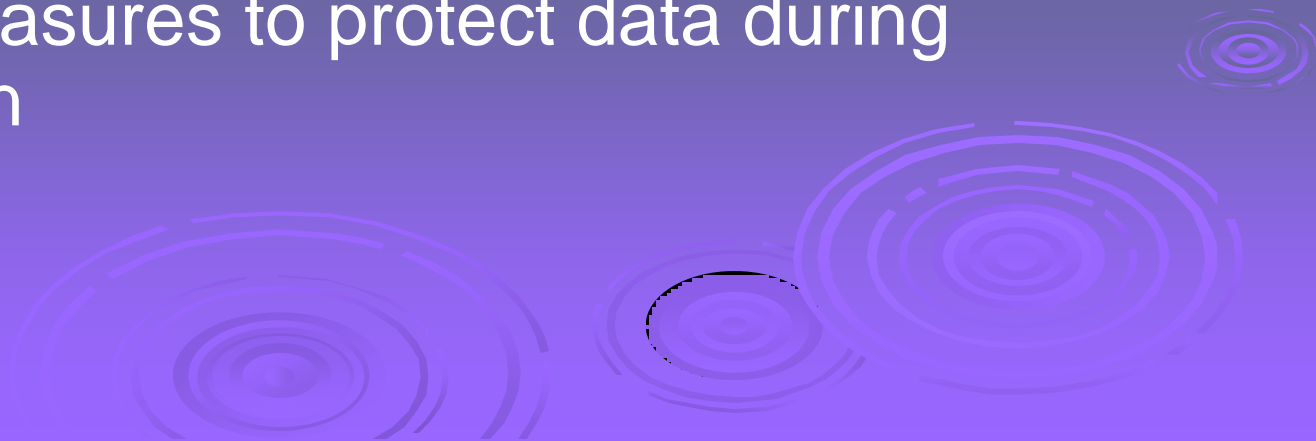
Sr. No.	Content	Total HRS	% Weightage
1	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	3	5%
2	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	10	25%
3	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	4	5%
10	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH	5	10%

Reference Books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Wiley India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill
4. Cryptography and Network Security Atul Kahate, TMH
5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
6. Information Systems Security, Godbole, Wiley-India
7. Information Security Principles and Practice, Deven Shah, Wiley-India
8. Security in Computing by Pfleeger and Pfleeger, PHI
9. Build Your Own Security Lab : A Field Guide for network testing, Michael Gregg, Wiley India

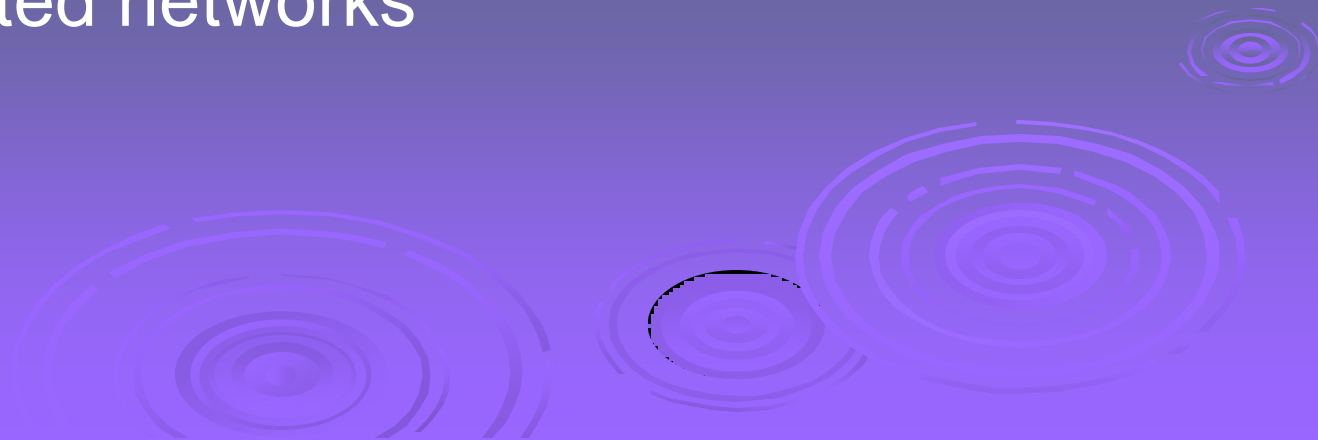
Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission



