

Computer Network Security , ITC502, M1L1

Who is going to represent the user?

` Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

- Network Security / PRIVATE Communication in a PUBLIC World by Charlie Kaufman, Radia Perlman, & Mike Speciner (Prentice Hall 2002)

Why Computer Security

- The past decade has seen an explosion in the concern for the security of information
 - Malicious codes (viruses, worms, etc.) caused over \$28 billion in economic losses in 2003, and will grow to over \$75 billion by 2007
- Jobs and salaries for technology professionals have lessened in recent years. BUT ...
- Security specialists markets are expanding !
 - " Full-time information security professionals will rise almost 14% per year around the world, going past 2.1 million in 2008" (IDC report)

Why Computer Security (cont'd)

- Internet attacks are increasing in frequency, severity and sophistication
- Denial of service (DoS) attacks
 - Cost \$1.2 billion in 2000
 - 1999 CSI/FBI survey 32% of respondents detected DoS attacks directed to their systems
 - Thousands of attacks per week in 2001
 - Yahoo, Amazon, eBay, Microsoft, White House, etc., attacked

Why Computer Security (cont'd)

- Virus and worms faster and powerful
 - Melissa, Nimda, Code Red, Code Red II, Slammer ...
 - Cause over \$28 billion in economic losses in 2003, growing to over \$75 billion in economic losses by 2007.
 - Code Red (2001): 13 hours infected >360K machines - \$2.4 billion loss
 - Slammer (2003): 10 minutes infected > 75K machines - \$1 billion loss

Overview

- Course Administrative
- What is security: history and definition
- Security policy, mechanisms and services
- Security models

Logistics

- Class Room Teaching 3 hours per week
- Twelve weeks in semester.
- Assignments, Quiz and IA1, IA2
- Case studies, Discussion

Course Objective

- The basic concepts of computer and Network Security
- Various cryptographic algorithms including secret key management and different authentication techniques.
- Different types of malicious Software and its effect on the security.
- Various secure communication standards including IPsec, SSL/TLS and email.
- The Network management Security and Network Access Control techniques in Computer Security.
- Different attacks on networks and infer the use of firewalls and security protocols.

Course Outcomes

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
1	Explain the fundamentals concepts of computer security and network security.	L1, L2
2	Identify the basic cryptographic techniques using classical and block encryption methods.	L1
3	Study and describe the system security malicious software.	L1, L2
4	Describe the Network layer security, Transport layer security and application layer security.	L1, L2
5	Explain the need of network management security and illustrate the need for NAC.	L1, L2
6	Identify the function of an IDS and firewall for the system security.	L1, L2, L3

Prerequisite

- Basic concepts of Computer Networks & Network Design, Operating System.

-

References

- Textbooks:

- William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
- Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill.
- Mark Stamp's Information Security Principles and Practice, Wiley
- Bernard Menezes, "Cryptography & Network Security", Cengage Learning.

- References:

- Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, Wiley.
- Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.
- www.rsa.com

Module 0: Prerequisite

- Basic concepts of Computer Networks & Network Design, Operating System

Module I: Introduction to Network Security & cryptography

- Computer security and Network Security(Definition), CIA, Services, Mechanisms and attacks, The OSI security architecture, Network security model. Classical Encryption techniques (mono-alphabetic and poly-alphabetic substitution techniques: Vigenere cipher, playfair cipher, transposition techniques: keyed and keyless transposition ciphers). Introduction to steganography.
- **Self-learning Topics:** Study some more classical encryption techniques and solve more problems on all techniques. Homomorphic encryption in cloud computing

Module II: Cryptography: Key management, distribution and user authentication

- . Block cipher modes of operation, Data Encryption Standard, Advanced Encryption Standard (AES). RC5 algorithm.
- Public key cryptography: RSA algorithm.
Hashing Techniques: SHA256, SHA-512, HMAC and CMAC,
- Digital Signature Schemes - RSA, DSS. Remote user Authentication Protocols, Kerberos, Digital Certificate: X.509, PKI
- **Self-learning Topics:** Study working of elliptical curve digital signature and its benefits over RSA digital signature.

Module III: Malicious Software

- SPAM, Trojan horse, Viruses, Worms, System Corruption, Attack Agents, Information Theft, Trapdoor, Keyloggers, Phishing, Backdoors, Rootkits, Denial of Service Attacks, Zombie
- **Self-learning Topics:** Study the recent malicious software's and their effects.

Module IV: IP Security, Transport level security and Email Security

- IP level Security: Introduction to IPSec, IPSec Architecture, Protection Mechanism (AH and ESP), Transport level security: VPN. Need Web Security considerations, Secure Sockets Layer (SSL) Architecture, Transport Layer Security (TLS), HTTPS, Secure Shell (SSH) Protocol Stack. Email Security: Secure Email S/MIME
- Screen reader support enabled.
- **Self-learning Topics:** Study Gmail security and privacy from Gmail help

Module V: Network Management Security and Network Access Control

- Network Management Security:SNMPv3, NAC:Principle elements of NAC,Principle NAC enforcement methods, How to implement NAC Solutions, Use cases for network access control
- **Self-learning Topics:** Explore any open source network management security tool
-

Module VI: System Security

- IDS, Firewall Design Principles, Characteristics of Firewalls, Types of Firewalls
- Self-learning Topics: Study firewall rules table

Overview

- Course Administrative Trivia
- What is security: history and definition
- Security policy, mechanisms and services
- Security models

The History of Computing

- For a long time, security was largely ignored in the community
 - The computer industry was in "survival mode", struggling to overcome technological and economic hurdles
 - As a result, a lot of corners were cut and many compromises made
 - There was lots of theory, and even examples of systems built with very good security, but were largely ignored or unsuccessful
 - E.g., ADA language vs. C (powerful and easy to use)

Computing Today is Very Different

- Computers today are far from "survival mode"
 - Performance is abundant and the cost is very cheap
 - As a result, computers now ubiquitous at every facet of society
- Internet
 - Computers are all connected and interdependent
 - This codependency magnifies the effects of any failures

Biological Analogy

- Computing today is very homogeneous.
 - A single architecture and a handful of OS dominates
- In biology, homogeneous populations are in danger
 - A single disease or virus can wipe them out overnight because they all share the same weakness
 - The disease only needs a vector to travel among hosts
- Computers are like the animals, the Internet provides the vector.
 - It is like having only one kind of cow in the world, and having them drink from one single pool of water!

The Warhol Worm

- A properly designed worm can infect every vulnerable host on the Internet within 15 minutes
 - "How to own the Internet in your spare time"
(Staniford, Paxon and Weaver, Usenix Security 2002)
 - Exploit many vectors such as P2P file sharing, intelligent scanning, hitlists, etc.
 - Referred to as Warhol worm after Andy Warhol's quote "In the future, everyone will have 15 minutes of fame"

The Definition of Computer Security

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable
- Security rests on confidentiality, authenticity, integrity, and availability

The Basic

Components(Attributes)

