

2017 REGULATION

IV YEAR/VII SEMESTER

1

CS8792 – Cryptography and Network Security

Handled by

Dr.M.K.Sandhya

Professor, CSE

Meenakshi Sundararajan Engineering College

Why ?

- ▶ Protect Data from Theft
 - ▶ Sensitive and critical data
- ▶ Career opportunities



Course Outcomes

At the end of the course, the student should be able to

- ▶ Understand the fundamentals of networks security, security architecture, threats and vulnerabilities
- ▶ Apply the different cryptographic operations of symmetric cryptographic algorithms
- ▶ Apply the different cryptographic operations of public key cryptography
- ▶ Apply the various Authentication schemes to simulate different applications.
- ▶ Understand various Security practices and System security standards

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Course Outcome – Unit I

- Understand the fundamentals of networks security, security architecture, threats and vulnerabilities

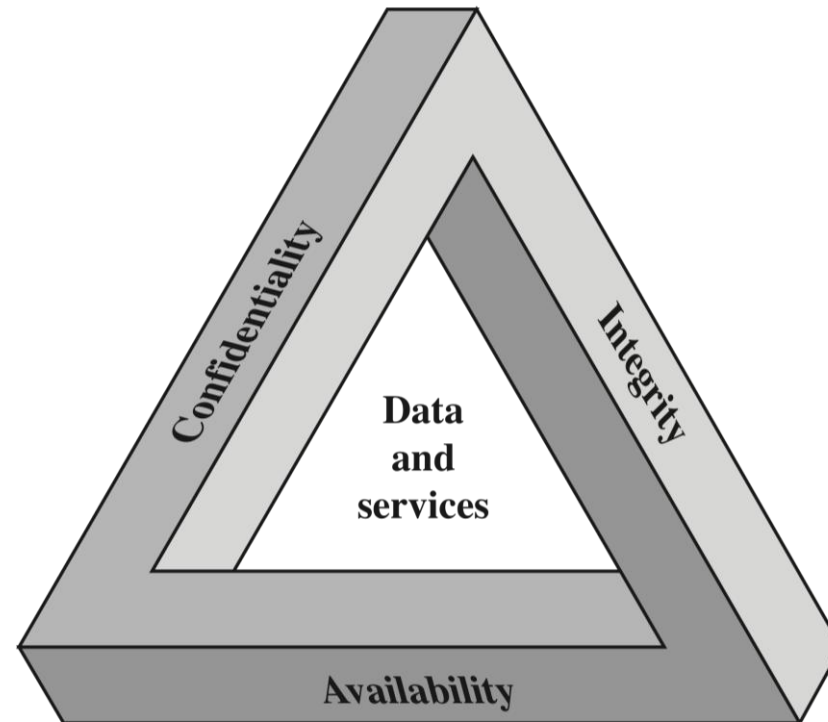


Security

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



CIA Triad



Computer Security Objectives

8

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
 - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
 - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
 - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Possible additional concepts:

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Threats and Attacks



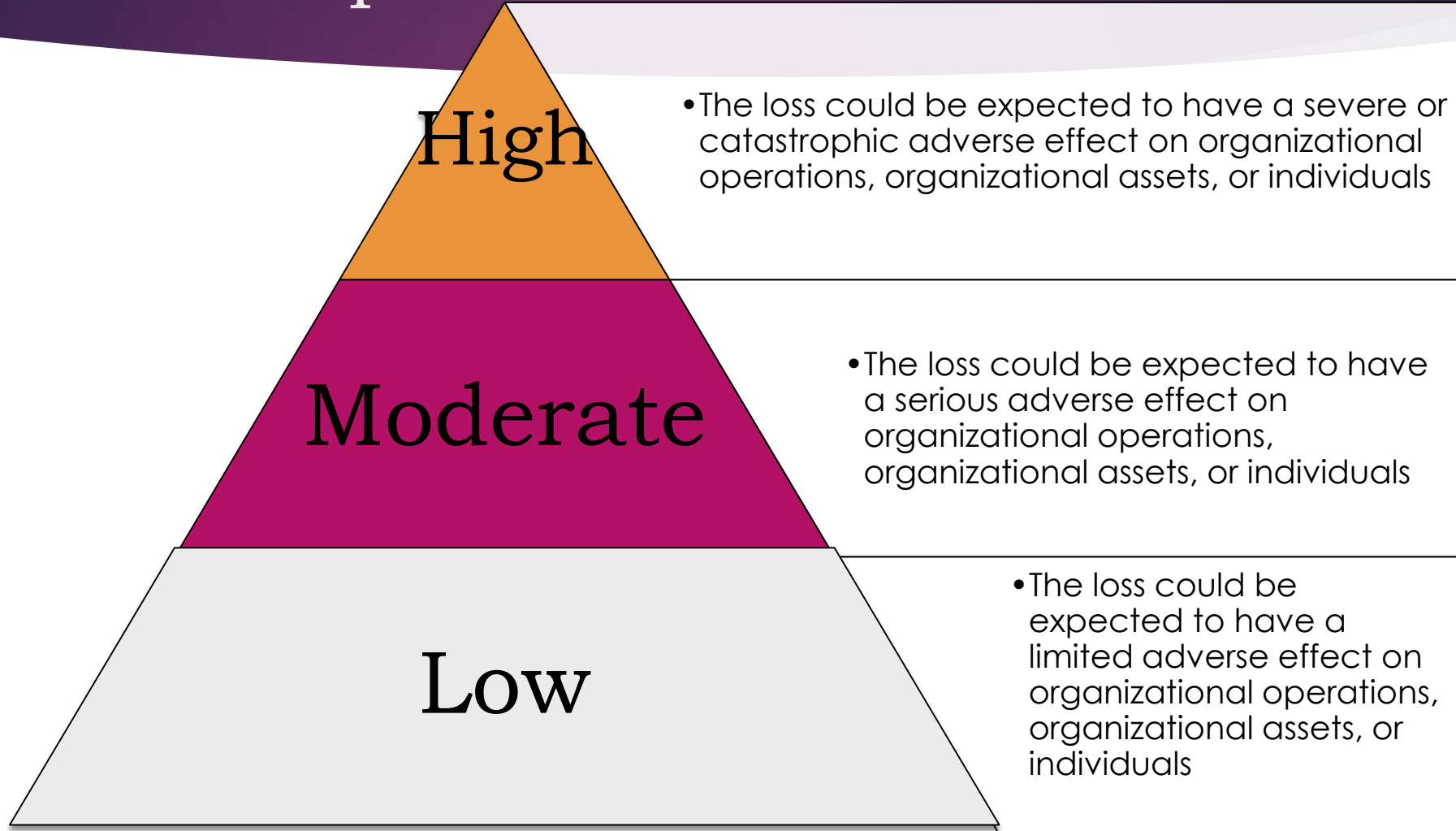
Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Breach of Security Levels of Impact

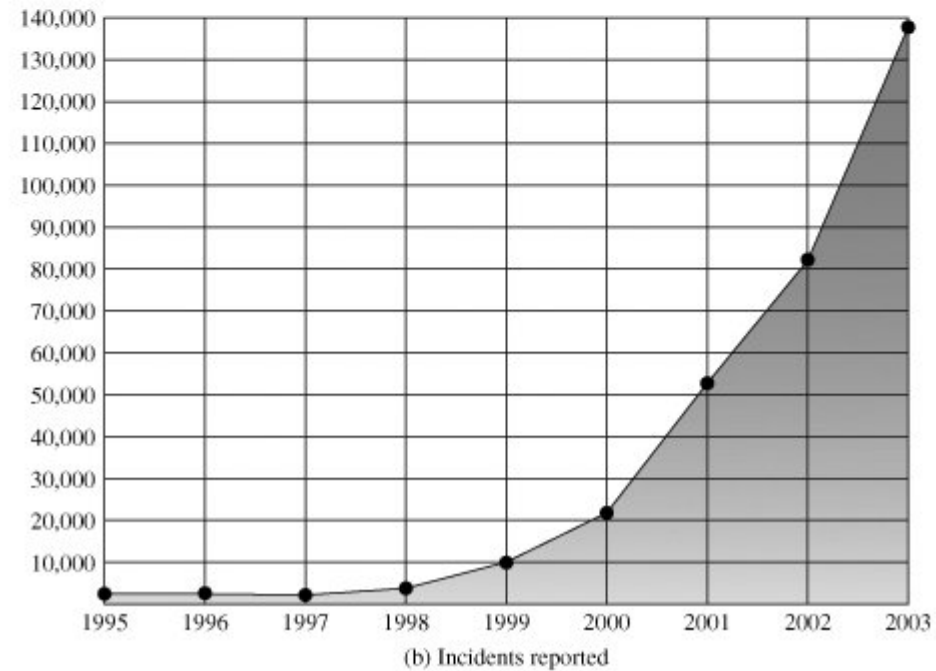
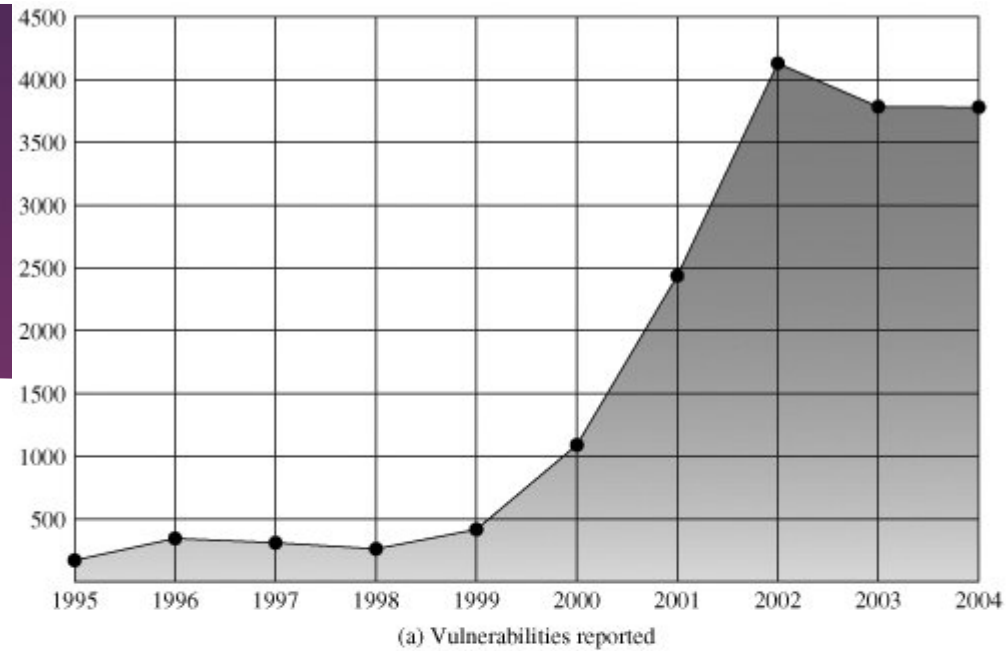