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



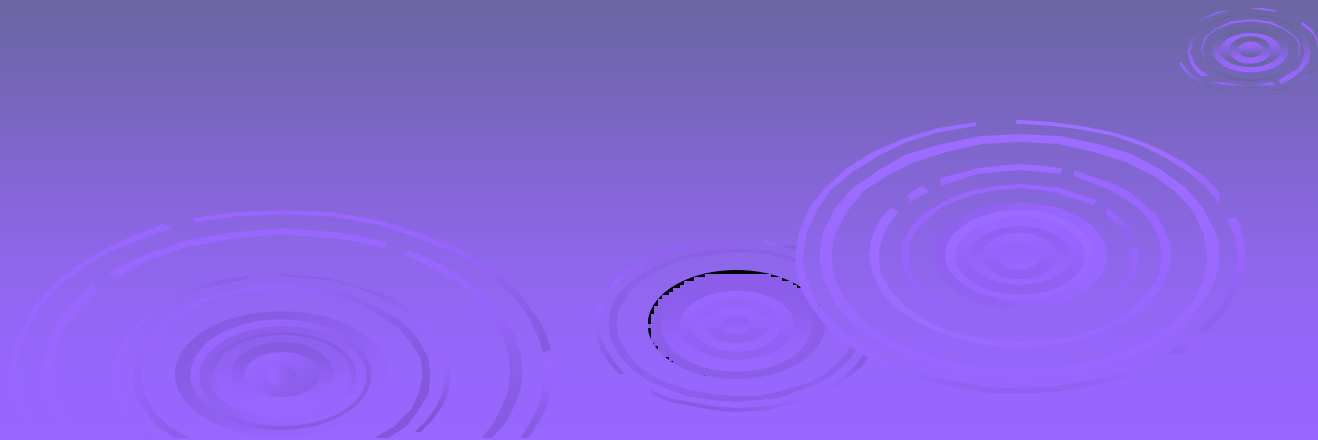
Aim of Course

- our focus is on **Internet Security**
- which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information