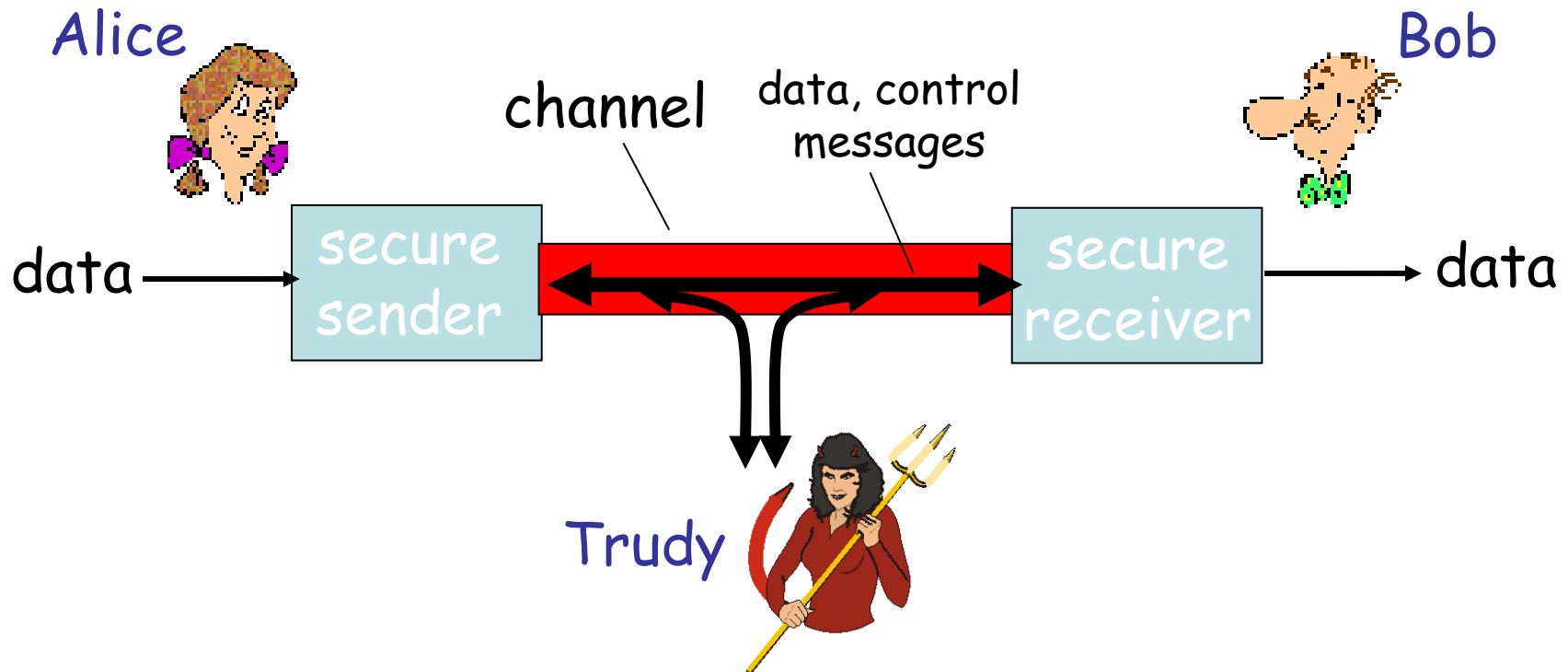
- **Confidentiality** is the concealment of information or resources.
 - E.g., only sender, intended receiver should "understand" message contents
- **Authenticity** is the identification and assurance of the origin of information.
- **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Availability** refers to the ability to use the information or resource desired.

Security Threats and Attacks

- A threat is a *potential* violation of security.
 - Flaws in design, implementation, and operation.
- An attack is any *action* that violates security.
 - Active adversary
- An attack has an implicit concept of "intent"
 - Router mis-configuration or server crash can also cause loss of availability, but they are not attacks

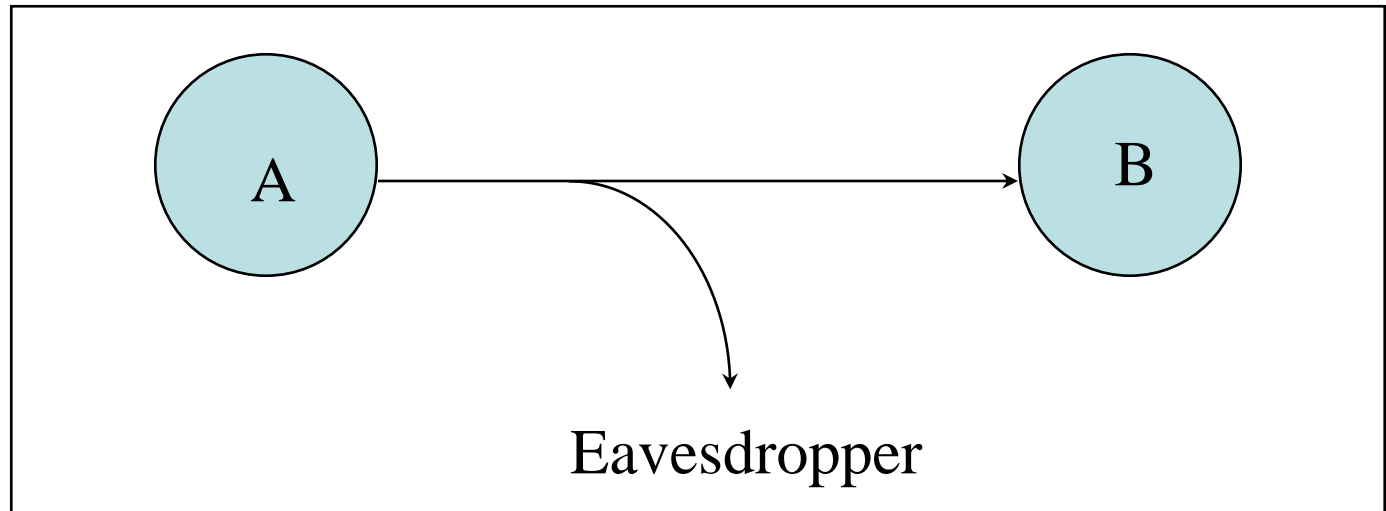
Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



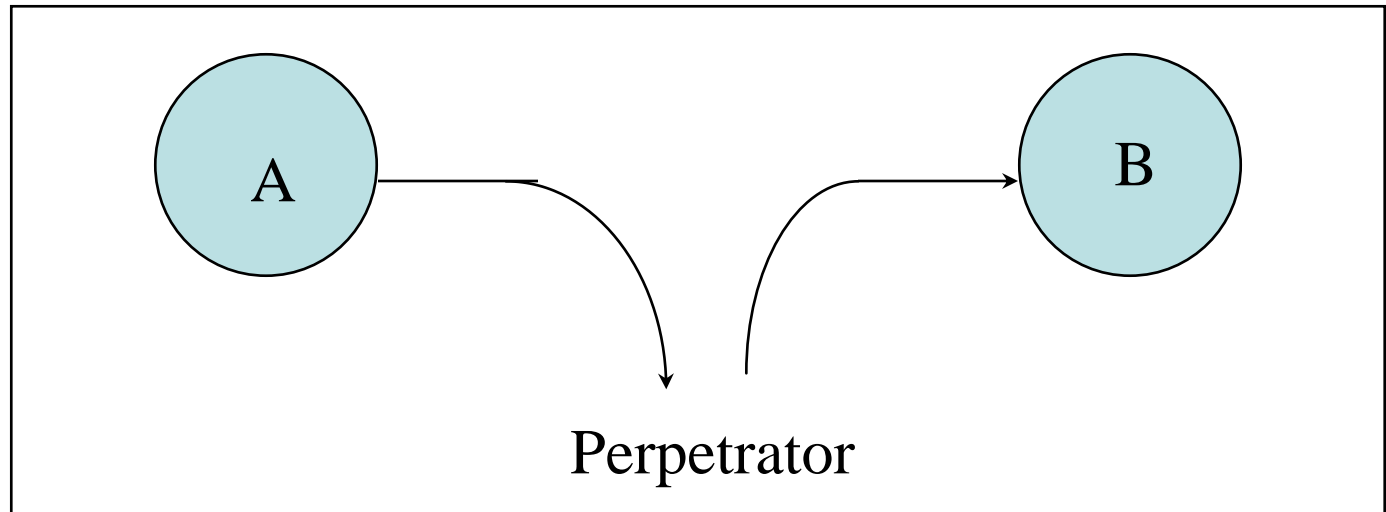
Eavesdropping - Message Interception (Attack on Confidentiality)

- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs



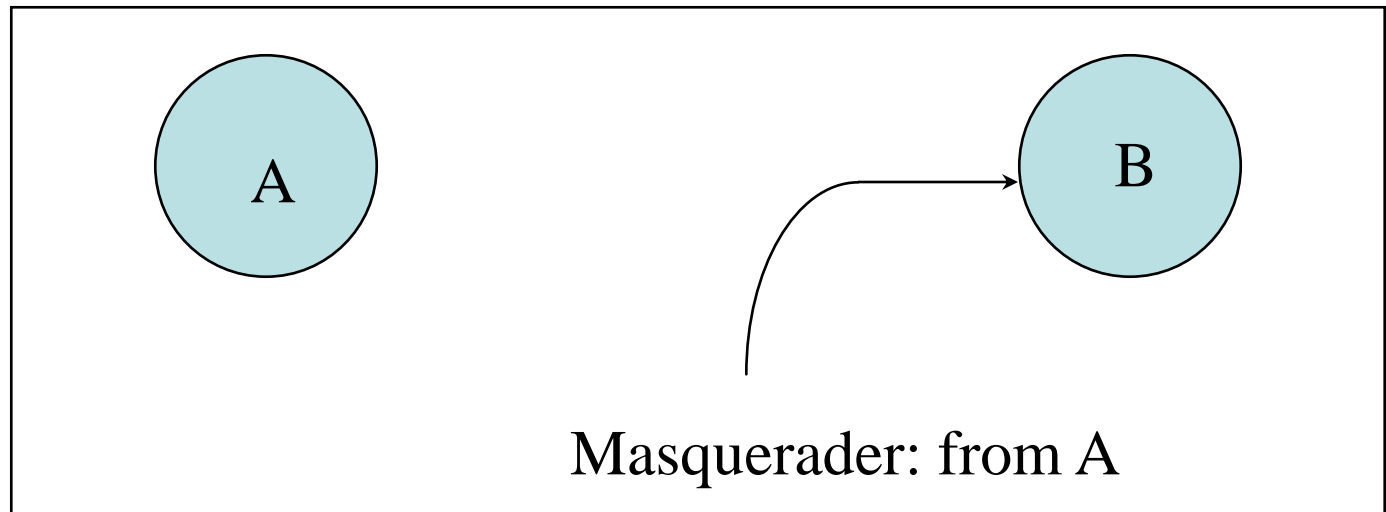
Integrity Attack - Tampering With Messages

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



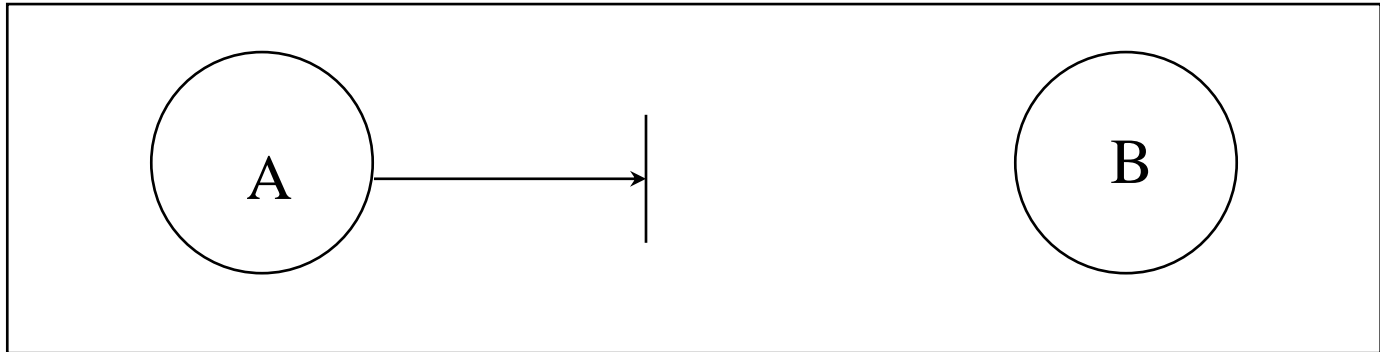
Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit



- *Blatant denial of service (DoS):*
 - Crashing the server
 - Overwhelm the server (use up its resource)

Classify Security Attacks as

- **Passive attacks** - eavesdropping on, or monitoring of, transmissions to:
 - obtain message contents, or
 - monitor traffic flows
- **Active attacks** - modification of data stream to:
 - masquerade of one entity as some other
 - replay previous messages
 - modify messages in transit
 - denial of service

Overview

- Course Administrative Trivia
- What is security: history and definition
- Security policy, mechanisms and services
- Security models

Security Policy and Mechanism

- **Policy**: a statement of what is, and is not allowed.
- **Mechanism**: a procedure, tool, or method of enforcing a policy.
- Security mechanisms implement functions that help *prevent, detect, and respond to recovery* from security attacks.
- Security functions are typically made available to users as a set of **security services** through APIs or integrated interfaces.
- Cryptography underlies many security mechanisms.

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
- X.800 defines security services in 5 major categories

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

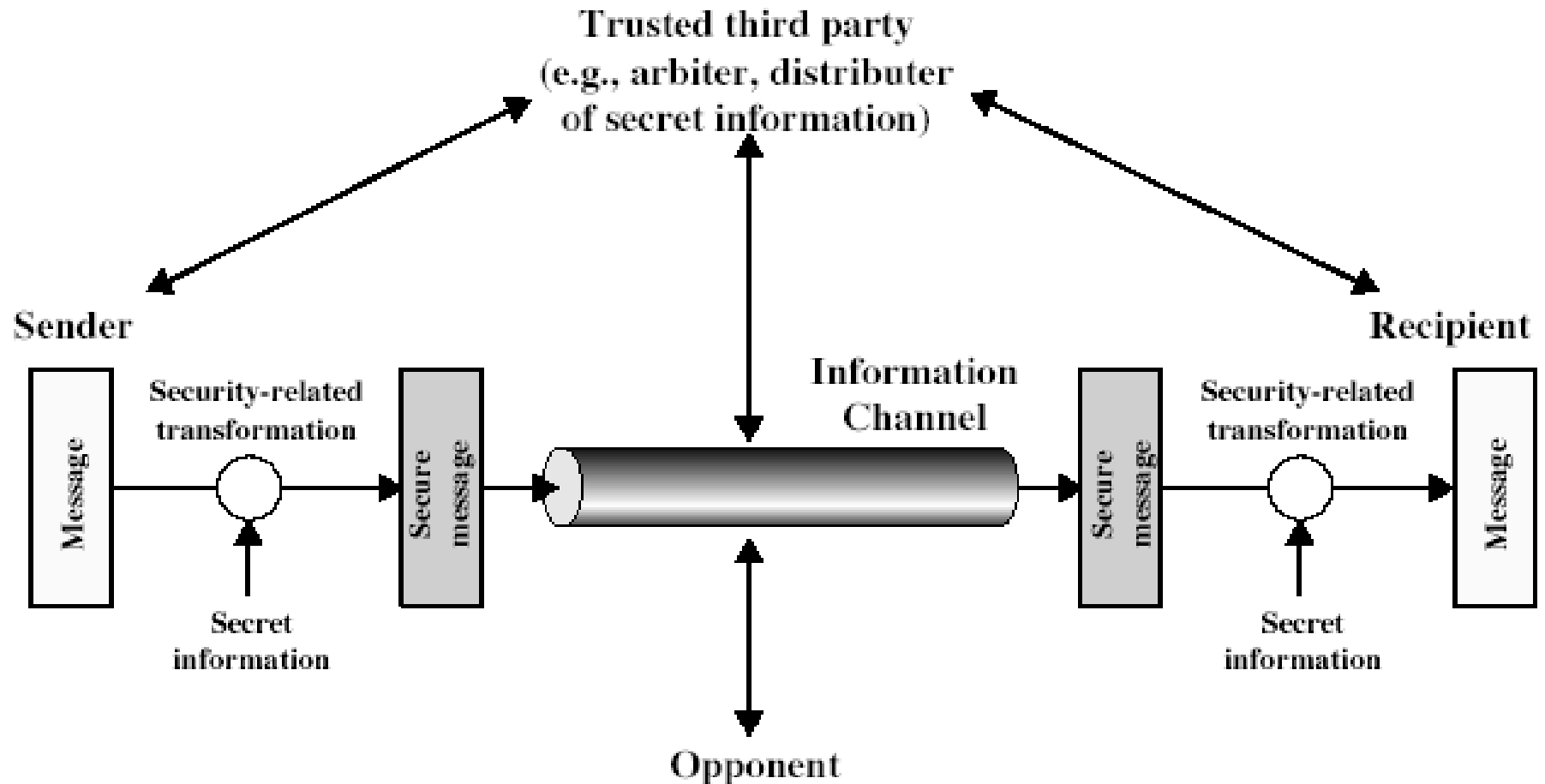
Security Mechanisms (X.800)