Unit I - Introduction

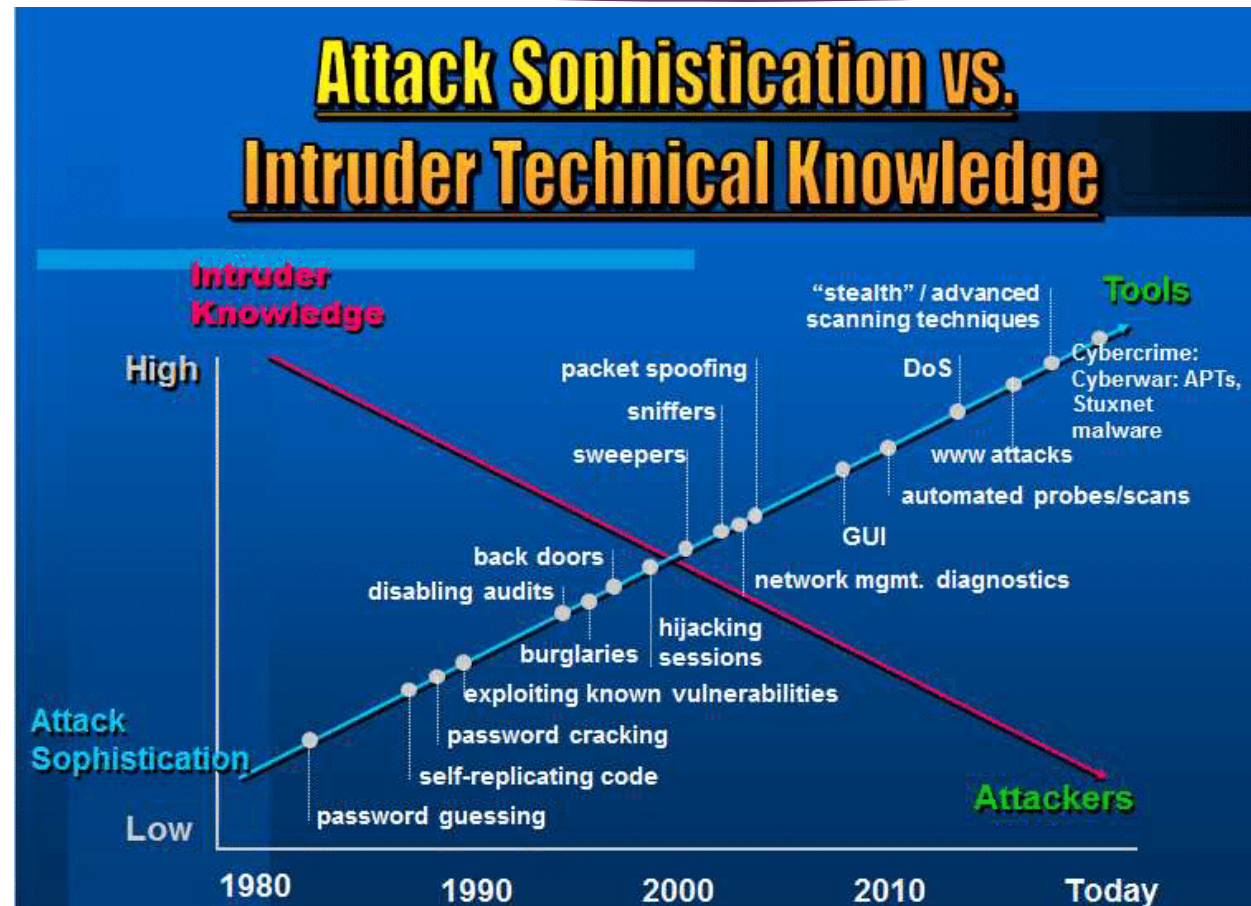
- ▶ **Security trends**
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Security Trends

- Computer Emergency Response Team (CERT) Coordination Center (CERT/CC)



Security Trends



Unit I - Introduction

- ▶ Security trends
- ▶ **Legal, Ethical and Professional Aspects of Security**
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Legal, Ethical and Professional Aspects of Security

16

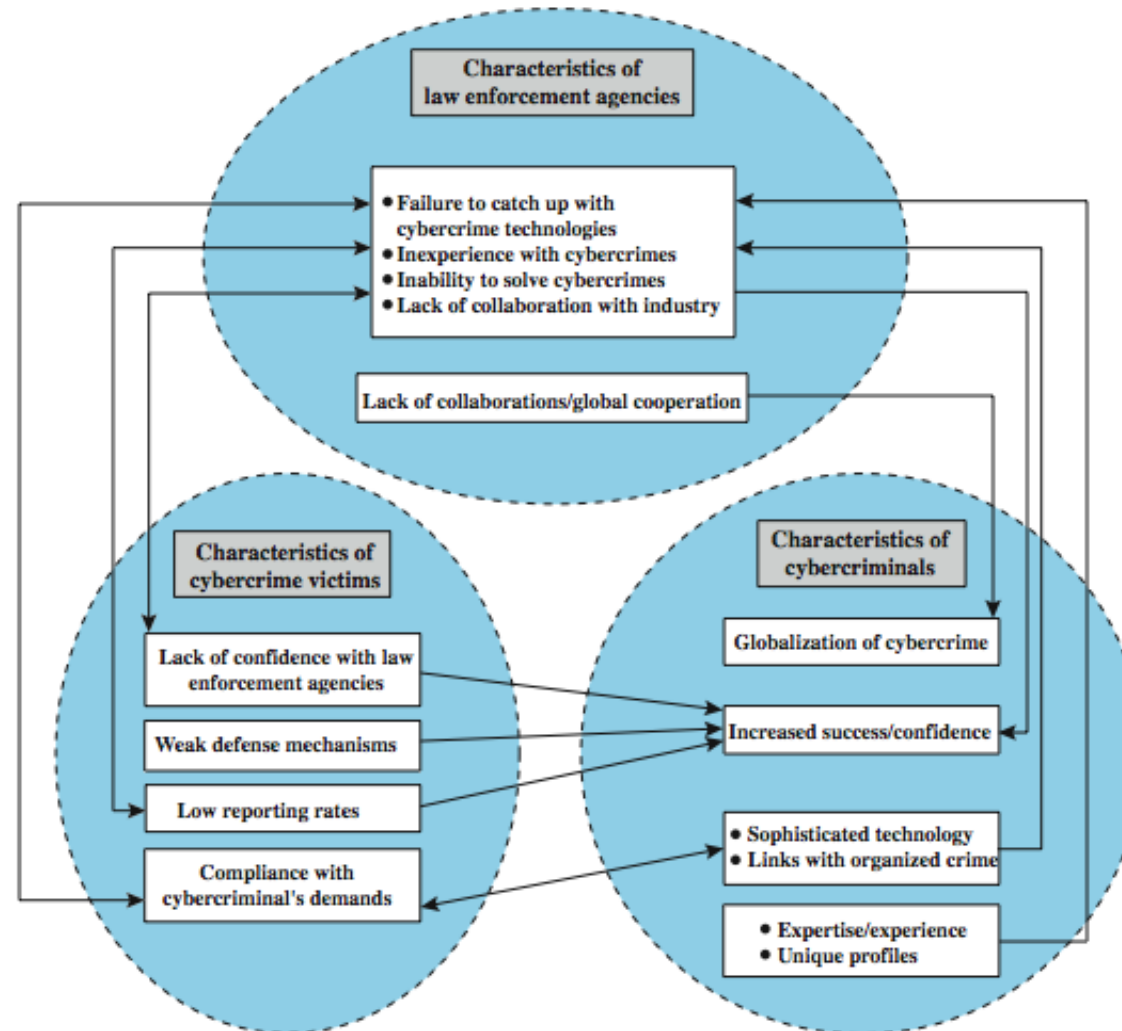
- ▶ Cybercrime and computer crime
- ▶ Intellectual property issues
- ▶ Privacy
- ▶ Ethical issues

Cybercrime / Computer Crime

- ▶ “criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity”
- ▶ categorize based on computer's role:
 - ▶ as target
 - ▶ as storage device
 - ▶ as communications tool

Law Enforcement Challenges

18



Intellectual Property

Patents

**Unauthorized
making,
using or selling**

Trademarks

**Unauthorized use or
colorable imitation**

Copyrights

Unauthorized use

Copyright

- protects tangible or fixed expression of an idea but not the idea itself
- is automatically assigned when created
- may need to be registered in some countries
- exists when:
 - proposed work is original
 - creator has put original idea in concrete form
 - e.g. literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphic, and sculptural works, motion pictures and other audiovisual works, sound recordings, architectural works, software-related works.

Copyright Rights

- copyright owner has these exclusive rights, protected against infringement:
 - reproduction right
 - modification right
 - distribution right
 - public-performance right
 - public-display right

Patents

- Grant a property right to the inventor
 - to exclude others from making, using, offering for sale, or selling the invention
- Types:
 - utility - any new and useful process, machine, article of manufacture, or composition of matter
 - design - new, original, and ornamental design for an article of manufacture
- e.g. RSA public-key cryptosystem patent

Trademarks

- a word, name, symbol, or device
 - used in trade with goods
 - indicate source of goods
 - to distinguish them from goods of others
- trademark rights may be used to:
 - prevent others from using a confusingly similar mark
 - but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark

Intellectual Property Issues and Computer Security

- Software programs
 - Protect using copyright, perhaps patent
- Database content and arrangement
 - Protect using copyright
- Digital content audio / video / media / web
 - Protect using copyright
- Algorithms
 - May be able to protect by patenting

U.S. Digital Millennium Copyright ACT (DMCA)

- implements WIPO treaties to strengthens protections of digital copyrighted materials
- encourages copyright owners to use technological measures to protect their copyrighted works, including:
 - measures that prevent access to the work
 - measures that prevent copying of the work
- prohibits attempts to bypass the measures
 - have both criminal and civil penalties for this