Aspects of Security

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

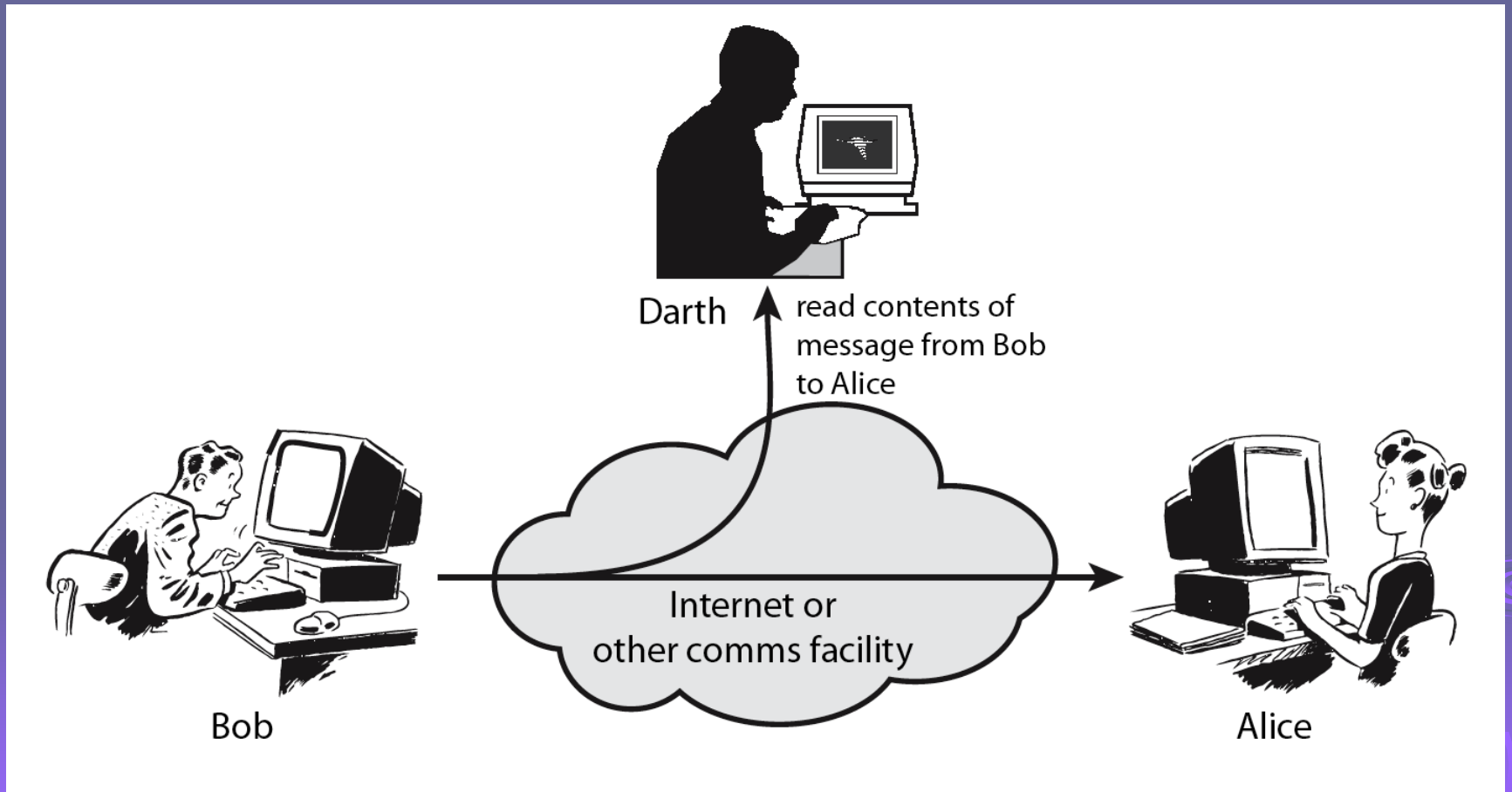


Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus on generic types of attacks
 - passive
 - active