- 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

Overview

- Course Administrative Trivia
- What is security: history and definition
- Security policy, mechanisms and services
- Security models

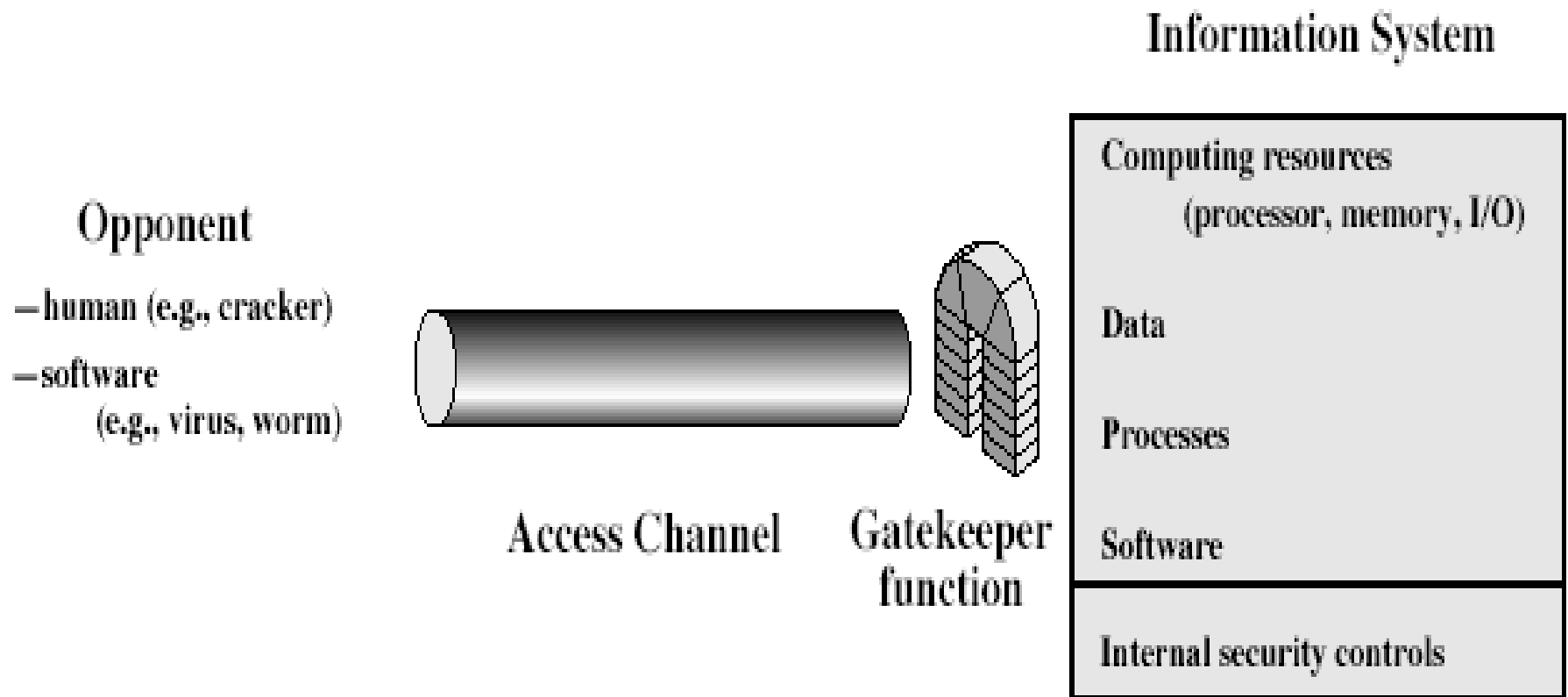
Model for Network Security



Model for Network Security

- Using this model requires us to:
 - Design a suitable algorithm for the security transformation
 - Generate the secret information (keys) used by the algorithm
 - Develop methods to distribute and share the secret information
 - 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:
 - Select appropriate gatekeeper functions to identify users
 - Implement security controls to ensure only authorised users access designated information or resources
- Trusted computer systems can be used to implement this model

How to Make a System Trustworthy

- Specification
 - A statement of desired functions
- Design
 - A translation of specifications to a set of components
- Implementation
 - Realization of a system that satisfies the design
- Assurance
 - The process to insure that the above steps are carried out correctly
 - Inspections, proofs, testing, etc.

The Security Life Cycle

- The *iterations* of
 - Threats
 - Policy
 - Specification
 - Design
 - Implementation
 - Operation and maintenance