DMCA Exemptions

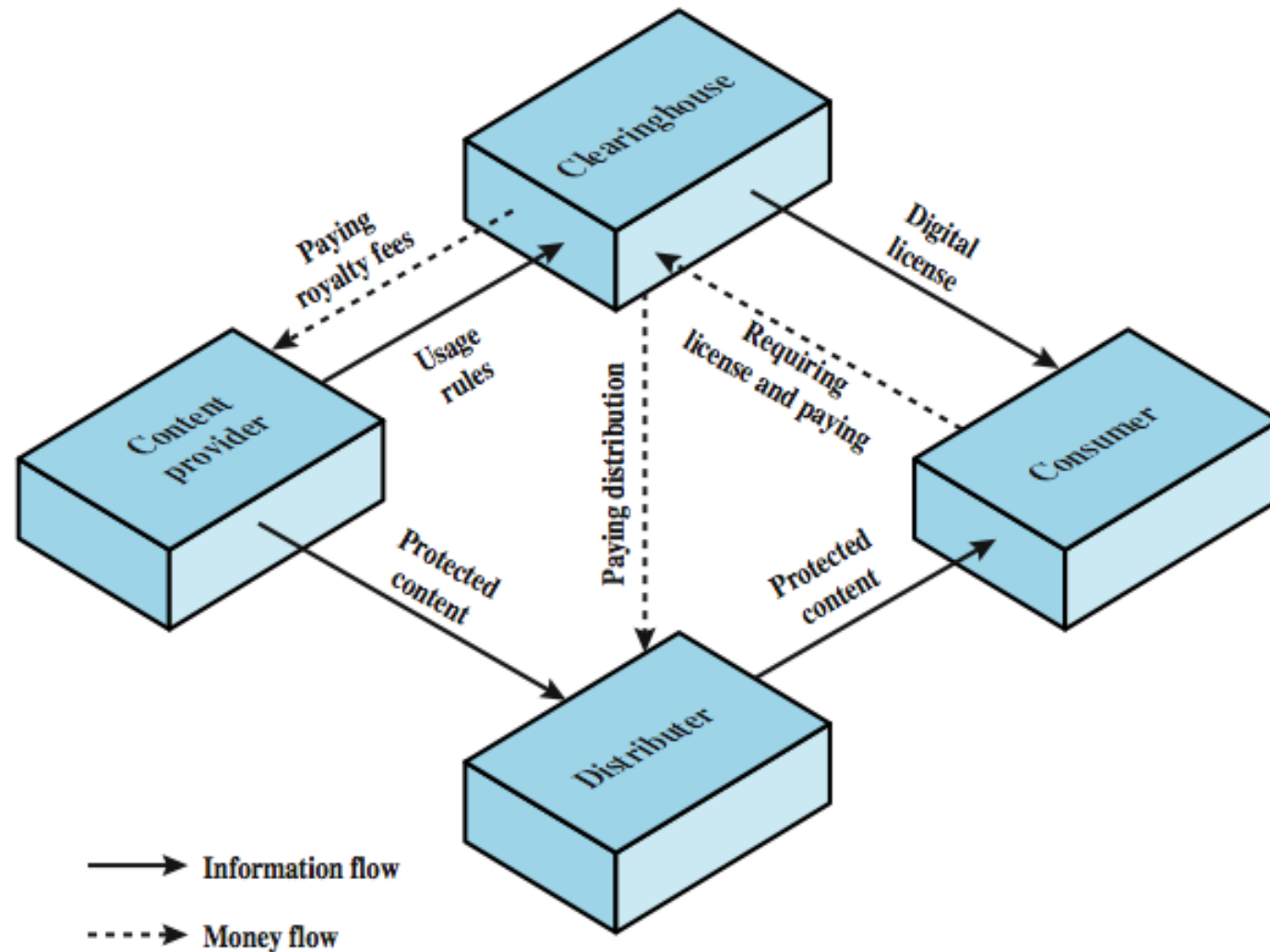
- certain actions are exempted from the DMCA provisions:
 - fair use
 - reverse engineering
 - encryption research
 - security testing
 - personal privacy
- considerable concern exists that DMCA inhibits legitimate security/crypto research

Digital Rights Management (DRM)

- systems and procedures ensuring digital rights holders are clearly identified and receive stipulated payment for their works
 - may impose further restrictions on their use
- no single DRM standard or architecture
- goal often to provide mechanisms for the complete content management lifecycle
- provide persistent content protection for a variety of digital content types / platforms / media

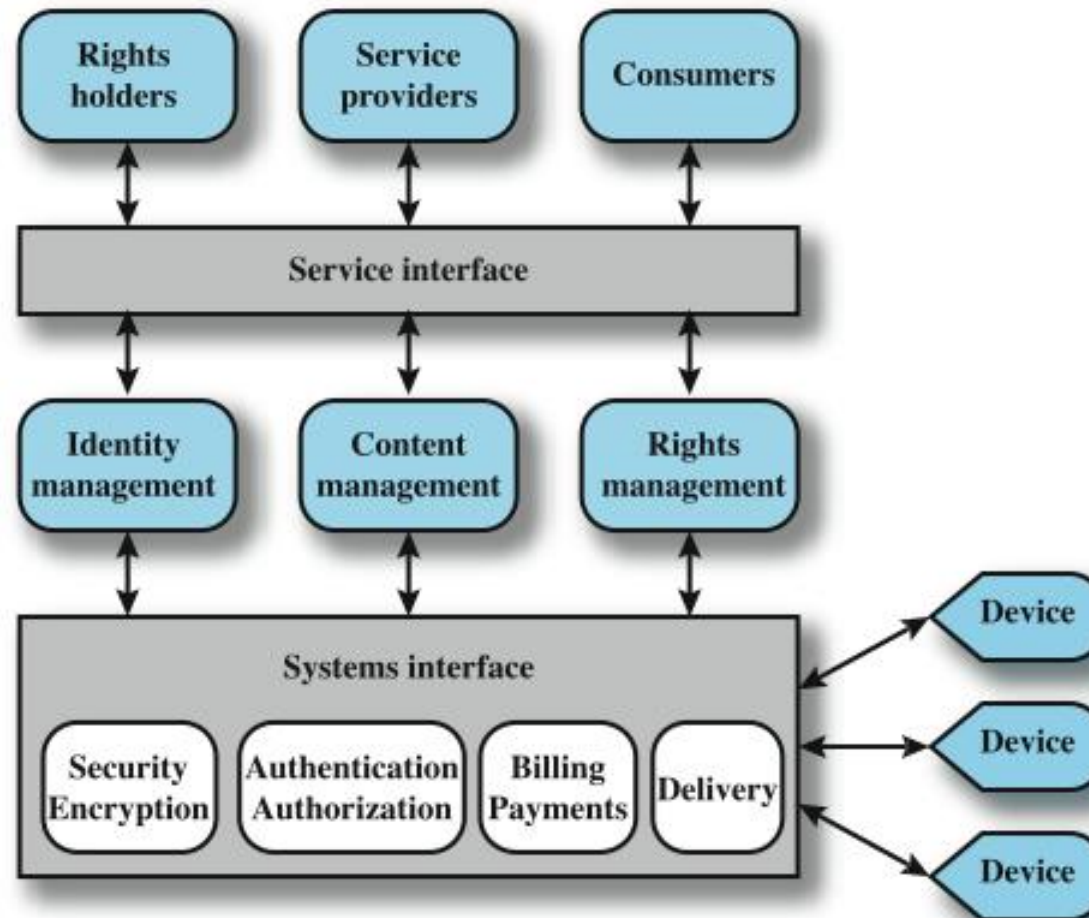
DRM Components

28



DRM System Architecture

29



Privacy

- overlaps with computer security
- have dramatic increase in scale of info collected and stored
 - motivated by law enforcement, national security, economic incentives
- but individuals increasingly aware of access and use of personal / private info
- concerns on extent of privacy compromise have seen a range of responses

EU Privacy Law

- European Union Data Protection Directive was adopted in 1998 to:
 - ensure member states protect fundamental privacy rights when processing personal info
 - prevent member states from restricting the free flow of personal info within EU
- organized around principles of:
 - notice, consent, consistency, access, security, onward transfer, enforcement

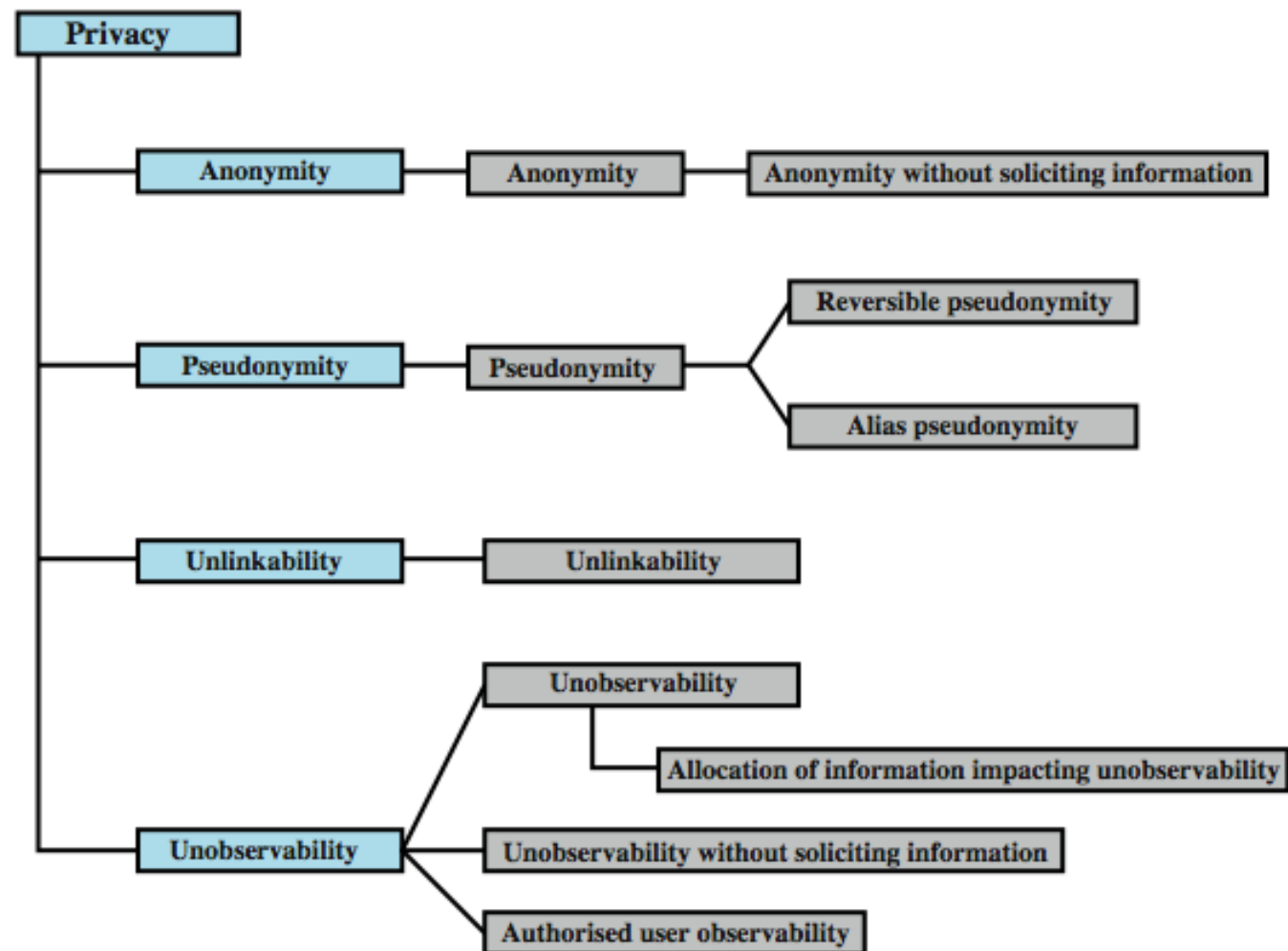
US Privacy Law

- have Privacy Act of 1974 which:
 - permits individuals to determine records kept
 - permits individuals to forbid records being used for other purposes
 - permits individuals to obtain access to records
 - ensures agencies properly collect, maintain, and use personal info
 - creates a private right of action for individuals
- also have a range of other privacy laws

