

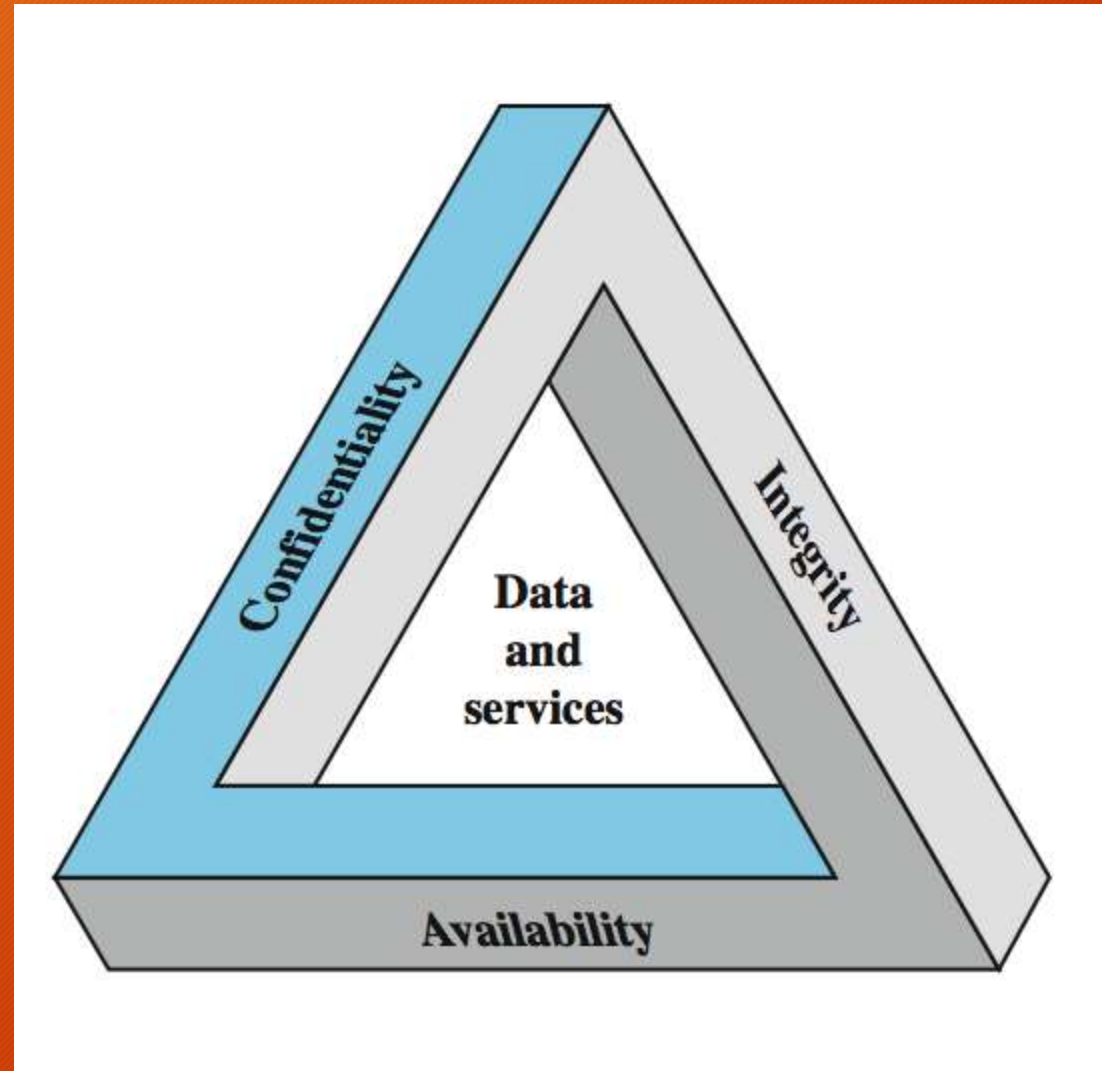
Cryptography and Network Security (17IS7DCCNS)

Faculty in Charge
Mrs. Prathima Mabel
Department of ISE
DSCE

Computer Security

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts

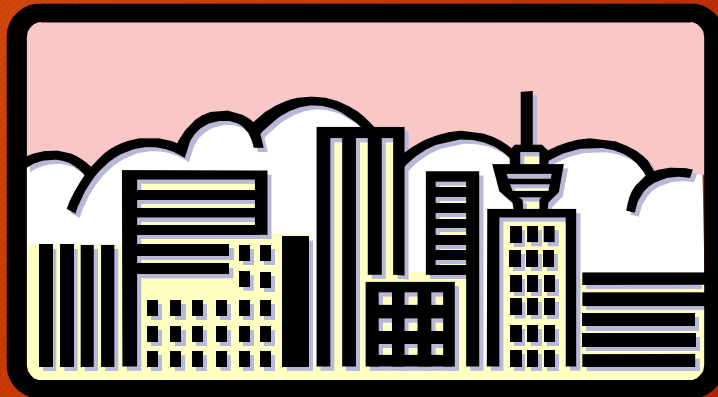


Computer Security Challenges

1. not simple
2. must consider potential attacks
3. involve algorithms and secret info
4. must decide where to deploy mechanisms
5. battle of wits between attacker / admin
6. requires regular monitoring
7. regarded as impediment to using system