7 Layers of the OSI Model

Application

- End User layer
- HTTP, FTP, IRC, SSH, DNS

Presentation

- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

Session

- Synch & send to port
- API's, Sockets, WinSock

Transport

- End-to-end connections
- TCP, UDP

Network

- Packets
- IP, ICMP, IPSec, IGMP

Data Link

- Frames
- Ethernet, PPP, Switch, Bridge

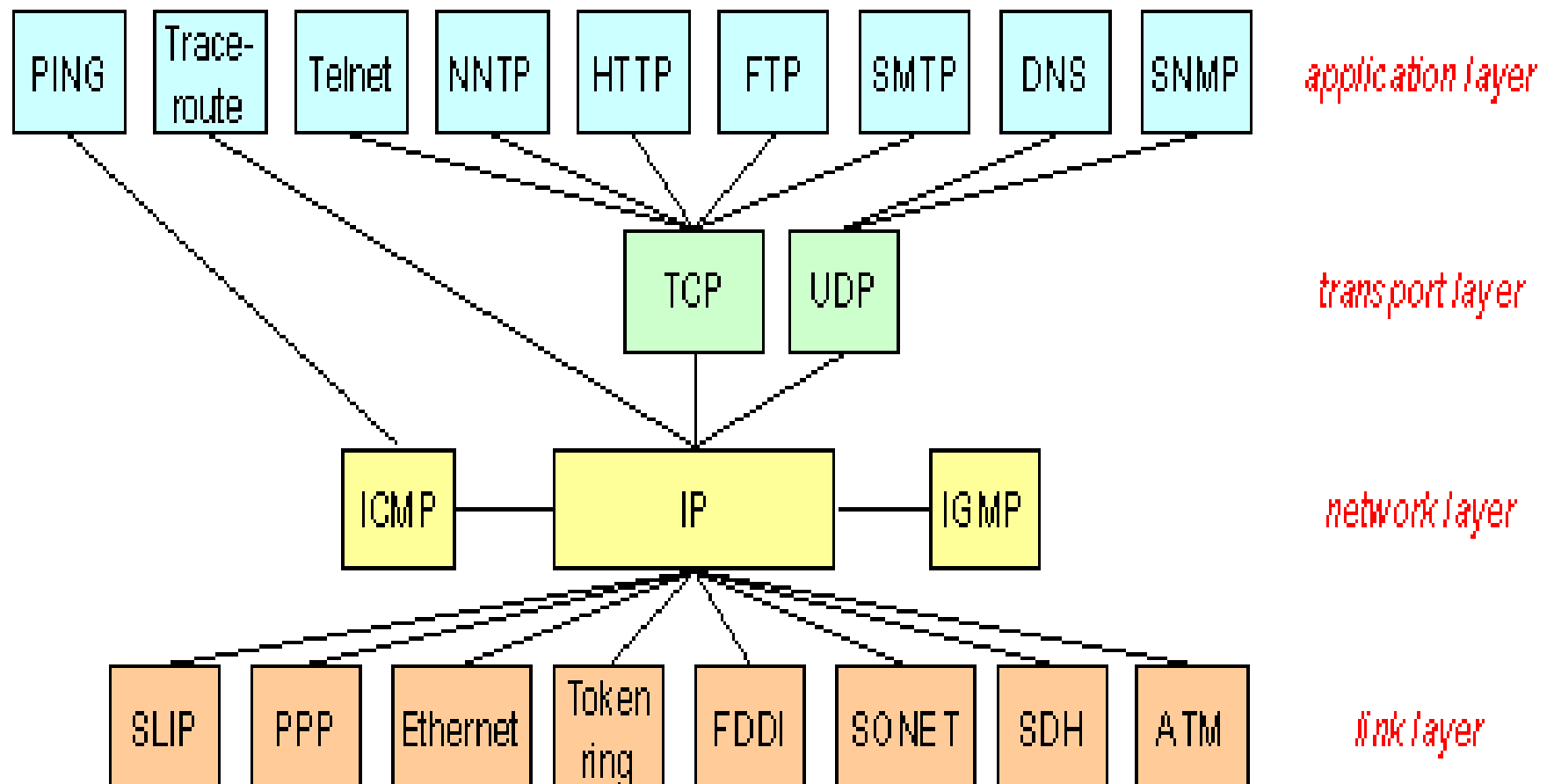
Physical

- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters

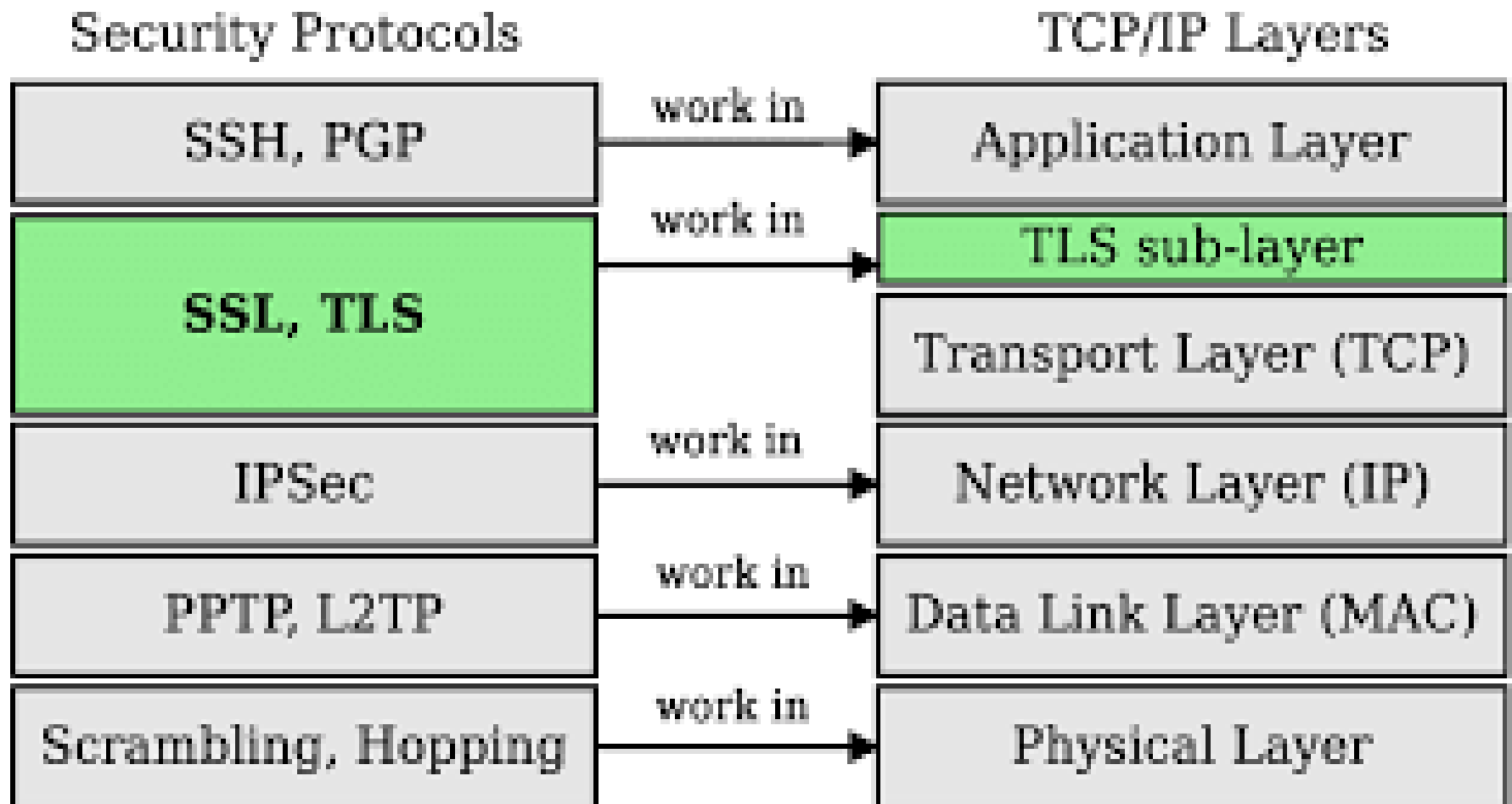
Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

OSI TCP/IP

OSI Layers	TCP/IP Layers	TCP/IP Protocols				
Application Layer	Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Presentation Layer						
Session Layer						
Transport Layer	Transport Layer	TCP		UDP		
Network Layer	Network Layer	IP				
Data Link Layer	Network Interface Layer	Ethernet	Token Ring		Other Link-Layer Protocols	
Physical Layer						