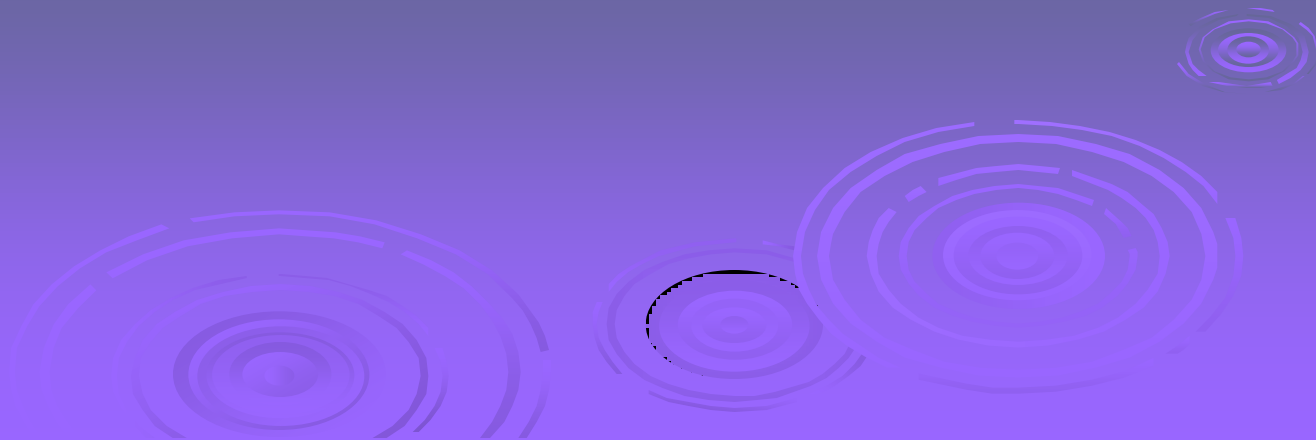


Passive Attacks

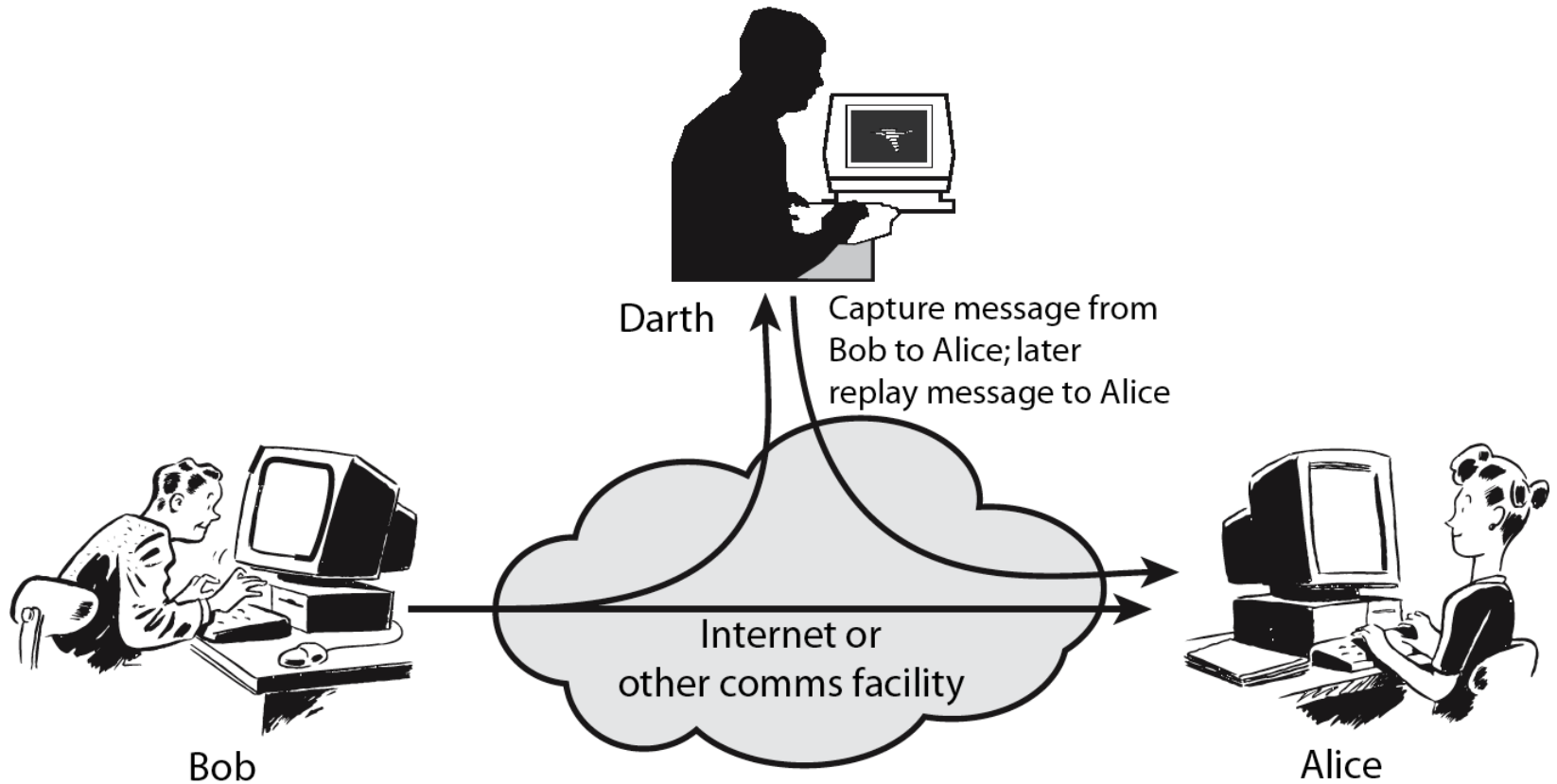


Passive Attacks

- Release of Message content
- Traffic Analysis

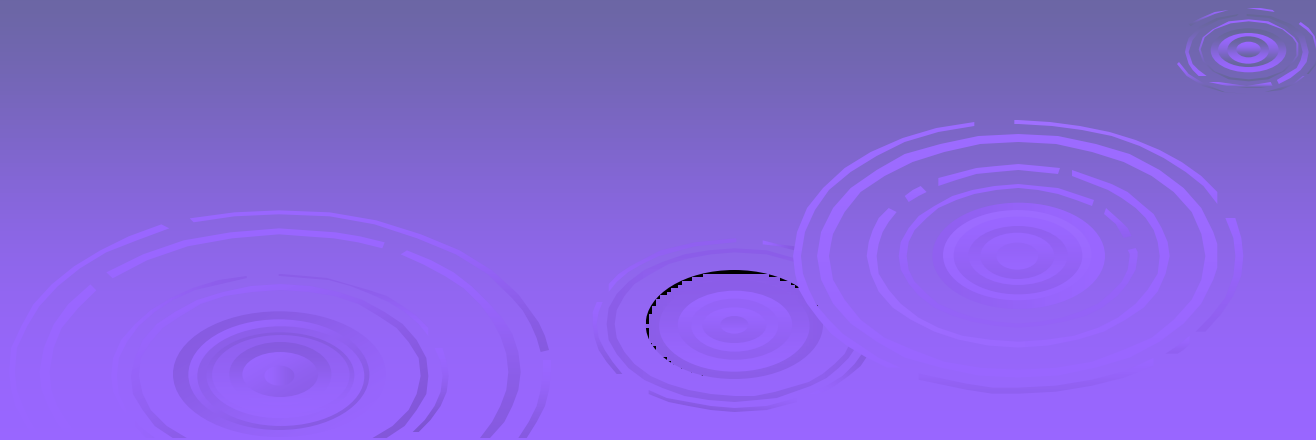


Active Attacks



Active Attacks

- Masquerade
- Replay
- Modification of Message
- Denial of Service



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

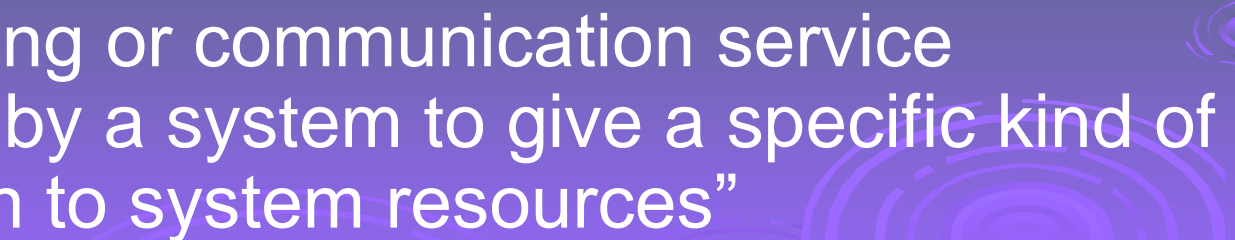
Security Services