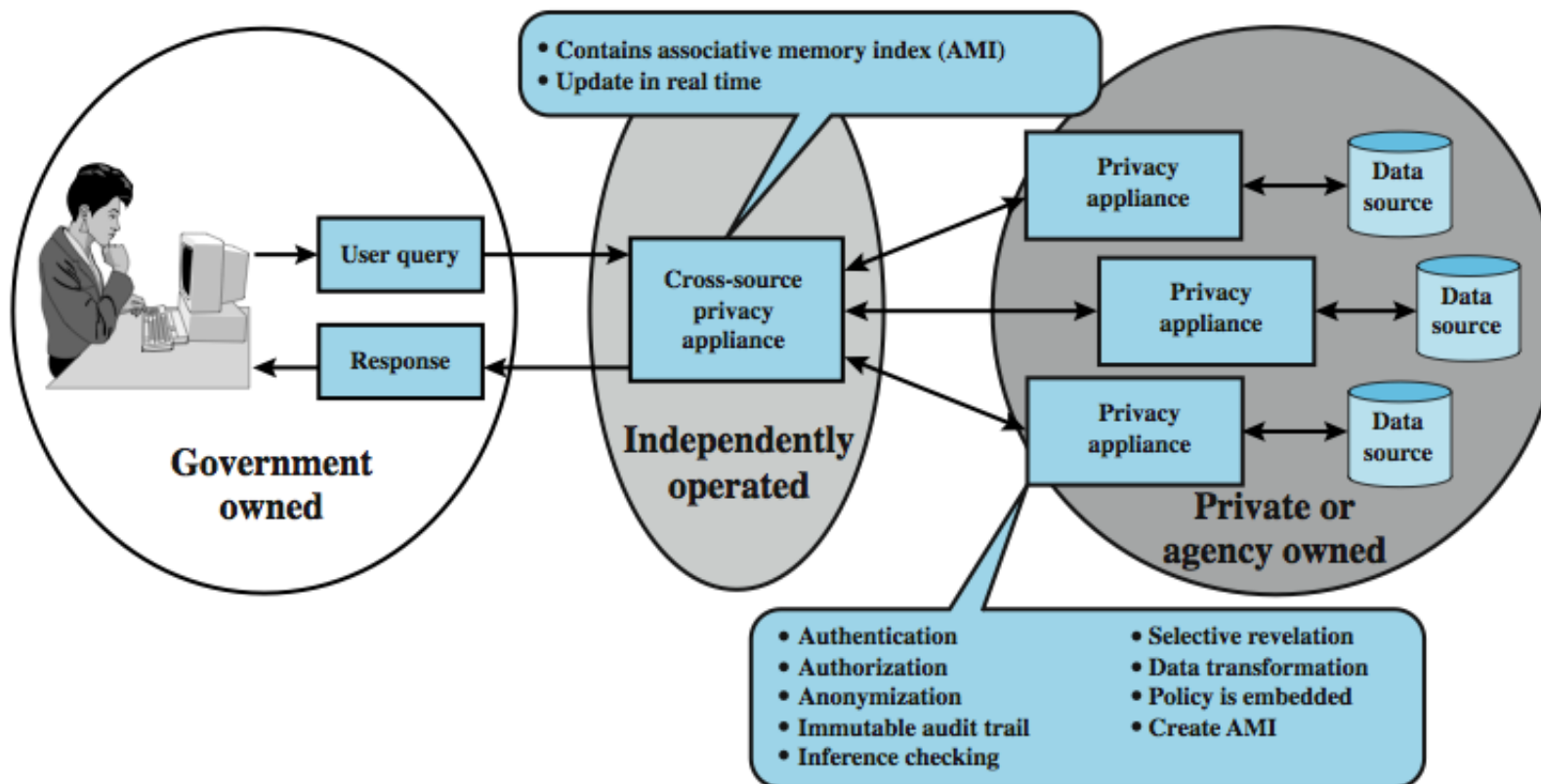
Organizational Response

- ▶ “An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information should be implemented.”

Common Criteria Privacy Class



Privacy and Data Surveillance

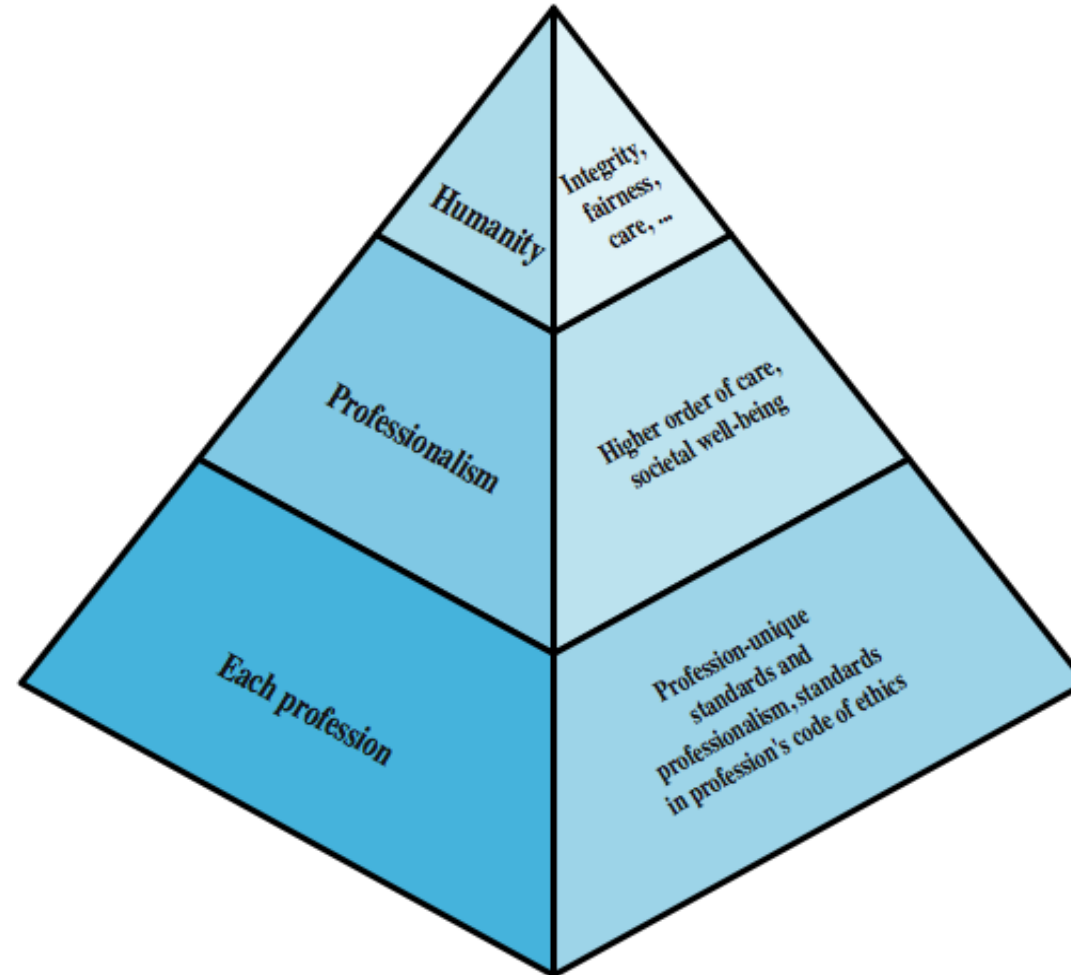


Ethical Issues

- have many potential misuses / abuses of information and electronic communication that create privacy and security problems
- ethics:
 - a system of moral principles relating benefits and harms of particular actions to rightness and wrongness of motives and ends of them
- ethical behavior here not unique
- but do have some unique considerations
 - in scale of activities, in new types of entities

Ethical Hierarchy

37



Ethical Issues Related to Computers and Info Systems

- some ethical issues from computer use:
 - repositories and processors of information
 - producers of new forms and types of assets
 - instruments of acts
 - symbols of intimidation and deception
- those who understand / exploit technology, and have access permission, have power over these
- issue is balancing professional responsibilities with ethical or moral responsibilities

Ethical Question Examples

- whistle-blower
 - when professional ethical duty conflicts with loyalty to employer
 - e.g. inadequately tested software product
 - organizations and professional societies should provide alternative mechanisms
- potential conflict of interest
 - e.g. consultant has financial interest in vendor which should be revealed to client

Codes of Conduct

- ethics not precise laws or sets of facts
- many areas may present ethical ambiguity
- many professional societies have ethical codes of conduct which can:
 1. be a positive stimulus and instill confidence
 2. be educational
 3. provide a measure of support
 4. be a means of deterrence and discipline
 5. enhance the profession's public image

Codes of Conduct

- see ACM, IEEE and AITP codes
- place emphasis on responsibility - other people
- have some common themes:
 1. dignity and worth of other people
 2. personal integrity and honesty
 3. responsibility for work
 4. confidentiality of information
 5. public safety, health, and welfare
 6. participation in professional societies to improve standards of the profession
 7. the notion that public knowledge and access to technology is equivalent to social power

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ **Need for Security at Multiple levels, Security Policies**
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Need for Security at Multiple levels, Security Policies

Trusted Computer Systems

- ▶ information security is increasingly important
- ▶ have varying degrees of sensitivity of information
 - ▶ military info classifications: confidential, secret etc.
- ▶ subjects (people or programs) have varying rights of access to objects (information)
- ▶ want to consider ways of increasing confidence in systems to enforce these rights
- ▶ known as multilevel security
 - ▶ subjects have **maximum** & **current** security level
 - ▶ objects have a fixed security level **classification**

Access Control

- ▶ given system has identified a user
- ▶ determine what resources they can access
- ▶ general model is that of access matrix with
 - ▶ **subject** - active entity (user, process)
 - ▶ **object** - passive entity (file or resource)
 - ▶ **access right** – way object can be accessed
- ▶ can decompose by
 - ▶ columns as access control lists
 - ▶ rows as capability tickets

Access Control Matrix

	Program1	...	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
•				
•				
•				

Bell LaPadula (BLP) Model

- ▶ one of the most famous security models
- ▶ implemented as mandatory policies on system
- ▶ has two key policies:
- ▶ **no read up** (simple security property)
 - ▶ a subject can only read/write an object if the current security level of the subject dominates (\geq) the classification of the object
- ▶ **no write down** (*-property)
 - ▶ a subject can only append/write to an object if the current security level of the subject is dominated by (\leq) the classification of the object

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ **Model of network security**
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Model of network security