Security Protocols



M1L2

Classical Encryption Techniques

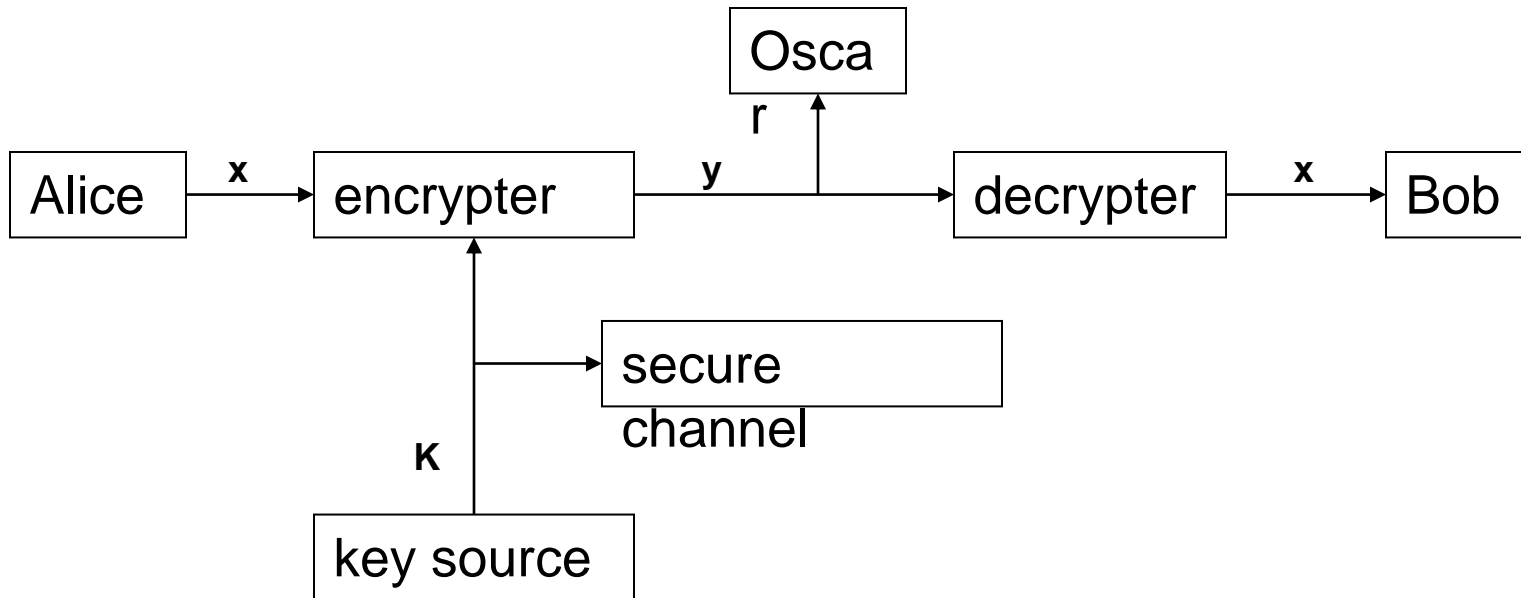
Introduction:
Some Simple Cryptosystems

Outline

- **[1] Introduction: Some Simple Cryptosystems**
 - <1> The Shift Cipher
 - <2> The Substitution Cipher
 - <3> The Affine Cipher
 - <4> The Vigenère Cipher
 - <5> The Hill Cipher
 - <6> The Permutation Cipher
 - <7> Stream Ciphers
- **[2] Cryptanalysis**
 - <1> Cryptanalysis of the Affine Cipher
 - <2> Cryptanalysis of the Substitution Cipher
 - <3> Cryptanalysis of the Vigenère Cipher
 - <4> Cryptanalysis of the Hill Cipher
 - <5> Cryptanalysis of the LFSR Stream Cipher

Introduction: Some Simple Cryptosystems

- [1] Introduction



Introduction:

Some Simple Cryptosystems

- Definition 1.1: A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfies
 - \mathcal{P} is a finite set of possible *plaintexts*
 - \mathcal{C} is a finite set of possible *ciphertexts*
 - \mathcal{K} , the *keyspace*, is a finite set of possible *keys*
 - For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$

-

$$e_K : \mathcal{P} \rightarrow \mathcal{C}$$

$$d_K : \mathcal{C} \rightarrow \mathcal{P}$$

- $d_K(e_K(x)) = x$ for every plaintext $x \in \mathcal{P}$

Introduction:

Some Simple Cryptosystems

- Definition 1.2: a and b are integers,
 m is a positive integer
 - congruence: $a \equiv b \pmod{m}$ if m divides $b-a$
- Z_m : the set $\{0, 1, \dots, m-1\}$
 - with 2 operations $+$ and \times
 - $10+20=4$ in Z_{26} ($10+20 \bmod 26=4$)
 - $10 \times 20=18$ in Z_{26} ($10 \times 20 \bmod 26=18$)

Introduction:

Some Simple Cryptosystems

- <1> Shift Cipher
 - Cryptosystem 1.1: Shift Cipher
 - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$
 - $K, x, y \in \mathbb{Z}_{26}$
 - $e_K(x) = (x + K) \bmod 26$
 - $d_K(y) = (y - K) \bmod 26$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Introduction:

Some Simple Cryptosystems

- eg.: Suppose $K=11$
 - Plaintext: student
 - Ciphertext: DEFOPZE

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
+K	3	4	5	14	15	25	4
ciphertext	D	E	F	O	P	Z	E

K=5, 17, information technology

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Introduction:

Some Simple Cryptosystems

- <2> Substitution Cipher
 - Cryptosystem 1.2: Substitution Cipher
 - $P=C=Z_{26}$
 - K : all possible permutations of the 26 symbols
 - For each $\pi \in K$
 - $e_{\pi}(x)=\pi(x)$
 - $d_{\pi}(y)=\pi^{-1}(y)$
- where π^{-1} is the inverse permutation to π

Introduction:

Some Simple Cryptosystems

- eg.:

x	a	b	C	d	e	f	g	h	i	j	k	l	m
$e_{\pi}(x)$	X	N	Y	A	H	P	O	G	Z	Q	W	B	T
x	n	o	p	q	r	s	t	u	v	w	x	y	z
$e_{\pi}(x)$	S	F	L	R	C	V	M	U	E	K	J	D	I

- Plaintext: student, information, **your name**
- Ciphertext: VMUSHSM , ZSPFCTXMZFS , ?

Introduction:

Some Simple Cryptosystems

- <3> Affine Cipher

- Theorem 1.1: $ax \equiv b \pmod{m}$ has a unique solution $x \in \mathbb{Z}_m$ for every $b \in \mathbb{Z}_m$ iff $\gcd(a, m) = 1$

- Definition 1.3: Suppose $a \geq 1$ and $m \geq 2$ are integers

- a and m are *relatively prime* if $\gcd(a, m) = 1$

- $\phi(m)$: the number of integers in \mathbb{Z}_m that are relatively prime to m

$$m = \prod_{i=1}^n p_i^{e_i}$$

- Theorem 1.2: Suppose

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1})$$

Introduction:

Some Simple Cryptosystems

- Definition 1.4: Suppose $a \in \mathbb{Z}_m$
 - $a^{-1} \bmod m$:
the multiplicative inverse of a modulo m
 - $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$
- Cryptosystem 1.3: Affine Cipher
 - $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
 - $\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$
 - For $K = (a, b) \in \mathcal{K}$; $x, y \in \mathbb{Z}_{26}$
 - $e_K(x) = (ax + b) \bmod 26$
 - $d_K(y) = a^{-1}(y - b) \bmod 26$

Introduction:

Some Simple Cryptosystems

- e.g.: Suppose $K=(7,3)$

- $7^{-1} \bmod 26 = 15$

- Plaintext: student, **Information**

$$e_K(x) = (7x+3) \bmod 26$$

- Ciphertext: ZGNYFQG

$$d_K(y) = 15(y-3) \bmod 26$$

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
$e_K(x)$	25	6	13	24	5	16	6
ciphertext	Z	G	N	Y	F	Q	G

Introduction:

Some Simple Cryptosystems

- <4> Vigenère Cipher (poly alphabetic substitution cipher)
 - Cryptosystem 1.4: Vigenère Cipher
 - m : a positive integer
 - $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
 - For a key $K = (k_1, k_2, \dots, k_m)$
 - $e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
 - $d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$

Example Vigenere Cipher

$$C_i = (P_i + k_i) \bmod 26$$

Key: venus; **Plain text:** college vasai,

Cipher Text: XSYFWBIIOKVM

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

PlainText	C	O	L	L	E	G	E	V	A	S	A	I
P value	2	14	11	11	4	6	4	21	0	18	0	8
Key	V	E	N	U	S	V	E	N	U	S	V	E
K value	21	4	13	20	18	21	4	13	14	18	21	4
C value	23	18	24	5	22	1	8	8	14	10	21	12
Cipher	X	S	Y	F	W	B	I	I	O	K	V	M

Vigenère Square

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Introduction:

Some Simple Cryptosystems

- e.g.: Suppose $m=4$ and $K=(2,8,15,7)$
 - Plaintext: student, **technology**
 - Ciphertext: UBJKGVI

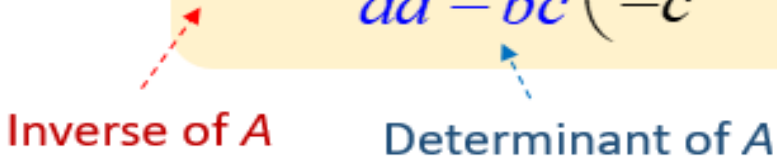
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
+K	2	8	15	7	2	8	15
ciphertext	20	1	9	10	6	21	8

Matrix operations

Inverse of 2x2 Matrix

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$



Inverse of A Determinant of A

$$AA^{-1} = A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \text{Identity Matrix}$$

If $ad - bc = 0$ then A^{-1} cannot be found and A is a **singular matrix**.

If $ad - bc \neq 0$ then A^{-1} can be found and A is a **non-singular matrix**.

How to multiply matrices

$$\begin{bmatrix} -2 & 1 \\ 0 & 4 \end{bmatrix} \times \begin{bmatrix} 6 & 5 \\ -7 & 1 \end{bmatrix} = \begin{bmatrix} -2 \times 6 + 1 \times -7 & -2 \times 5 + 1 \times 1 \\ 0 \times 6 + 4 \times -7 & 0 \times 5 + 4 \times 1 \end{bmatrix}$$

$$= \begin{bmatrix} -19 & -9 \\ -28 & 4 \end{bmatrix}$$

Introduction:

Some Simple Cryptosystems

- <5> Hill Cipher
 - Definition 1.5: Suppose $A=(a_{i,j})$ is an $m \times m$ matrix
 - $A_{i,j}$: the matrix obtained from A by deleting the i th row and the j th column
 - $\det A$: the determinant of A
 - $m=1$: $\det A=a_{1,1}$ $\det A = \sum_{j=1}^m (-1)^{i+j} a_{i,j} \det A_{i,j}$
 - $m>1$: for any fixed i

Introduction:

Some Simple Cryptosystems

- Theorem 1.3: Suppose $K=(k_{i,j})$ is an $m \times m$ invertible matrix over \mathbb{Z}_n

- $K^{-1}=(\det K)^{-1}K^*$

- e.g.: $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ $K_{1,2} = 3 \quad \therefore \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

$$K^* = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \qquad \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

- $\det K = 11 \times 7 - 8 \times 3 \pmod{26} = 1$

- $K^{-1}=(\det K)^{-1}K^*=$

Introduction:

Some Simple Cryptosystems

- Cryptosystem 1.5: Hill Cipher (Lester Hill 1929)
 - $M \geq 2$ is an integer
 - $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^M$
 - $\mathcal{K} = \{M \times M \text{ invertible matrices over } \mathbb{Z}_{26}\}$
 - For a key K
 - $e_K(x) = xK$
 - $d_K(y) = yK^{-1}$
- where K^{-1} is the inverse of K

Introduction:

Some Simple Cryptosystems

- e.g.:

$$K = \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}, \quad K^{-1} = \begin{pmatrix} 21 & 15 & 17 \\ 23 & 2 & 16 \\ 25 & 4 & 3 \end{pmatrix}$$

- Plaintext: GOD (6 14 3)
- Ciphertext: WTJ (22 19 9)

$$(6 \quad 14 \quad 3) \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix} = (22 \quad 19 \quad 9)$$

Introduction:

Some Simple Cryptosystems

- <6> Permutation Cipher
 - Cryptosystem 1.6: Permutation Cipher
 - m is a positive integer
 - $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
 - \mathcal{K} consist of all permutations of $\{1, \dots, m\}$
 - For a key(a permutation) π

$$d_{\pi}(y_1, \dots, y_m) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)})$$
$$- e_{\pi}(x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)})$$

where π^{-1} is the inverse permutation to π

Introduction:

Some Simple Cryptosystems

- e.g.: Suppose $m=6$
 - Plaintext: CYBERFORMULA
 - Ciphertext: BRCFEYMLOAUR

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

plaintext	C	Y	B	E	R	F	O	R	M	U	L	A
ciphertext	B	R	C	F	E	Y	M	L	O	A	U	R

Introduction:

Some Simple Cryptosystems

- <7> Stream Ciphers
 - Block ciphers

Plaintext string $x = x_1 x_2 \dots$ (each x_i is a plaintext)

Ciphertext string $y = y_1 y_2 \dots = e_k(x_1) e_k(x_2) \dots$

- Stream ciphers
- Plaintext string $x = x_1 x_2 \dots$

Generate a keystream (by using some K) $z = z_1 z_2 \dots$

Ciphertext string $y = y_1 y_2 \dots = e_{z_1}(x_1) e_{z_2}(x_2) \dots$

Introduction:

Some Simple Cryptosystems

- Definition 1.6: A synchronous stream cipher is a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, E, D)$ with a function g
 - \mathcal{P} : a finite set of possible plaintexts
 - \mathcal{C} : a finite set of possible ciphertexts
 - \mathcal{K} : a finite set of possible keys
 - \mathcal{L} : a finite set called the keystream alphabet
 - g : the keystream generator
 - Input: K
 - g generates an infinite string $z_1 z_2 \dots$

Introduction:

Some Simple Cryptosystems

- Definition 1.6 (cont.)
 - For each $z \in \mathcal{L}$, there is an encryption rule $e_z \in \mathcal{E}$ and a corresponding decryption rule $d_z \in \mathcal{D}$
 - $e_K : \mathcal{P} \rightarrow \mathcal{C}$
 - $d_K : \mathcal{C} \rightarrow \mathcal{P}$
 - $d_z(e_z(x)) = x$ for every plaintext $x \in \mathcal{P}$

Introduction:

Some Simple Cryptosystems

- Vigenère Cipher can be defined as a synchronous stream cipher

- $\mathcal{K} = (\mathbb{Z}_{26})^m$

- $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_{26}$

- $e_z(x) = (x+z) \bmod 26$

- $d_z(y) = (y-z) \bmod 26$

- Keystream $z_1 z_2 \dots$

$$= k_1 k_2 \dots k_m k_1 k_2 \dots k_m k_1 k_2 \dots k_m \dots$$

$$z_i = \begin{cases} k_i & \text{if } 1 \leq i \leq m \\ z_{i-m} & \text{if } i \geq m+1 \end{cases}$$