➤ X.800:


“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

➤ RFC 2828:

“a processing or communication service provided by a system to give a specific kind of protection to system resources”

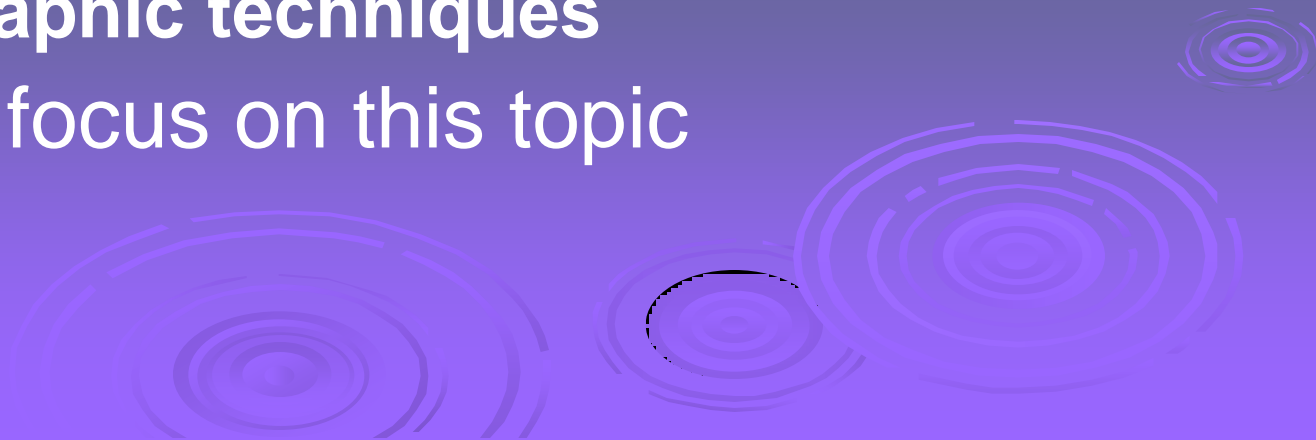
A series of concentric circles, resembling ripples in water, are positioned in the bottom right corner of the slide. They are rendered in a lighter shade of purple than the background.