OSI Security Architecture

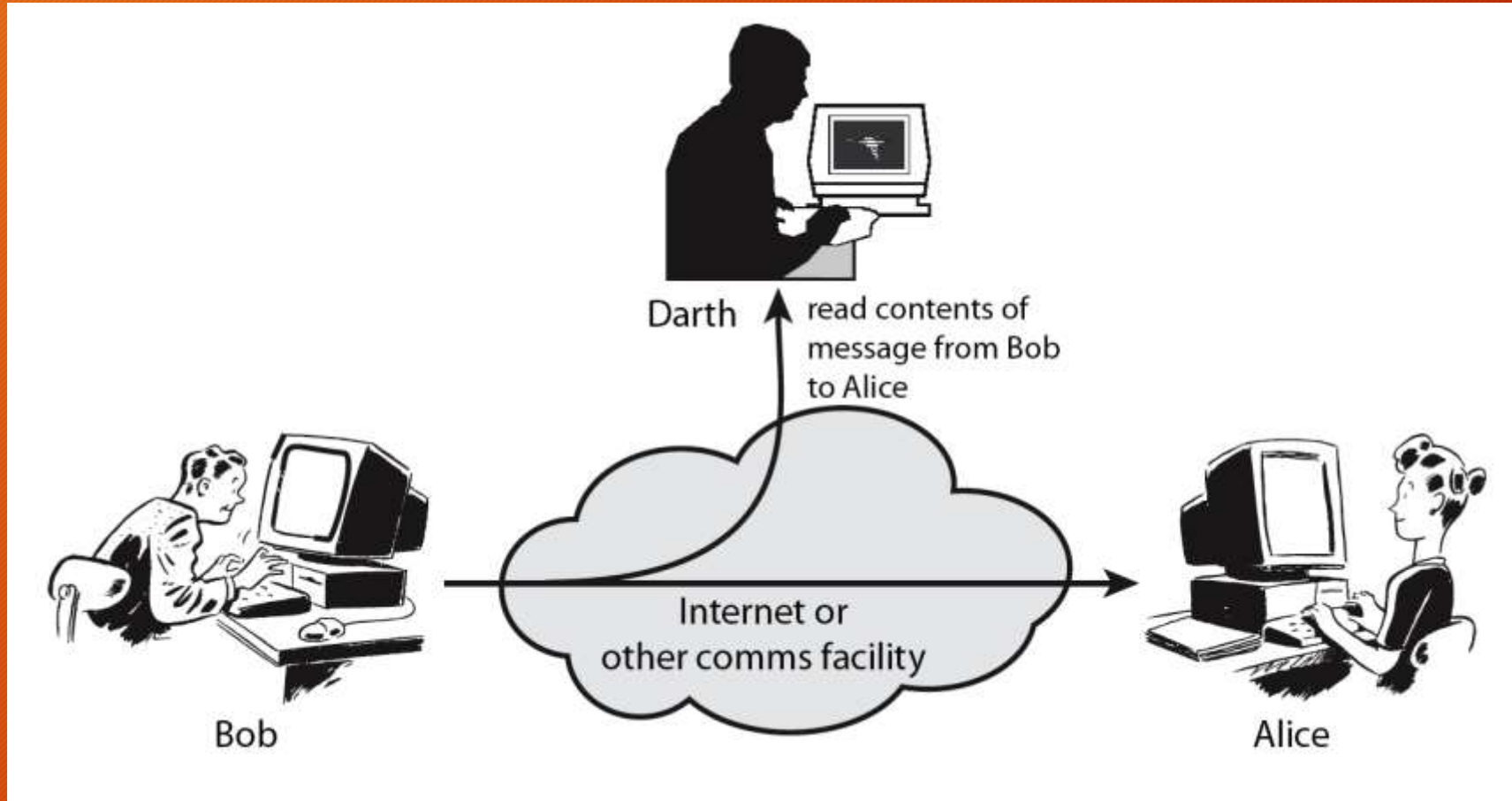
- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements



Aspects of Security

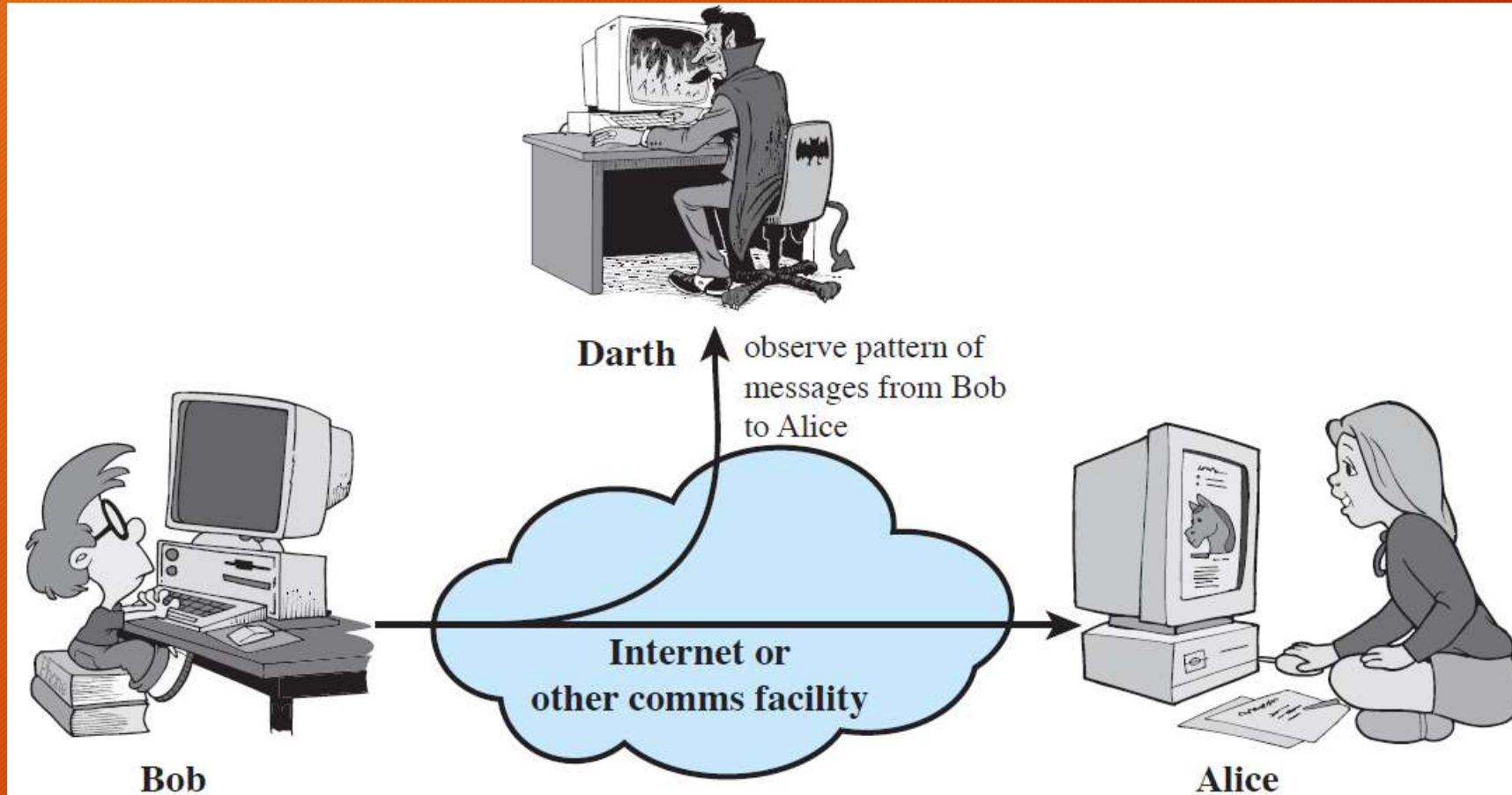
- consider 3 aspects of information security:
 - **security attack**
 - **security mechanism**
 - **security service**
- note terms
 - *threat* – a potential for violation of security
 - *attack* – an assault on system security, a deliberate attempt to evade security services


Passive Attacks



Passive Attacks (2)