Introduction:

Some Simple Cryptosystems

- Keystream can be produced efficiently in hardware using a LFSR (Linear Feedback Shift Register)
 - k_1 would be tapped as the next keystream bit
 - k_2, \dots, k_m would each be shifted 1 stage to the left
 - The new value of k_m would be

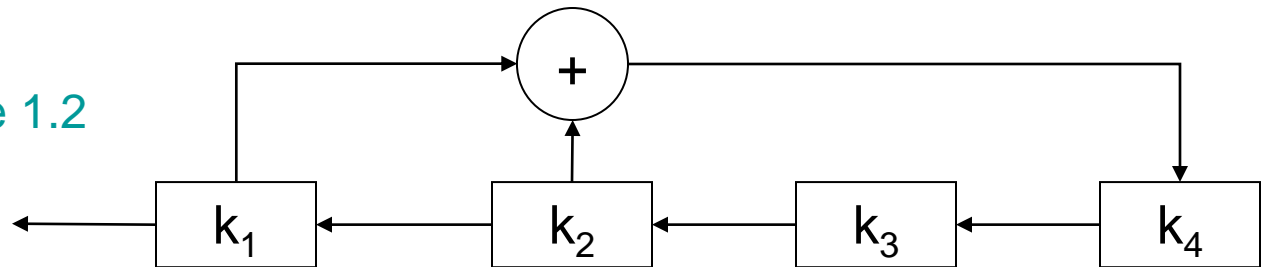
$$\sum_{j=0}^{m-1} c_j k_{j+1}$$

this is “linear feedback“ (see Figure 1.2)

- This system is modulo 2

Introduction: Some Simple Cryptosystems

Figure 1.2



- e.g.: in Figure 1.2, suppose $K=(1,0,0,0)$
 - $c_0=1, c_1=1, c_2=0, c_3=0$
 - The keystream is
100010011010111...

Introduction:

Some Simple Cryptosystems

- Non-synchronous stream cipher:
 - Each keystream element z_i depends on previous plaintext or ciphertext elements
- cryptosystem 1.7: Autokey Cipher
 - $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$
 - $z_1 = K, z_i = x_{i-1}$ for all $i > 1$
 - For $x, y, z \in \mathbb{Z}_{26}$
 - $e_z(x) = (x + z) \bmod 26$
 - $d_z(y) = (y - z) \bmod 26$

Introduction:

Some Simple Cryptosystems

- e.g.: Suppose $K=8$
 - Plaintext: student
 - Ciphertext: ALNXHRG

plaintext	s	t	u	d	e	n	t
	18	19	20	3	4	13	19
keystream	8	18	19	20	3	4	13
ciphertext	0	11	13	23	7	17	6
	A	L	N	X	H	R	G

Steganography

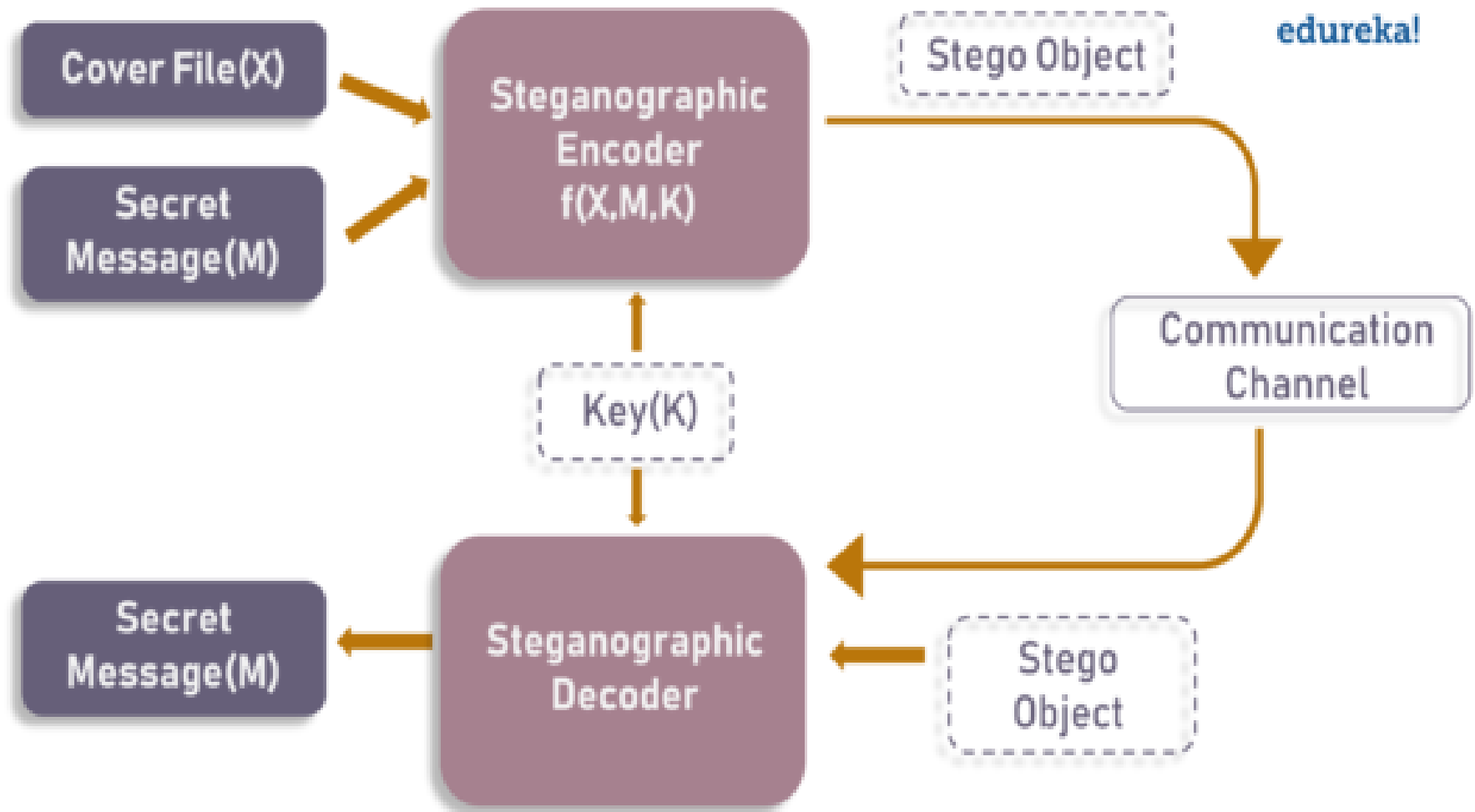
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.

The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

What is Steganography?

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message

Basic Steganographic Model.



Steganography Techniques

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

Steganography different from Cryptography ?

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

Question Bank

1. What is the OSI security architecture?
2. What is the difference between passive and active security threats?
3. List and briefly define categories of passive and active security attacks.
4. List and briefly define categories of security services.
5. List and briefly define categories of security mechanisms.
6. What are the essential ingredients of a symmetric cipher?
7. What are the two basic functions used in encryption algorithms?
8. How many keys are required for two people to communicate via a cipher?
9. What is the difference between a block cipher and a stream cipher?
10. What are the two general approaches to attacking a cipher?

11. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
12. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
13. Briefly define the Caesar cipher.
14. Briefly define the monoalphabetic cipher.
15. Briefly define the Playfair cipher