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
 - **Access Control** - prevention of the unauthorized use of a resource
 - **Data Confidentiality** –protection of data from unauthorized disclosure
 - **Data Integrity** - assurance that data received is as sent by an authorized entity
 - **Non-Repudiation** - protection against denial by one of the parties in a communication
- 
- A decorative graphic consisting of several concentric circles, resembling ripples in water, located in the bottom right corner of the slide.

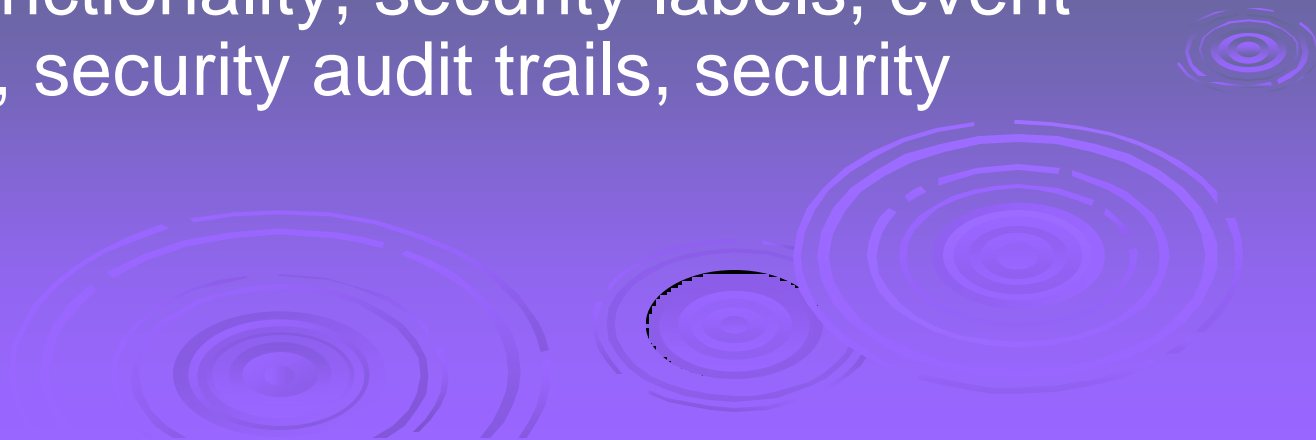
Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
 - **cryptographic techniques**
- hence our focus on this topic