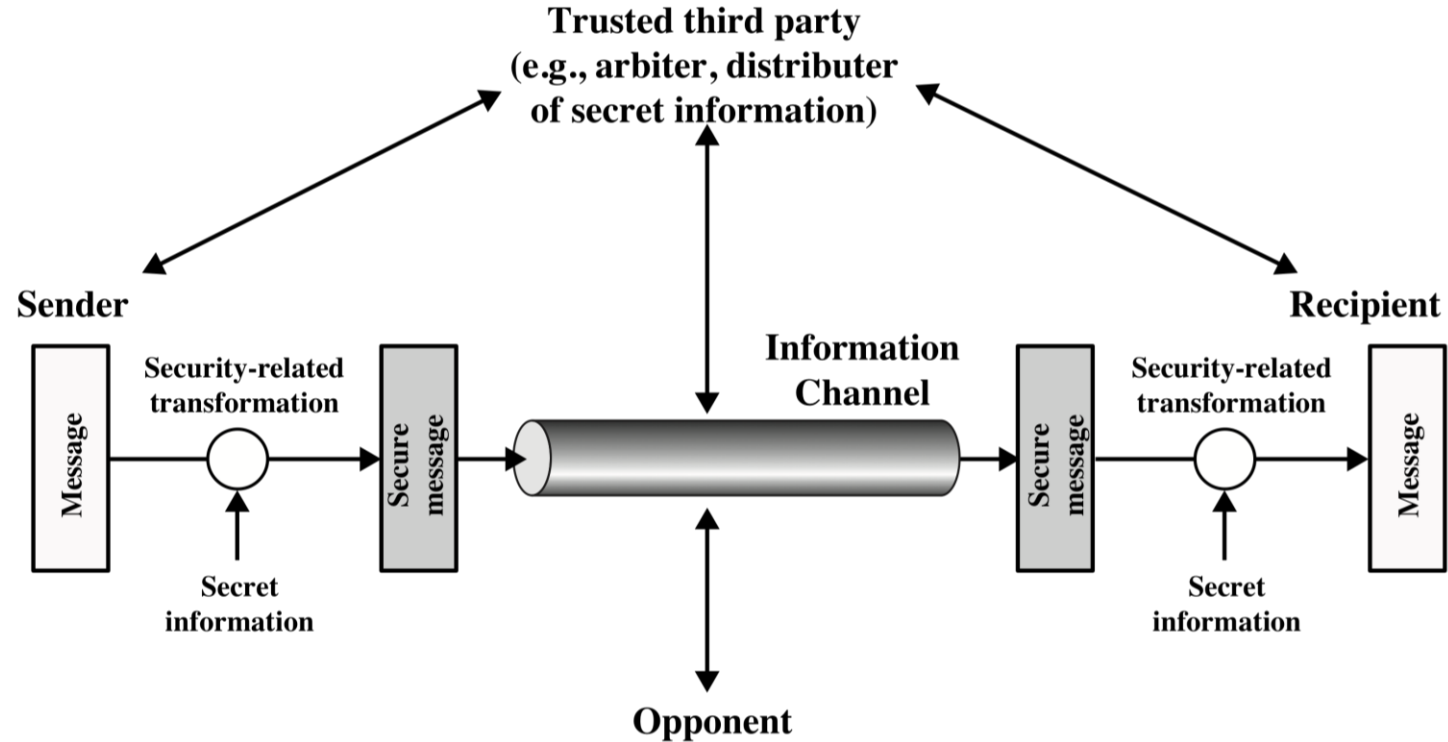


Figure 1.2 Model for Network Security

Network Access Security Model

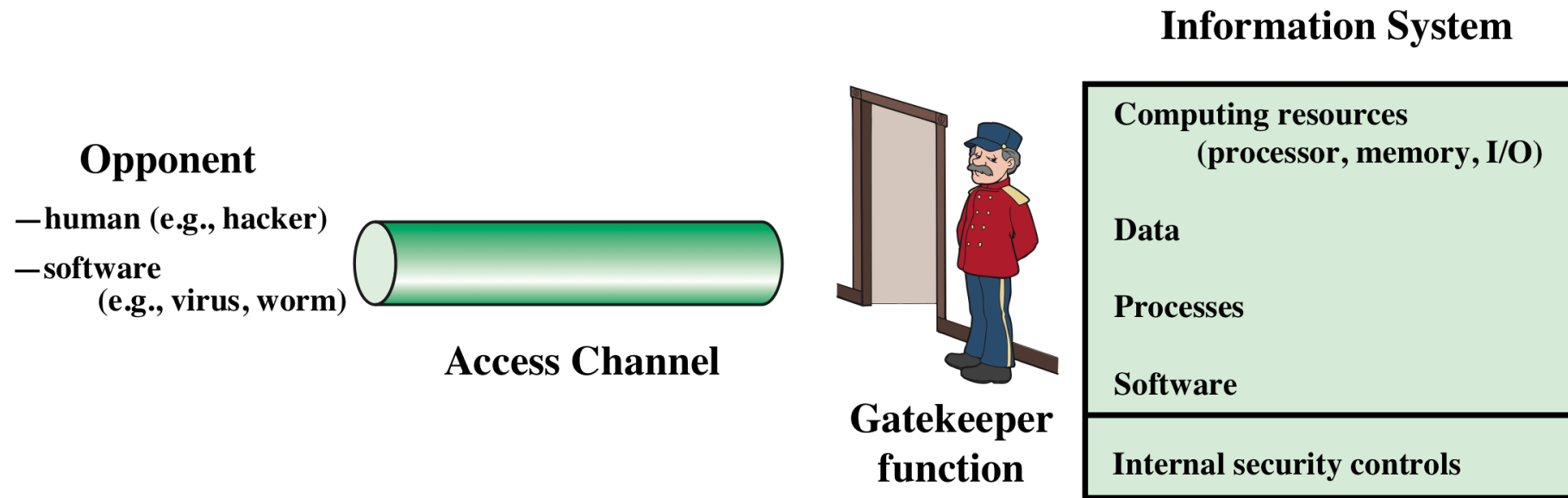


Figure 1.3 Network Access Security Model

Unwanted Access

- ▶ Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- ▶ Programs can present two kinds of threats:
 - ▶ Information access threats
 - ▶ Intercept or modify data on behalf of users who should not have access to that data
 - ▶ Service threats
 - ▶ Exploit service flaws in computers to inhibit use by legitimate users



Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ **Security attacks, services and mechanisms**
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Security attacks, services and mechanisms

- ▶ Security attack
 - ▶ Any action that compromises the security of information owned by an organization
- ▶ Security mechanism
 - ▶ A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- ▶ Security service
 - ▶ A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
 - ▶ Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation

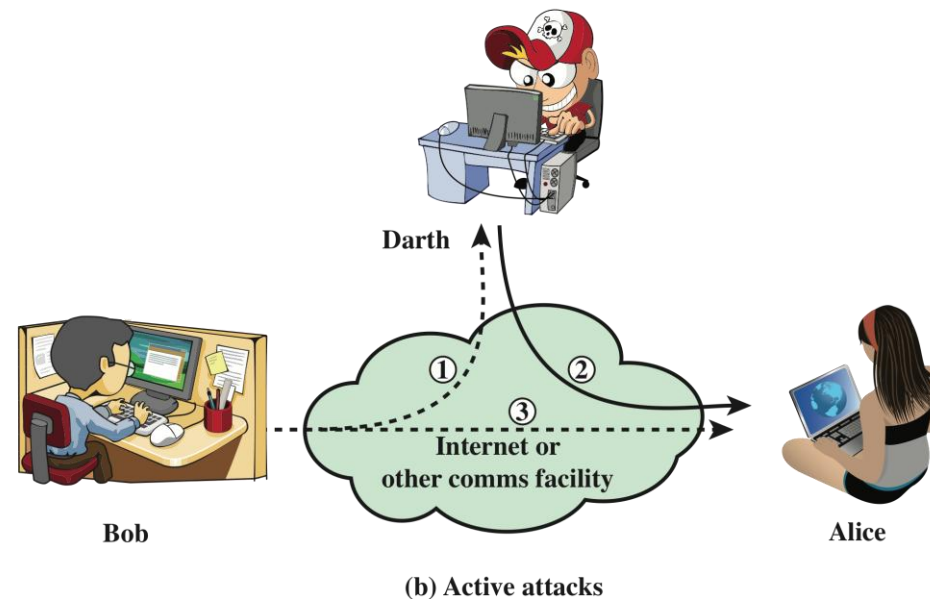
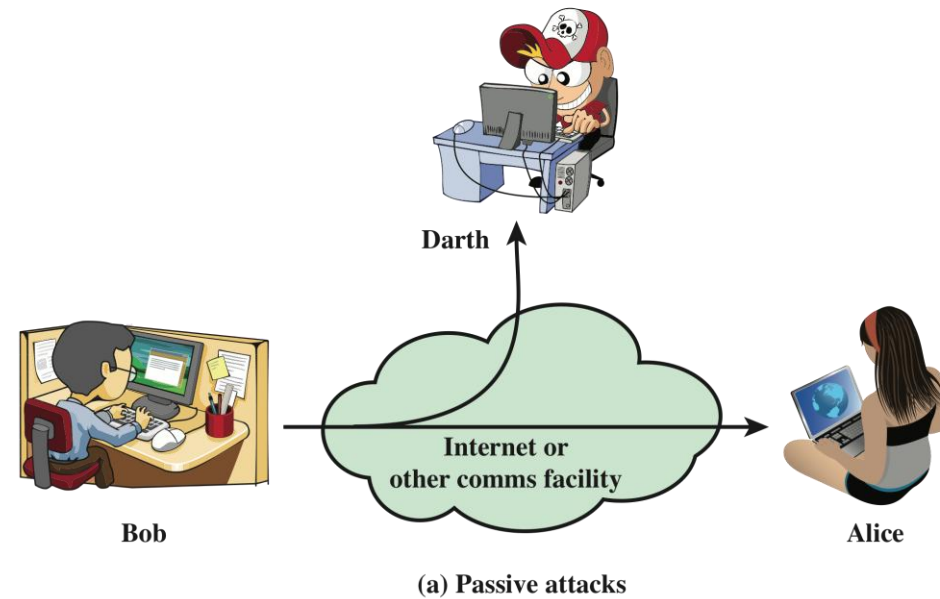


Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted



- ▶ Two types of passive attacks are:
 - ▶ The release of message contents
 - ▶ Traffic analysis

Active Attacks

- ▶ Involve some modification of the data stream or the creation of a false stream
- ▶ Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- ▶ Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security Services

- Defined by X.800 as:
 - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
 - A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- ▶ Authentication
- ▶ Access control
- ▶ Data confidentiality
- ▶ Data integrity
- ▶ Non-repudiation



Authentication

- ▶ Concerned with assuring that a communication is authentic
 - ▶ In the case of a single message, assures the recipient that the message is from the source that it claims to be from
 - ▶ In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Access Control


- ▶ The ability to limit and control the access to host systems and applications via communications links
- ▶ To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual



Data Confidentiality

- ▶ The protection of transmitted data from passive attacks
 - ▶ Broadest service protects all user data transmitted between two users over a period of time
 - ▶ Narrower forms of service includes the protection of a single message or even specific fields within a message
- ▶ The protection of traffic flow from analysis
 - ▶ This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity



Can apply to a stream of messages, a single message, or selected fields within a message

Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

Nonrepudiation

- ▶ Prevents either sender or receiver from denying a transmitted message
- ▶ When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- ▶ When a message is received, the sender can prove that the alleged receiver in fact received the message

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery

As above, but provides only detection without recovery.

Selective-Field Connection Integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

Nonrepudiation, Destination

Proof that the message was received by the specified party.