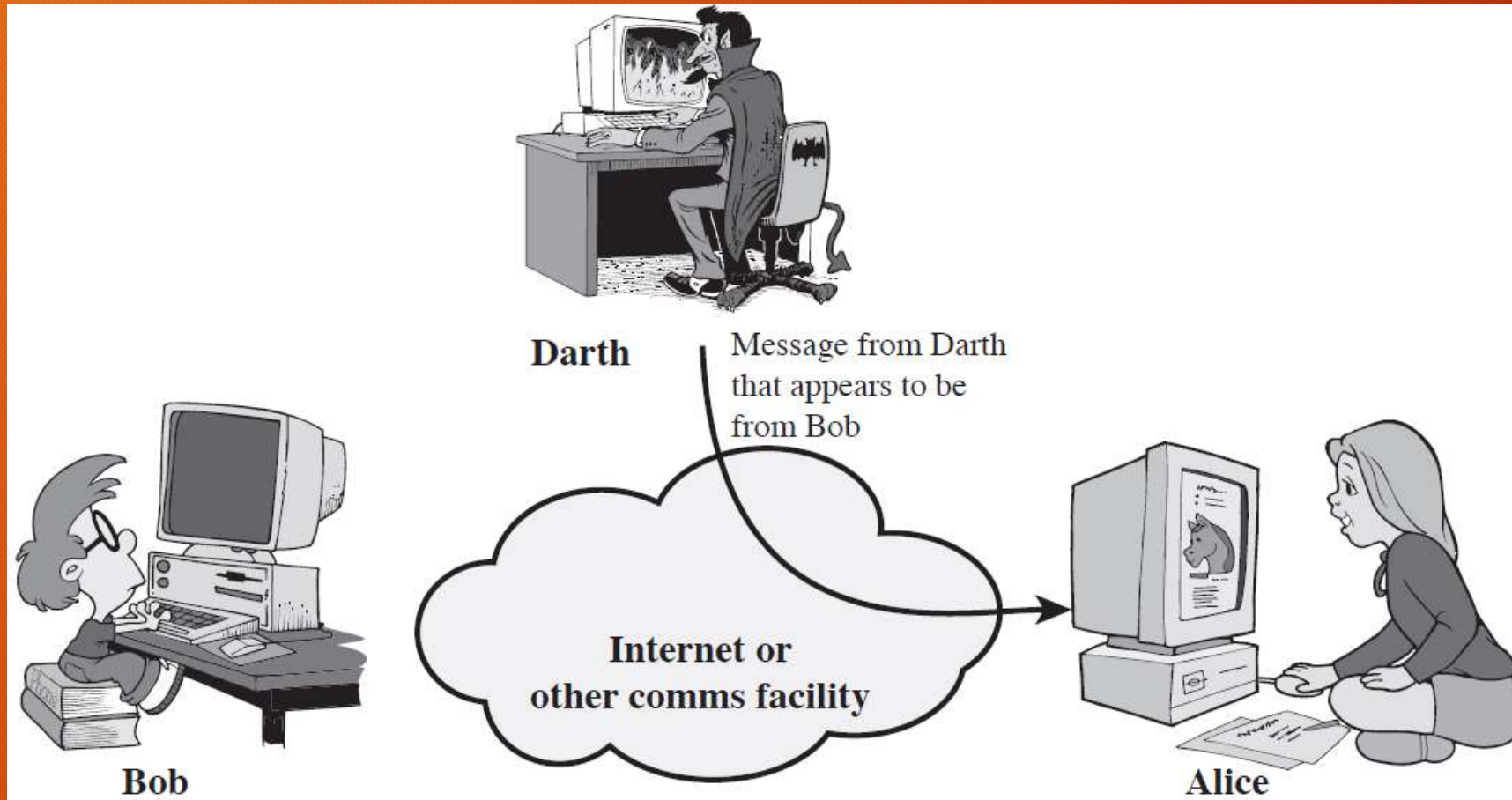
Traffic Analysis



- 
- Passive attacks do not affect system resources
 - Eavesdropping, monitoring
 - Two types of passive attacks
 - Release of message contents
 - Traffic analysis
 - Passive attacks are very difficult to detect
 - Message transmission apparently normal
 - No alteration of the data
 - Emphasis on prevention rather than detection
 - By means of encryption

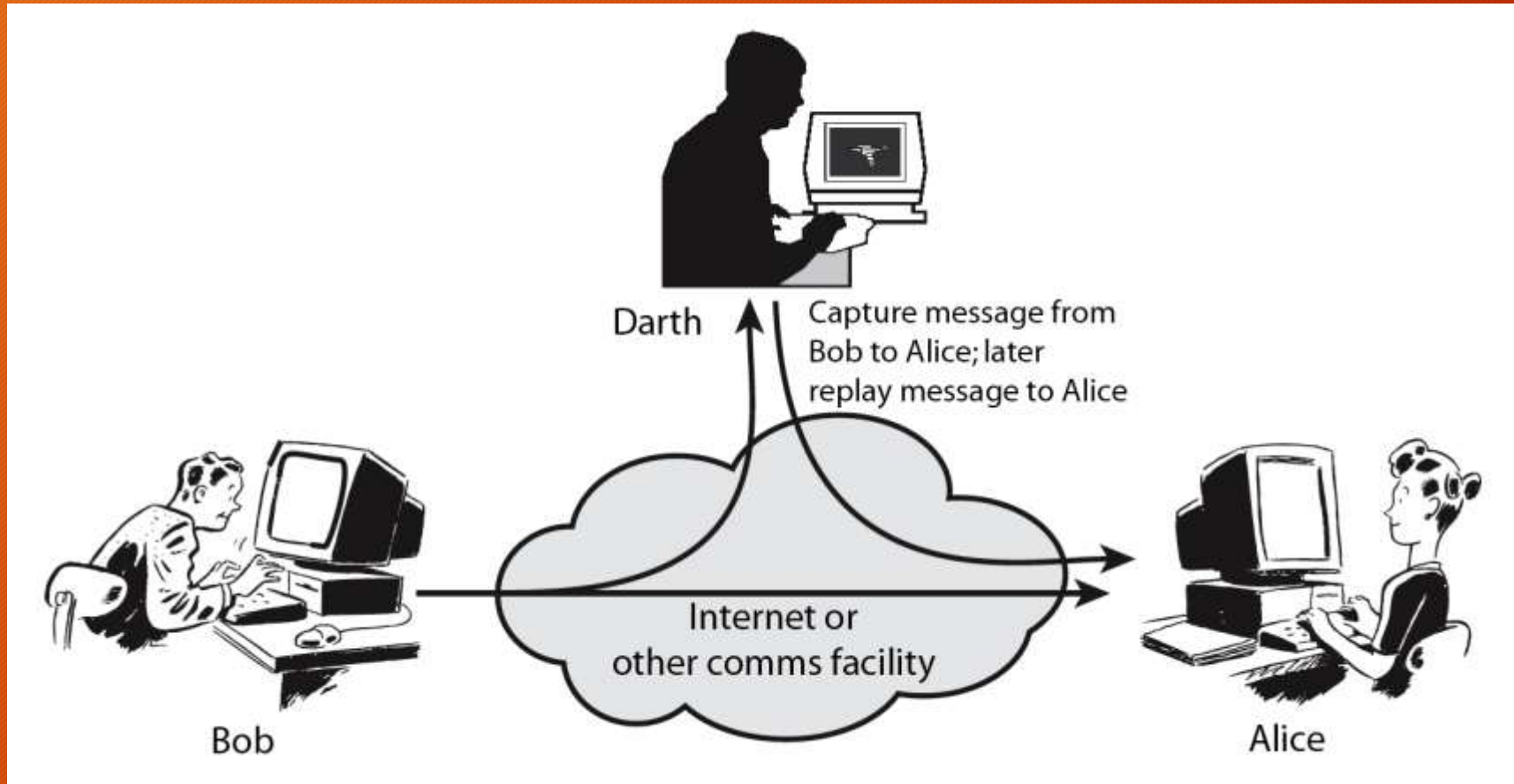
Active Attacks (1)