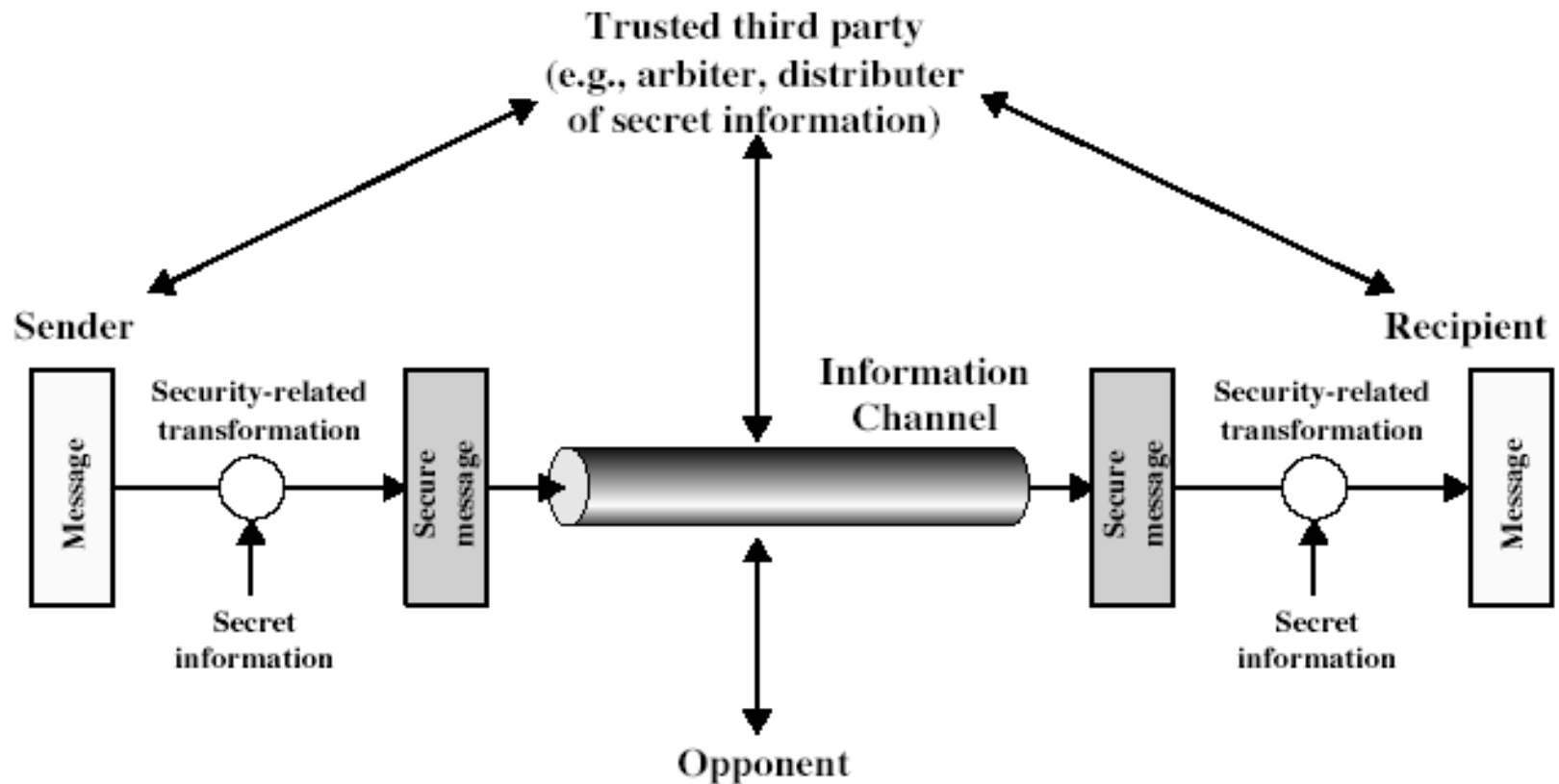


Security Mechanisms (X.800)

- specific security mechanisms:
 - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
 - trusted functionality, security labels, event detection, security audit trails, security recovery