Security Services (X.800)

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

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control

A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization

The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

Security Audit Trail

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Security Mechanisms (X.800)

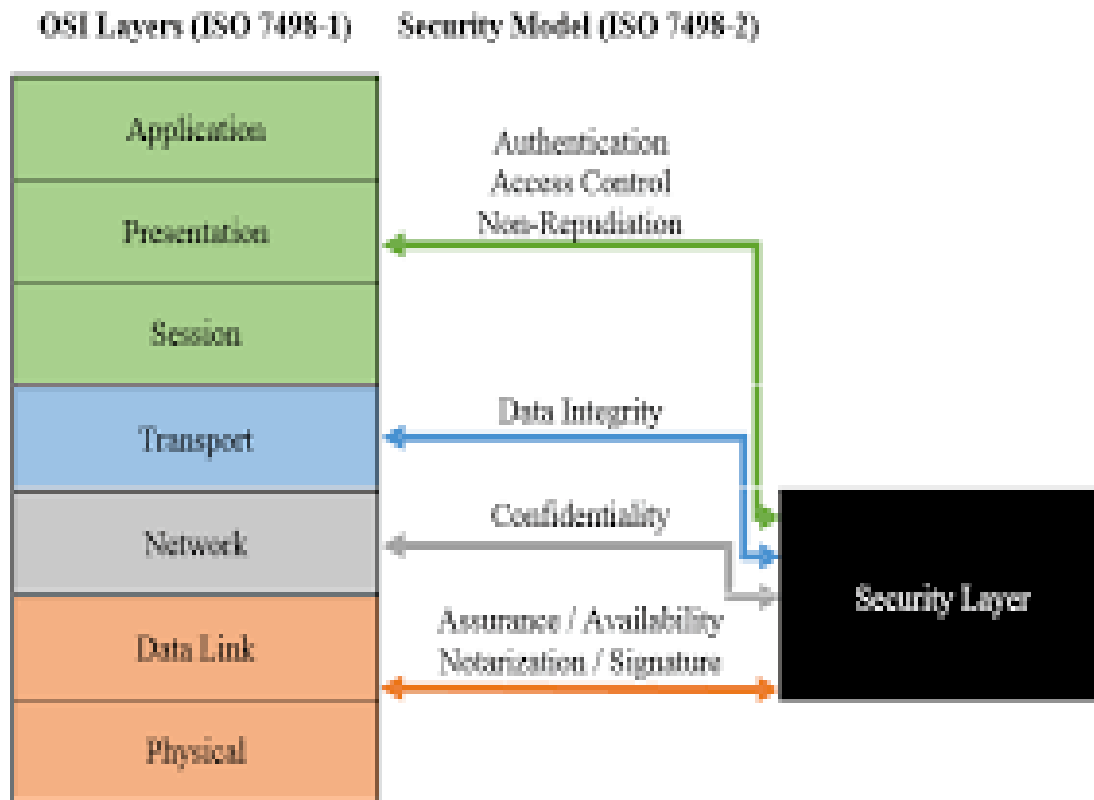
Security Services & Security Mechanisms

Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ **OSI security architecture**
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

OSI Security Architecture



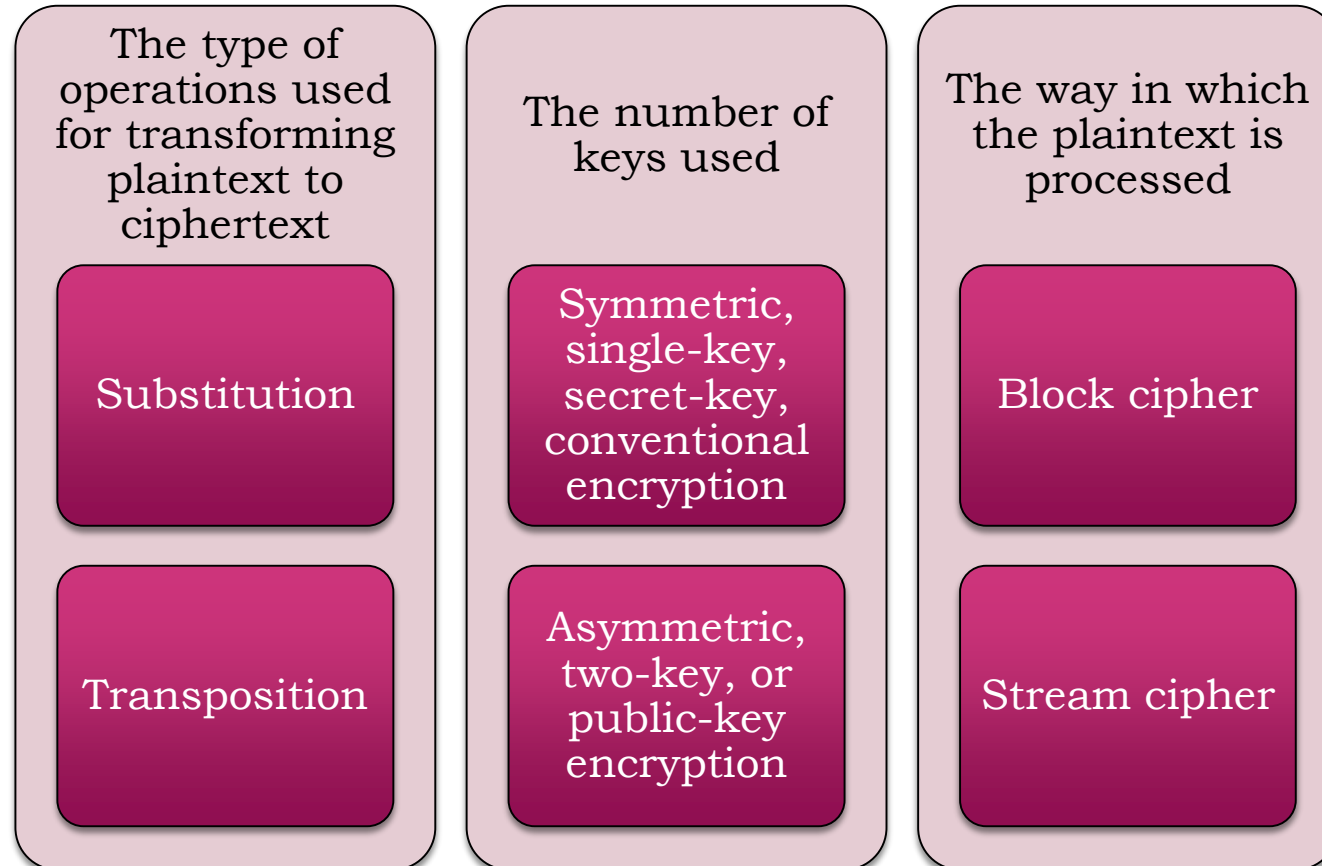
- ▶ ITU-T X.800 “Security Architecture for OSI”
- ▶ Defines a systematic way of defining and providing security requirements
- ▶ Provides a useful, if abstract, overview of concepts the fundamentals of networks security, security architecture, threats and vulnerabilities

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ **Classical encryption techniques**
 - ▶ **Substitution techniques, transposition techniques, steganography**
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Cryptographic Systems

- Characterized along three independent dimensions:



Classical encryption techniques

- ▶ Substitution techniques
- ▶ Transposition techniques

Substitution techniques

- ▶ Letters of plaintext are replaced by other letters or by numbers or symbols
- ▶ If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- ▶ Simplest and earliest known use of a substitution cipher
- ▶ Used by Julius Caesar
- ▶ Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- ▶ Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

- ▶ Can define transformation as:

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

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

- ▶ Mathematically give each letter a number

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

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25



Caesar Cipher Algorithm

- ▶ Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod 26$$

- ▶ A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k, p) = (p + k) \bmod 26$$

- ▶ Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

Brute-Force Cryptanalysis of Caesar Cipher

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrpc	rfe	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlg
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fghjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgr	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

Monoalphabetic Cipher

- ▶ Permutation
 - ▶ Of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once
- ▶ If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are $26!$ or greater than 4×10^{26} possible keys
 - ▶ This is 10 orders of magnitude greater than the key space for DES
 - ▶ Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message

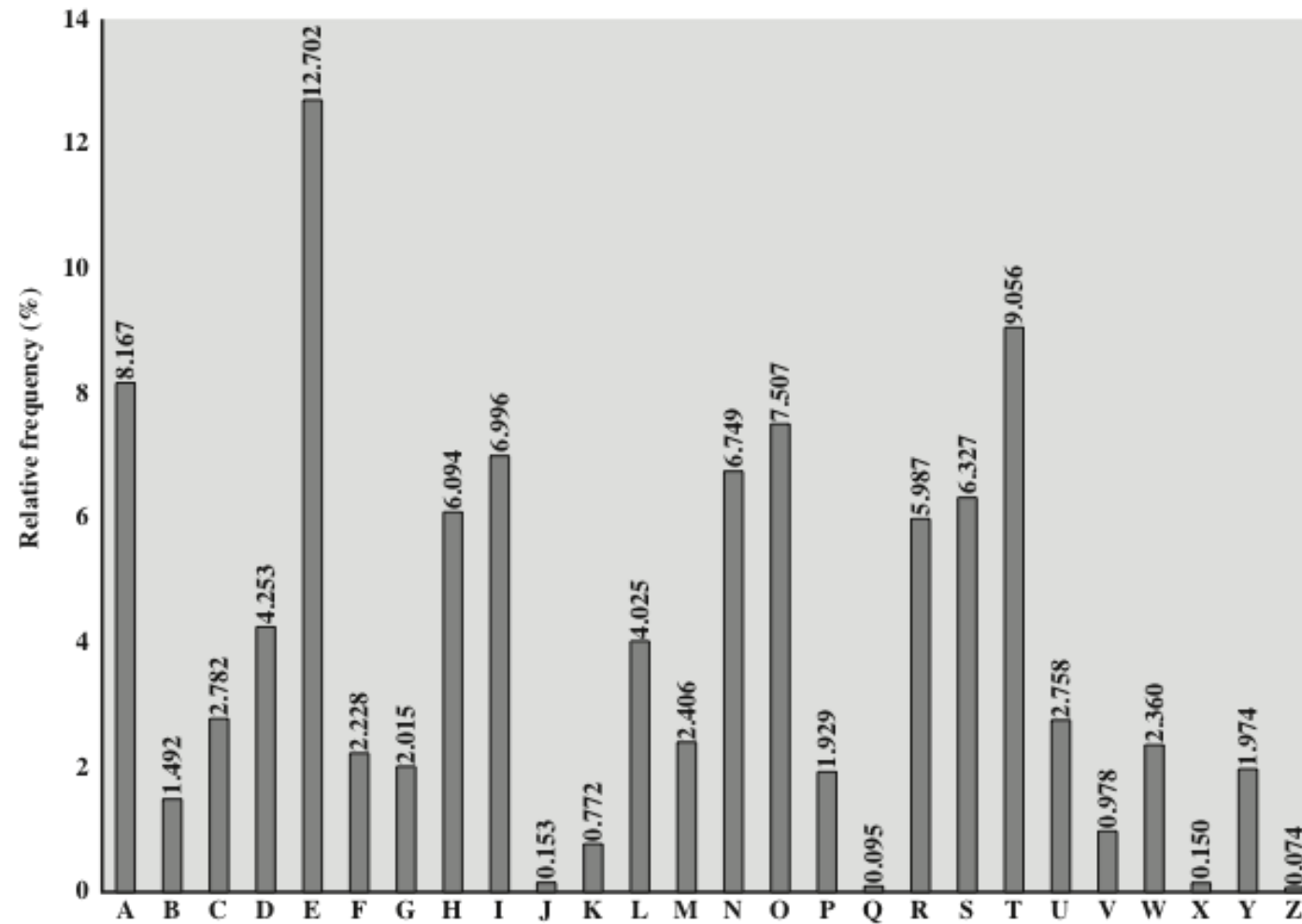


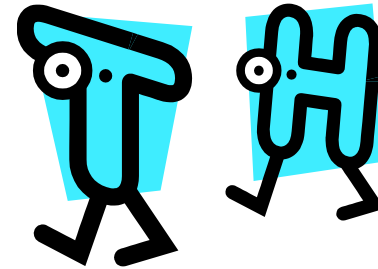
Figure 2.5 Relative Frequency of Letters in English Text