Masquerade



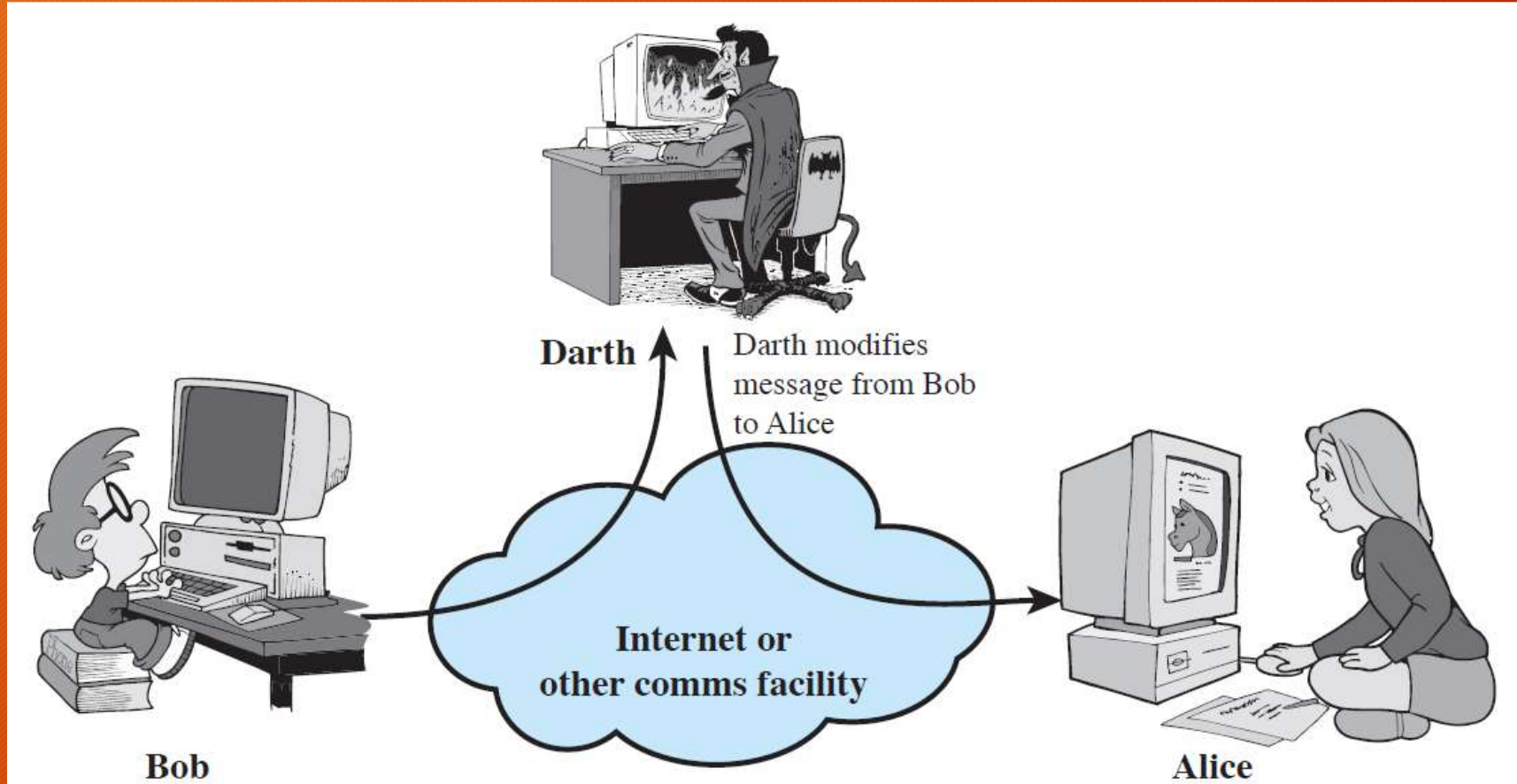
Active Attacks (2)

Replay



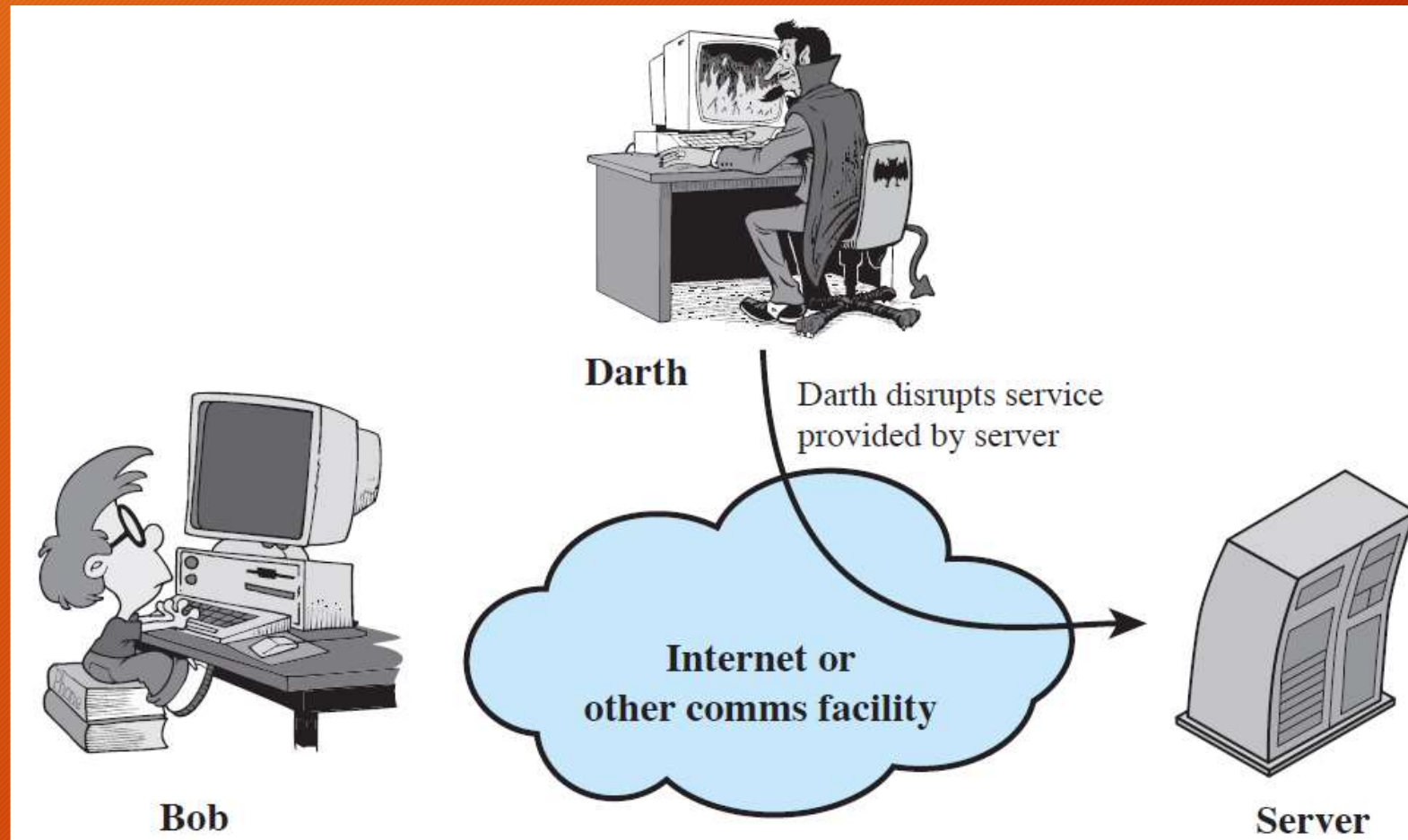
Active Attacks (3)