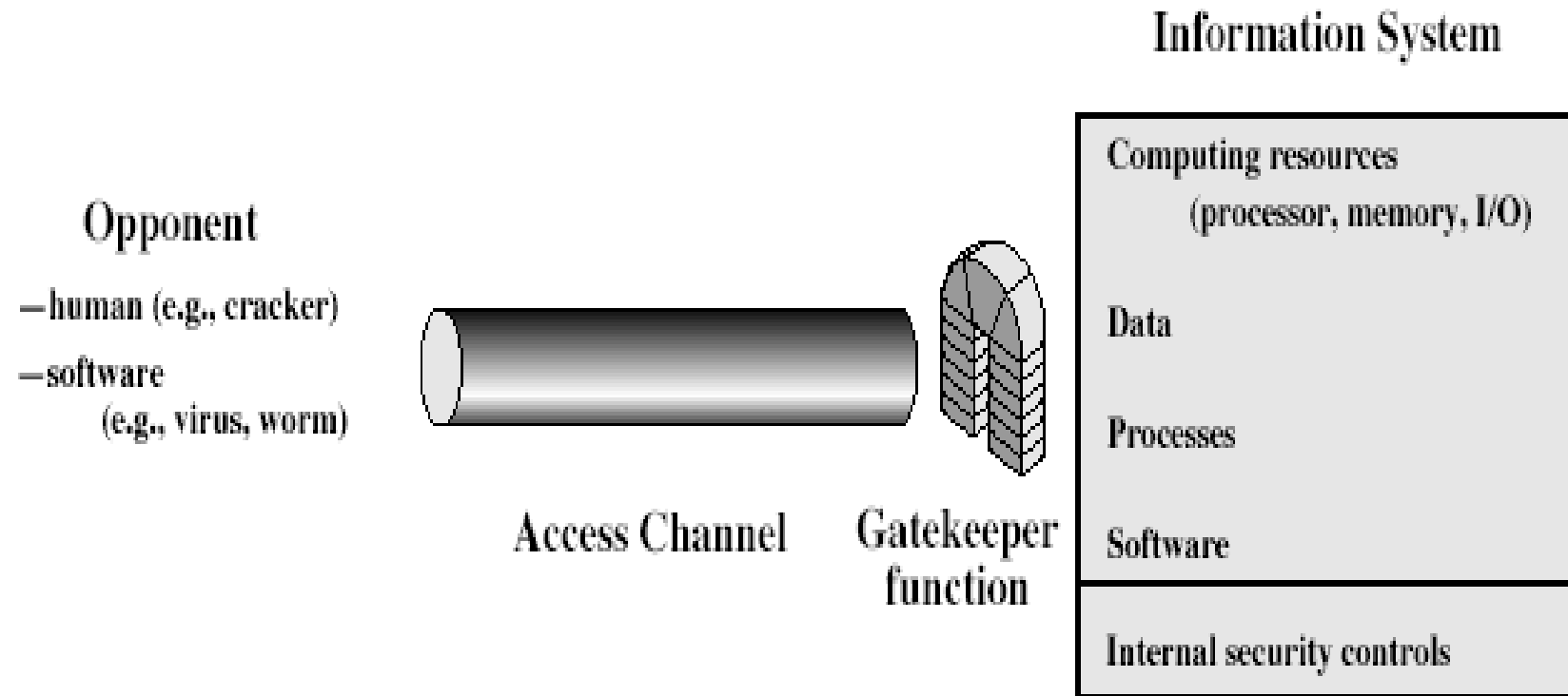
Model for Network Security



Model for Network Security

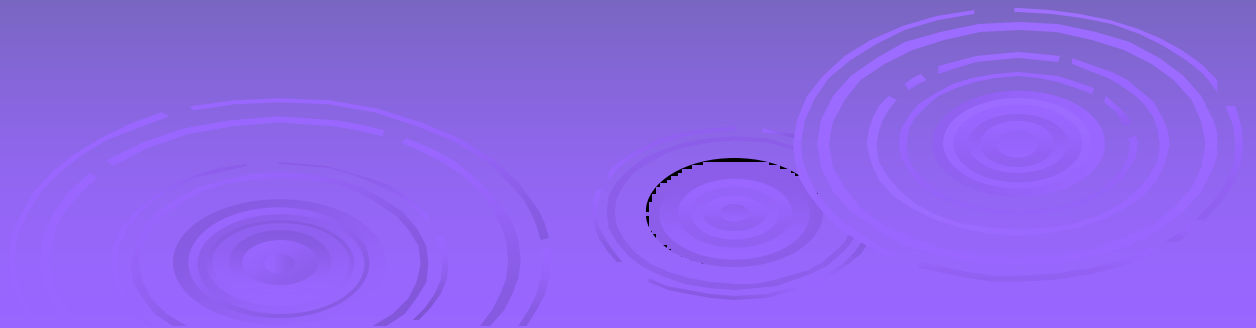
- using this model requires us to:
 1. design a suitable algorithm for the security transformation
 2. generate the secret information (keys) used by the algorithm
 3. develop methods to distribute and share the secret information
 4. specify a protocol enabling the principals to use the transformation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

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
 1. select appropriate gatekeeper functions to identify users
 2. implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems may be useful to help implement this model



Summary

- have considered:
 - definitions for:
computer, network, internet security
- X.800 standard
- security attacks, services, mechanisms
- models for network (access) security