Monoalphabetic Ciphers

- ▶ Easy to break because they reflect the frequency data of the original alphabet
- ▶ Countermeasure is to provide multiple substitutes (homophones) for a single letter

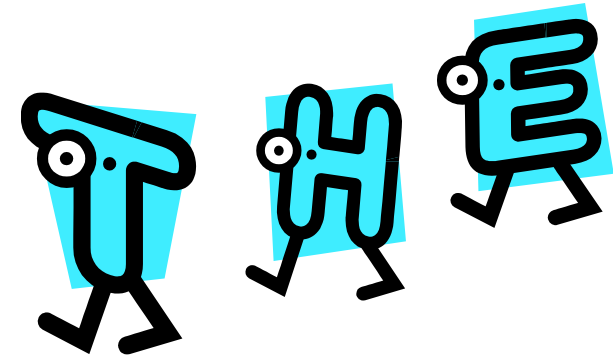
- ▶ Digram

- ▶ Two-letter combination
 - ▶ Most common is *th*



- ▶ Trigram

- ▶ Three-letter combination
 - ▶ Most frequent is *the*



Playfair Cipher

- ▶ Best-known multiple-letter encryption cipher
- ▶ Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- ▶ Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- ▶ Invented by British scientist Sir Charles Wheatstone in 1854
- ▶ Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Playfair Key Matrix

- ▶ Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- ▶ Using the keyword MONARCHY:

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

Encrypting and Decrypting

- ▶ Plaintext encrypted two letters at a time:
 - ▶ if a pair is a repeated letter, insert a filler like 'X',
 - ▶ eg. "balloon" encrypts as "ba lx lo on"
 - ▶ if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
 - ▶ eg. "ar" encrypts as "RM"
 - ▶ if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
 - ▶ eg. "mu" encrypts to "CM"
 - ▶ otherwise each letter is replaced by the one in its row in the column of the other letter of the pair,
 - ▶ eg. "hs" encrypts to "BP", and "ea" to "IM" or "JM" (as desired)

Security of the Playfair Cipher

- ▶ security much improved over monoalphabetic
- ▶ since have $26 \times 26 = 676$ digrams
- ▶ would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- ▶ and correspondingly more ciphertext
- ▶ was widely used for many years (eg. US & British military in WW1)
- ▶ it **can** be broken, given a few hundred letters
- ▶ since still has much of plaintext structure

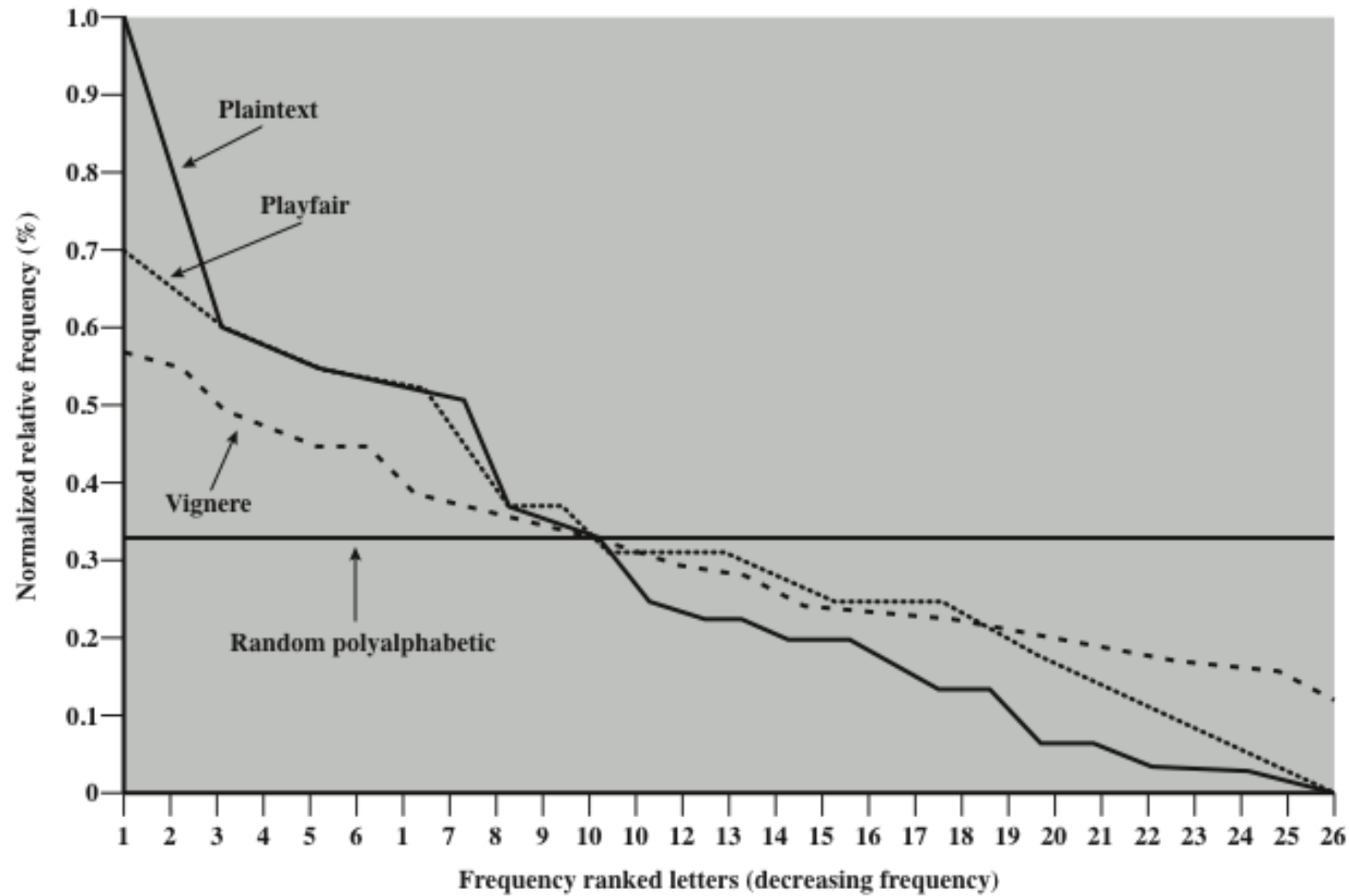


Figure 2.6 Relative Frequency of Occurrence of Letters

Hill Cipher

- ▶ Developed by the mathematician Lester Hill in 1929
- ▶ Strength is that it completely hides single-letter frequencies
 - ▶ The use of a larger matrix hides more frequency information
 - ▶ A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
- ▶ Strong against a ciphertext-only attack but easily broken with a known plaintext attack

Hill Cipher

In general terms, the Hill system can be expressed as

$$\mathbf{C} = E(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

$$\mathbf{P} = D(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

Hill Cipher

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$

$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$

$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in terms of row vectors and matrices:⁶

$$(c_1 \ c_2 \ c_3) = (p_1 \ p_2 \ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

Polyalphabetic Ciphers

- ▶ Polyalphabetic substitution cipher
 - ▶ Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:

- A set of related monoalphabetic substitution rules is used
- A key determines which particular rule is chosen for a given transformation

Vigenère Cipher

- ▶ Best known and one of the simplest polyalphabetic substitution ciphers
- ▶ In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- ▶ Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a

Example of Vigenère Cipher

- ▶ To encrypt a message, a key is needed that is as long as the message
- ▶ Usually, the key is a repeating keyword
- ▶ For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as:

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenère Autokey System

- ▶ A keyword is concatenated with the plaintext itself to provide a running key
- ▶ Example:
key: deceptivewearediscoveredsav
plaintext: wearediscoveredsaveyourself
ciphertext: ZICVTWQNGKZEIIGASXSTSLVWLA
- ▶ Even this scheme is vulnerable to cryptanalysis
 - ▶ Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Vernam Cipher

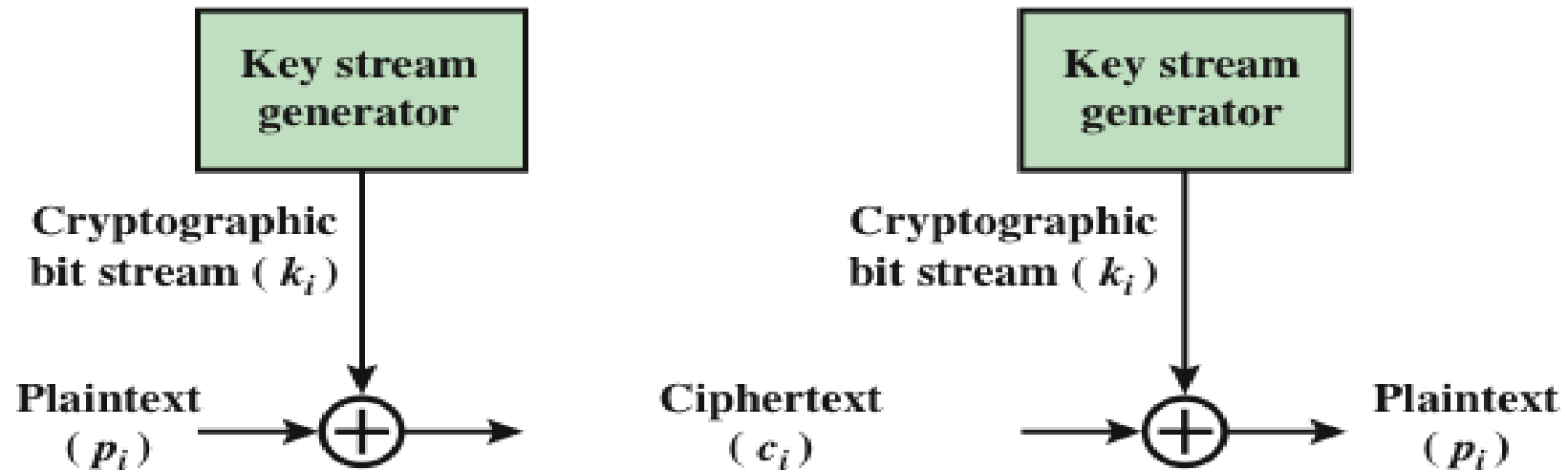


Figure 2.7 Vernam Cipher

Transposition techniques

- ▶ Rail Fence Cipher
- ▶ Row Column Transposition

Rail Fence Cipher

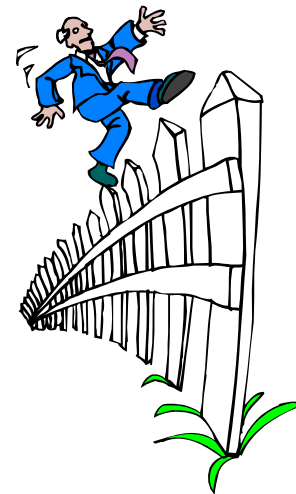
- ▶ Simplest transposition cipher
- ▶ Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- ▶ To encipher the message “meet me after the toga party” with a rail fence of depth 2, we would write:

m e m a t r h t g p r y

e t e f e t e o a a t

Encrypted message is:

MEMATRHTGPRYETEFETEOAAT



Row Transposition Cipher

- ▶ Is a more complex transposition
- ▶ Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
 - ▶ The order of the columns then becomes the key to the algorithm

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Steganography

- ▶ an alternative to encryption
- ▶ hides existence of message
 - ▶ using only a subset of letters/words in a longer message marked in some way
 - ▶ using invisible ink
 - ▶ hiding in LSB in graphic image or sound file
- ▶ has drawbacks
 - ▶ high overhead to hide relatively few info bits

Steganography Techniques



- **Character marking**
 - Selected letters of printed or typewritten text are over-written in pencil
 - The marks are ordinarily not visible unless the paper is held at an angle to bright light
- **Invisible ink**
 - A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper
- **Pin punctures**
 - Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light
- **Typewriter correction ribbon**
 - Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ **Foundations of modern cryptography:**
 - ▶ **Perfect security**
 - ▶ **Information theory**
- ▶ Product cryptosystem
- ▶ Cryptanalysis

Foundations of modern cryptography:

Classic Cryptography	Modern Cryptography
It manipulates traditional characters, i.e., letters and digits directly.	It operates on binary bit sequences.
It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secret key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
It requires the entire cryptosystem for communicating confidentially.	Modern cryptography requires parties interested in secure communication to possess the secret key only.