Modification of Messages



Active Attacks (4)

Denial of Service



- 
- Active attacks try to alter system resources or affect their operation
 - Modification of data, or creation of false data
 - Four categories
 - Masquerade
 - Replay
 - Modification of messages
 - Denial of service: preventing normal use
 - A specific target or entire network
 - Difficult to prevent
 - The goal is to detect and recover

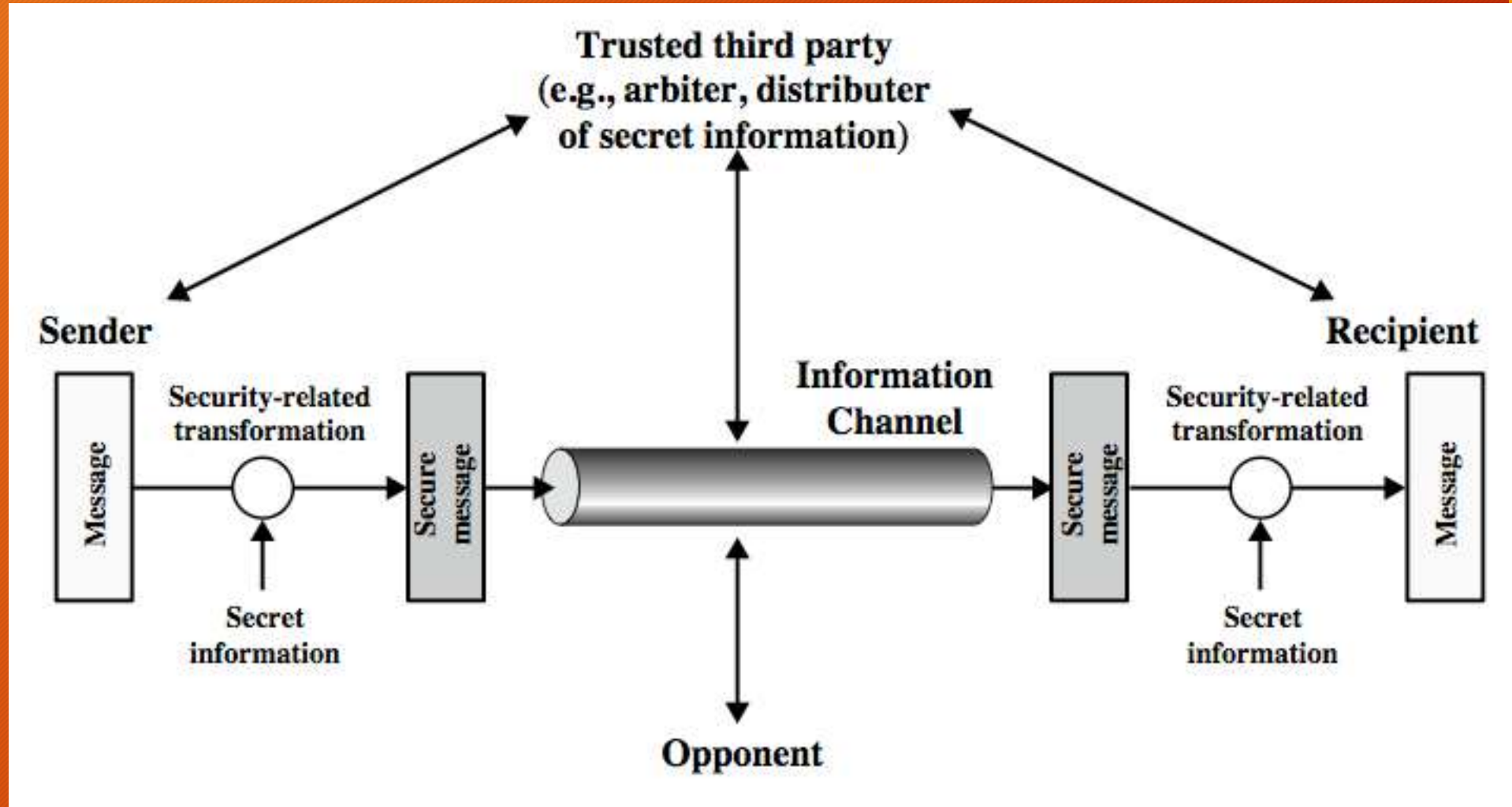
Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
 - have both peer-entity & data origin authentication
- **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
- **Availability** – resource accessible/usable

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**

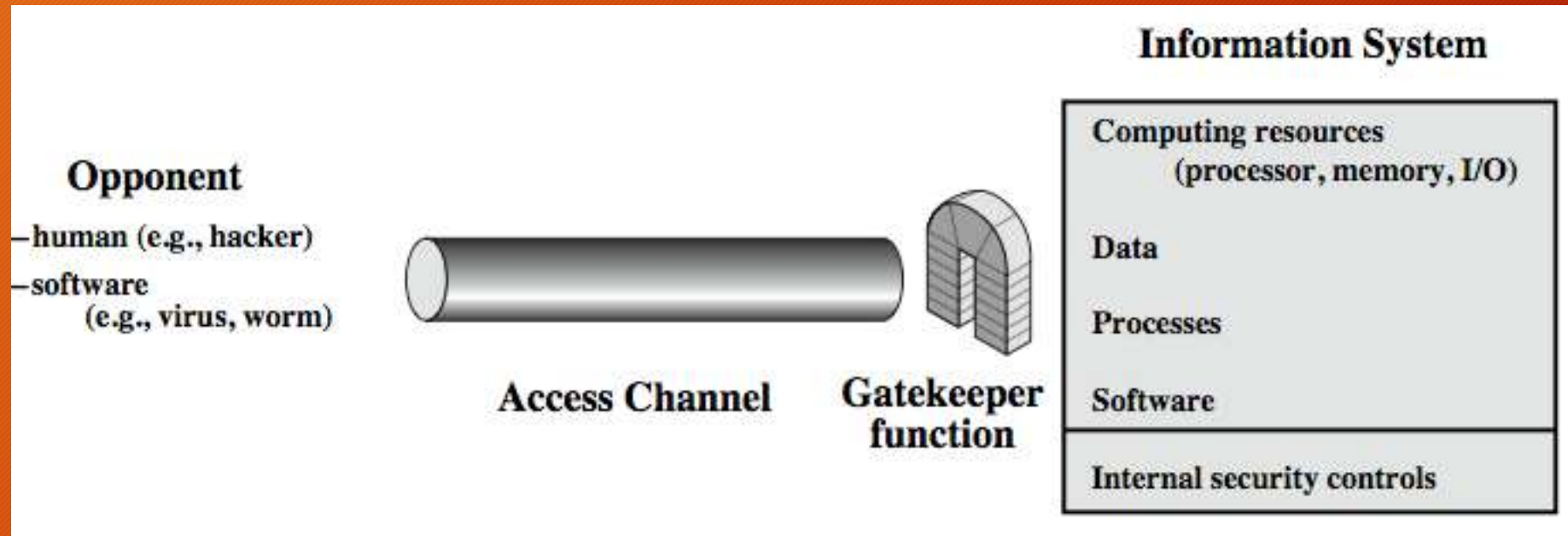
Model for Network Security



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







Classical Encryption Techniques

Classical encryption techniques

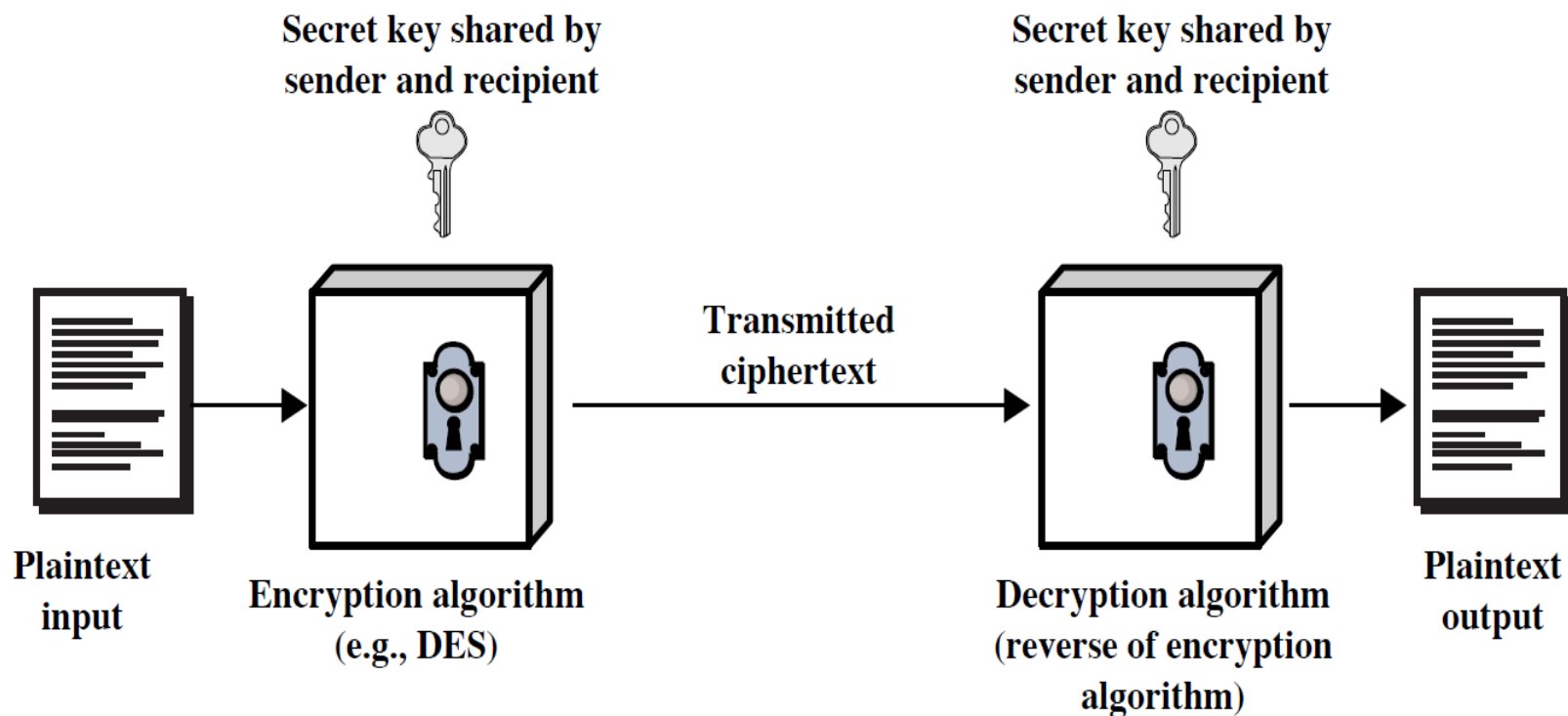
2

- ▶ As opposed to modern cryptography
- ▶ Goals:
 - ▶ to introduce basic concepts & terminology of encryption
 - ▶ to prepare us for studying modern cryptography

Basic terminology

- ▶ **Plaintext:** original message to be encrypted
- ▶ **Ciphertext:** the encrypted message
- ▶ **Enciphering or encryption:** the process of converting plaintext into ciphertext
- ▶ **Encryption algorithm:** performs encryption
 - ▶ Two inputs: a **plaintext** and a **secret key**

Symmetric Cipher Model



- ▶ **Deciphering or decryption:** recovering plaintext from ciphertext
- ▶ **Decryption algorithm:** performs decryption
 - ▶ Two inputs: **ciphertext** and **secret key**
- ▶ **Secret key:** same key used for encryption and decryption
 - ▶ Also referred to as a **symmetric key**

- ▶ **Cipher** or **cryptographic system** : a scheme for encryption and decryption
- ▶ **Cryptography**: science of studying ciphers
- ▶ **Cryptanalysis**: science of studying attacks against cryptographic systems
- ▶ **Cryptology**: cryptography + cryptanalysis