Perfect security

- ▶ Special case of information-theoretic security.
- ▶ For an encryption algorithm, if there is ciphertext produced that uses it, no information about the plaintext is provided without knowledge of the key.
- ▶ If E is a perfectly secure encryption function, for any fixed message m , there must be, for each ciphertext c , at least one key k such that

$$C = E_k(m).$$

- ▶ Mathematically, let m and c be the random variables representing the plaintext and ciphertext messages, respectively; then, we have that

$$I(m; c) = 0$$

- ▶ Where $I(m; c)$ is the mutual information between m and c .
- ▶ In other words, the plaintext message is independent of the transmitted ciphertext if we do not have access to the key.
- ▶ It has been proved that any cipher with the perfect secrecy property must use keys with effectively the same requirements as one-time pad keys.

One-Time Pad

- ▶ Improvement to Vernam cipher proposed by an Army Signal Corp officer, Joseph Mauborgne
- ▶ Use a random key that is as long as the message so that the key need not be repeated
- ▶ Key is used to encrypt and decrypt a single message and then is discarded
- ▶ Each new message requires a new key of the same length as the new message
- ▶ Scheme is unbreakable
 - ▶ Produces random output that bears no statistical relationship to the plaintext
 - ▶ Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code



Difficulties

- ▶ The one-time pad offers complete security but, in practice, has two fundamental difficulties:
 - ▶ There is the practical problem of making large quantities of random keys
 - ▶ Any heavily used system might require millions of random characters on a regular basis
 - ▶ Mammoth key distribution problem
 - ▶ For every message to be sent, a key of equal length is needed by both sender and receiver
- ▶ Because of these difficulties, the one-time pad is of limited utility
 - ▶ Useful primarily for low-bandwidth channels requiring very high security
- ▶ The one-time pad is the only cryptosystem that exhibits *perfect secrecy*

Information theory

- ▶ Information-theoretic security is a cryptosystem whose security derives purely from information theory
- ▶ The system **cannot be broken even if the adversary has unlimited computing power.**
- ▶ The cryptosystem is **considered cryptanalytically unbreakable if the adversary does not have enough information to break the encryption.**
- ▶ An encryption protocol with information-theoretic security **does not depend for its effectiveness on unproven assumptions** about computational hardness.
- ▶ Such a protocol is not vulnerable to future developments in computer power such as quantum computing.

Information theory

- ▶ An example of an information-theoretically secure cryptosystem is the **one-time pad**.
- ▶ The concept of information-theoretically secure communication was introduced in 1949 by **American mathematician Claude Shannon**
 - ▶ The inventor of information theory, who used it to prove that the one-time pad system was secure.
- ▶ Information-theoretically secure cryptosystems have been used for the most sensitive governmental communications, such as diplomatic cables and high-level military communications, because of the great efforts enemy governments expend toward breaking them.

Information theory

- ▶ There are a variety of cryptographic tasks for which information-theoretic security is a meaningful and useful requirement.
- ▶ A few of these are:
 - ▶ Secret sharing schemes
 - ▶ Secure multiparty computation protocols
 - ▶ Private information retrieval
 - ▶ Reductions between cryptographic primitives
 - ▶ Symmetric encryption
 - ▶ Quantum cryptography

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography:
 - ▶ Perfect security
 - ▶ Information theory
- ▶ **Product cryptosystem**
- ▶ Cryptanalysis

Product cryptosystem

Product Ciphers

- ▶ Ciphers using substitutions or transpositions are not secure because of language characteristics
- ▶ hence consider using several ciphers in succession to make harder, but:
 - ▶ two substitutions make a more complex substitution
 - ▶ two transpositions make more complex transposition
 - ▶ but a substitution followed by a transposition makes a new much harder cipher
- ▶ this is bridge from classical to modern ciphers

Rotor Machines

- ▶ before modern ciphers, rotor machines were most common product cipher
- ▶ were widely used in WW2
 - ▶ German Enigma, Allied Hagelin, Japanese Purple
- ▶ implemented a very complex, varying substitution cipher
- ▶ used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
- ▶ with 3 cylinders have $26^3=17576$ alphabets

Rotor Machines

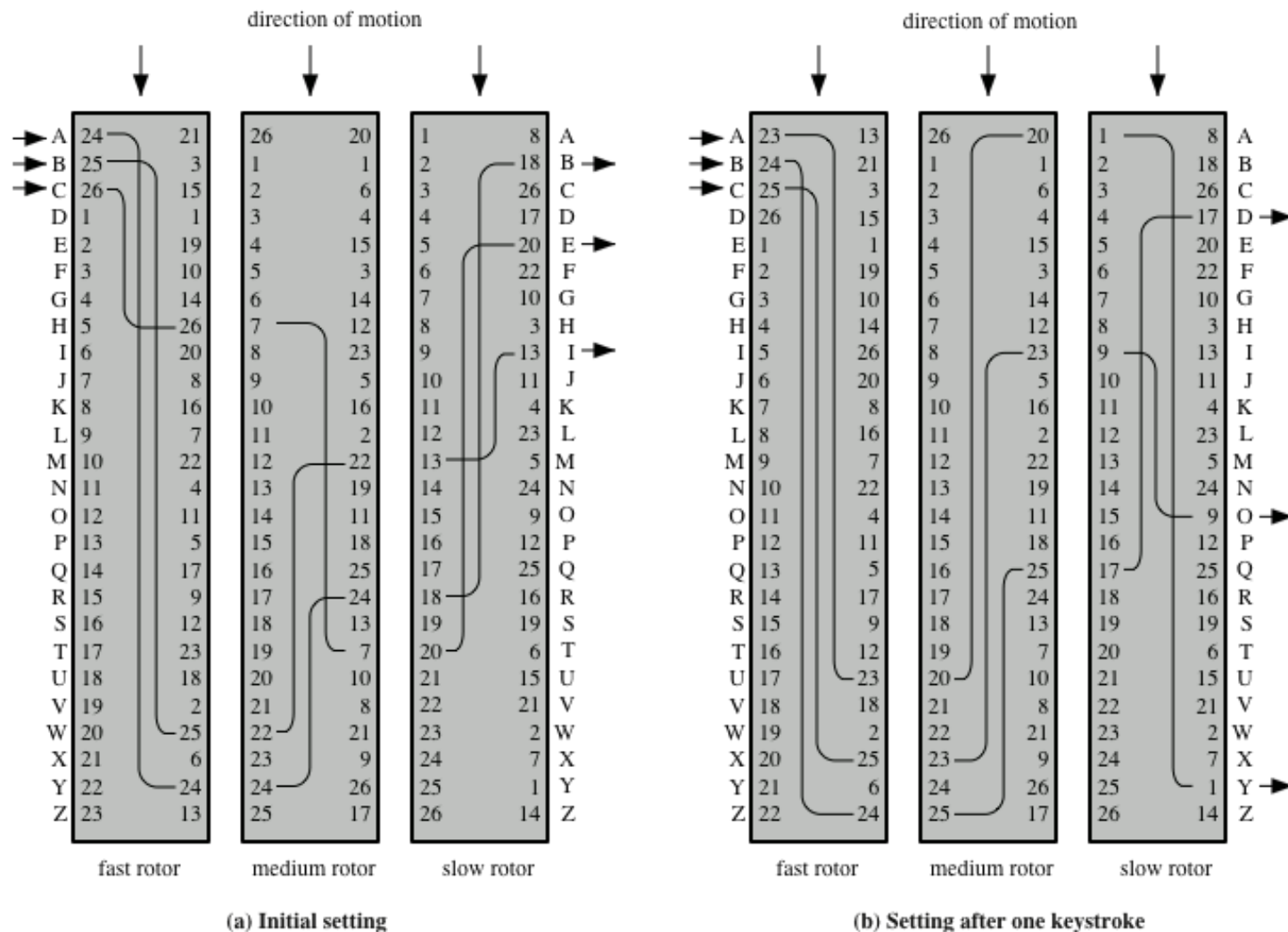


Figure 2.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts

Unit I - Introduction

- ▶ Security trends
- ▶ Legal, Ethical and Professional Aspects of Security
- ▶ Need for Security at Multiple levels, Security Policies
- ▶ Model of network security
- ▶ Security attacks, services and mechanisms
- ▶ OSI security architecture
- ▶ Classical encryption techniques
 - ▶ Substitution techniques, transposition techniques, steganography
- ▶ Foundations of modern cryptography: perfect security
- ▶ Information theory
- ▶ Product cryptosystem
- ▶ **Cryptanalysis**

Cryptanalysis

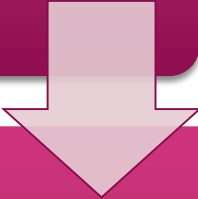
- ▶ The art and science of breaking the ciphertext is known as cryptanalysis.
- ▶ It involves the study of cryptographic mechanism with the intention to break them.
- ▶ Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.
- ▶ **Types**
 - ▶ Linear Cryptanalysis
 - ▶ Differential Cryptanalysis

Brute-Force Attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained



On average, half of all possible keys must be tried to achieve success



To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

Cryptanalysis and Brute-Force Attack

Cryptanalysis

- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

Brute-force attack

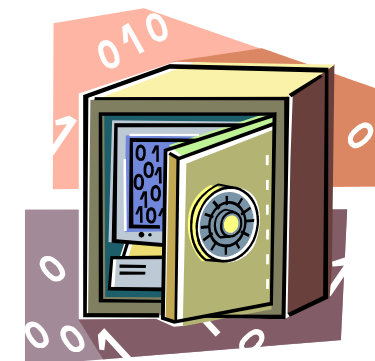
- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext
Known Plaintext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Types of Attacks on Encrypted Messages

Encryption Scheme Security

- ▶ Unconditionally secure
 - ▶ No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
- ▶ Computationally secure
 - ▶ The cost of breaking the cipher exceeds the value of the encrypted information
 - ▶ The time required to break the cipher exceeds the useful lifetime of the information



Any Queries???