Ciphers

- ▶ **Symmetric cipher:** same key used for encryption and decryption
 - ▶ **Block cipher:** encrypts a block of plaintext at a time (typically 64 or 128 bits)
 - ▶ **Stream cipher:** encrypts data one bit or one byte at a time
- ▶ **Asymmetric cipher:** different keys used for encryption and decryption

Symmetric Encryption

- ▶ or conventional / secret-key / single-key
- ▶ sender and recipient share a common key
- ▶ all classical encryption algorithms are symmetric
- ▶ The only type of ciphers prior to the invention of asymmetric-key ciphers in 1970's
- ▶ by far most widely used

Symmetric Encryption

- ▶ Mathematically:

$$Y = E_K(X) \quad \text{or} \quad Y = E(K, X)$$

$$X = D_K(Y) \quad \text{or} \quad X = D(K, Y)$$

- ▶ X = plaintext
- ▶ Y = ciphertext
- ▶ K = secret key
- ▶ E = encryption algorithm
- ▶ D = decryption algorithm
- ▶ Both E and D are known to public

Cryptography

- ▶ Cryptographic systems are characterized along three independent dimensions:
 - ▶ **The type of operations used for transforming plaintext to ciphertext**
 - ▶ **The number of keys used**
 - ▶ **The way in which the plaintext is processed**

Cryptanalysis

- ▶ Objective: to recover the plaintext of a ciphertext or, more typically, to recover the secret key.
- ▶ **Kerckhoff's principle**: the adversary knows all details about a cryptosystem except the secret key.
- ▶ Two general approaches:
 - ▶ **brute-force** attack
 - ▶ **non-brute-force** attack (cryptanalytic attack)

Cryptanalytic Attacks

- ▶ May be classified by how much information needed by the attacker:
 - ▶ Ciphertext-only attack
 - ▶ Known-plaintext attack
 - ▶ Chosen-plaintext attack
 - ▶ Chosen-ciphertext attack

Table 2.1 Types of Attacks on Encrypted Messages

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

Brute-Force Attack

- ▶ Try every key to decipher the ciphertext.
- ▶ On average, need to try half of all possible keys
- ▶ Time needed proportional to size of **key space**

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ μ s	Time required at 10^6 decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

Classical Ciphers

- ▶ Plaintext is viewed as a sequence of elements (e.g., bits or characters)
- ▶ **Substitution cipher**: replacing each element of the plaintext with another element.
- ▶ **Transposition (or permutation) cipher**: rearranging the order of the elements of the plaintext.
- ▶ **Product cipher**: using multiple stages of substitutions and transpositions

Caesar Cipher

- ▶ Earliest known substitution cipher
- ▶ Invented by Julius Caesar
- ▶ Each letter is replaced by the letter three positions further down the alphabet.

• Plain: 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

Cipher: 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

- ▶ Example: ohio state → RKLR VWDWH

Caesar Cipher

- ▶ Mathematically, map letters to numbers:

a, b, c, ..., x, y, z

0, 1, 2, ..., 23, 24, 25

- ▶ Then the general Caesar cipher is:

$$c = E_k(p) = (p + k) \bmod 26$$

$$p = D_k(c) = (c - k) \bmod 26$$

- ▶ Can be generalized with any alphabet.

Cryptanalysis of Caesar Cipher

- ▶ Key space: $\{0, 1, \dots, 25\}$
- ▶ Vulnerable to brute-force attacks.
- ▶ E.g., break ciphertext "UNOU YZGZK"

KEY		PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1		oggv	og	chvgt	vjg	vqic	rectva
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	rhc	rmey	nyprw
6		jbbq	jb	xcqbo	qeb	qldx	mxxqv
7		iaap	ia	wbpan	pda	pkcw	lwnpu
8		hzzo	hz	vaozm	ocz	objv	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	fqhjo
14		btti	bt	putg	iwt	idvp	epgin
15		assh	as	othsf	hvs	hcuo	dofhm
16		zrrg	zr	nsgre	gur	gbtn	cnegl
17		yqqf	yq	mrfqd	ftq	fasm	bmdfk
18		xppe	xp	lqepc	esp	ezrl	alcej
19		wood	wo	kpdob	dro	dyqk	zkbd
20		vnn	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	tevx

Monoalphabetic Substitution Cipher

- ▶ Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

Plain letters: **a**b**c**defghijklmnopqrstuvwxyz

Cipher letters: **D****K****V**QFIBJWPESCXHTMYAUOLRGZN

Plaintext: if**w**e wish**t**o replace**l**etters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

- ▶ What does a key look like?

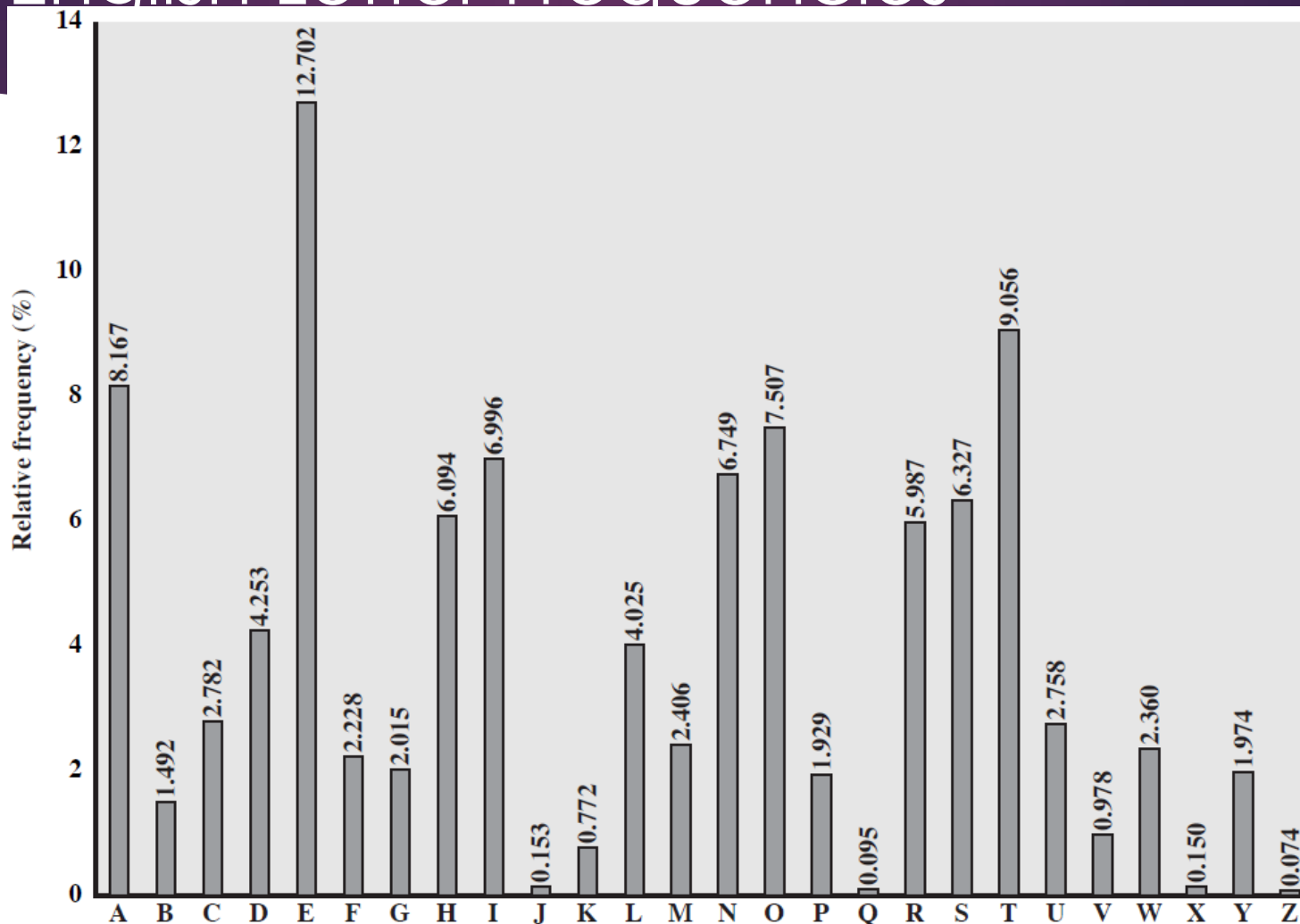
Monoalphabetic Cipher Security

- ▶ Now we have a total of $26! = 4 \times 10^{26}$ keys.
- ▶ With so many keys, it is secure against brute-force attacks.
- ▶ But not secure against some cryptanalytic attacks.
- ▶ Problem is language characteristics.

Language Statistics and Cryptanalysis

- ▶ Human languages are not random.
- ▶ Letters are not equally frequently used.
- ▶ In English, E is by far the most common letter, followed by T, R, N, I, O, A, S.
- ▶ Other letters like Z, J, K, Q, X are fairly rare.
- ▶ There are tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Statistics for double & triple letters

- ▶ In decreasing order of frequency
- ▶ Double letters:
th he an in er re es on, ...
- ▶ Triple letters:
the and ent ion tio for nde, ...

Use in Cryptanalysis

- ▶ Key concept: monoalphabetic substitution does not change relative letter frequencies
- ▶ To attack, we
 - ▶ calculate letter frequencies for ciphertext
 - ▶ compare this distribution against the known one

Example Cryptanalysis

- ▶ Given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- ▶ Count relative letter frequencies (see next page)
- ▶ Guess $\{P, Z\} = \{e, t\}$
- ▶ Of double letters, ZW has highest frequency, so guess ZW = th and hence ZWP = the
- ▶ Proceeding with trial and error finally get:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

Letter frequencies in ciphertext

P	H	F	B	C
13.33	5.83	3.33	1.67	0.00
Z	D	W	G	K
11.67	5.00	3.33	1.67	0.00
S	E 5.00	Q	Y	L
8.33		2.50	1.67	0.00
U	V 4.17	T	I	N
8.33		2.50	0.83	0.00
O	X 4.17	A	J	R
7.50		1.67	0.83	0.00
M				
6.67				

Playfair Cipher

- ▶ Not even the large number of keys in a monoalphabetic cipher provides security.
- ▶
- ▶ One approach to improving security is to **encrypt multiple letters at a time**.
- ▶ The **Playfair Cipher** is the best known such cipher.
- ▶ Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

Playfair Key Matrix

- ▶ Use a 5 x 5 matrix.
- ▶ Fill in letters of the key (w/o duplicates).
- ▶ Fill the rest of matrix with other letters.
- ▶ E.g., key = **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

1. Plaintext is encrypted two letters at a time. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Security of Playfair Cipher

- ▶ Equivalent to a monoalphabetic cipher with an alphabet of $26 \times 26 = 676$ characters.
- ▶ Security is much improved over the simple monoalphabetic cipher.
- ▶ Was widely used for many decades
 - ▶ eg. by US & British military in WW1 and early WW2
- ▶ Once thought to be unbreakable.
- ▶ Actually, it **can** be broken, because it still leaves some structure of plaintext intact.

Transposition Ciphers

- ▶ Also called **permutation** ciphers.
- ▶ Shuffle the plaintext, without altering the actual letters used.
- ▶ Example: Row Transposition Ciphers

Row Transposition Ciphers

- ▶ Plaintext is written row by row in a rectangle.
- ▶ Ciphertext: write out the **columns** in an order specified by a key.

Key: 3 4 2 1 5 6 7

Plaintext:

Ciphertext: **T****T****N****A****A****P****T****M****T****S****U****O****A****O****D****W****C****O****I****X****K****N****L****Y****P****E****T****Z**

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

► Double transposition

```

Key:      4 3 1 2 5 6 7
Input:    t t n a a p t
          m t s u o a o
          d w c o i x k
          n l y p e t z
Output:   NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

```

To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is

```

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

```

After the first transposition, we have

```

03 10 17 24 04 11 18 25 02 09| 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

```


which has a somewhat regular structure. But after the second transposition, we have

```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

This is a much less structured permutation and is much more difficult to cryptanalyze.



Block cipher principles

Block vs Stream Ciphers

- ▶ block ciphers process messages into blocks, each of which is then en/decrypted
- ▶ like a substitution on very big characters
 - ▶ 64-bits or more
- ▶ stream ciphers process messages a bit or byte at a time when en/decrypting
- ▶ many current ciphers are block ciphers
- ▶ hence are focus of course

Block Cipher Principles

- ▶ block ciphers look like an extremely large substitution
- ▶ would need table of 2^{64} entries for a 64-bit block
- ▶ arbitrary reversible substitution cipher for a large block size is not practical
 - ▶ 64-bit general substitution block cipher, key size $2^{64}!$
- ▶ most symmetric block ciphers are based on a **Feistel Cipher Structure**
- ▶ needed since must be able to **decrypt** ciphertext to recover messages efficiently

C. Shannon and Substitution-Permutation Ciphers

- ▶ in 1949 Shannon introduced idea of substitution-permutation (S-P) networks
 - ▶ modern substitution-transposition product cipher
- ▶ these form the basis of modern block ciphers
- ▶ S-P networks are based on the two primitive cryptographic operations we have seen before:
 - ▶ *substitution* (S-box)
 - ▶ *permutation* (P-box) (transposition)
- ▶ provide *confusion* and *diffusion* of message

Diffusion and Confusion

- ▶ Introduced by Claude Shannon to thwart cryptanalysis based on statistical analysis
 - ▶ Assume the attacker has some knowledge of the statistical characteristics of the plaintext
- ▶ cipher needs to completely obscure statistical properties of original message
- ▶ a one-time pad does this

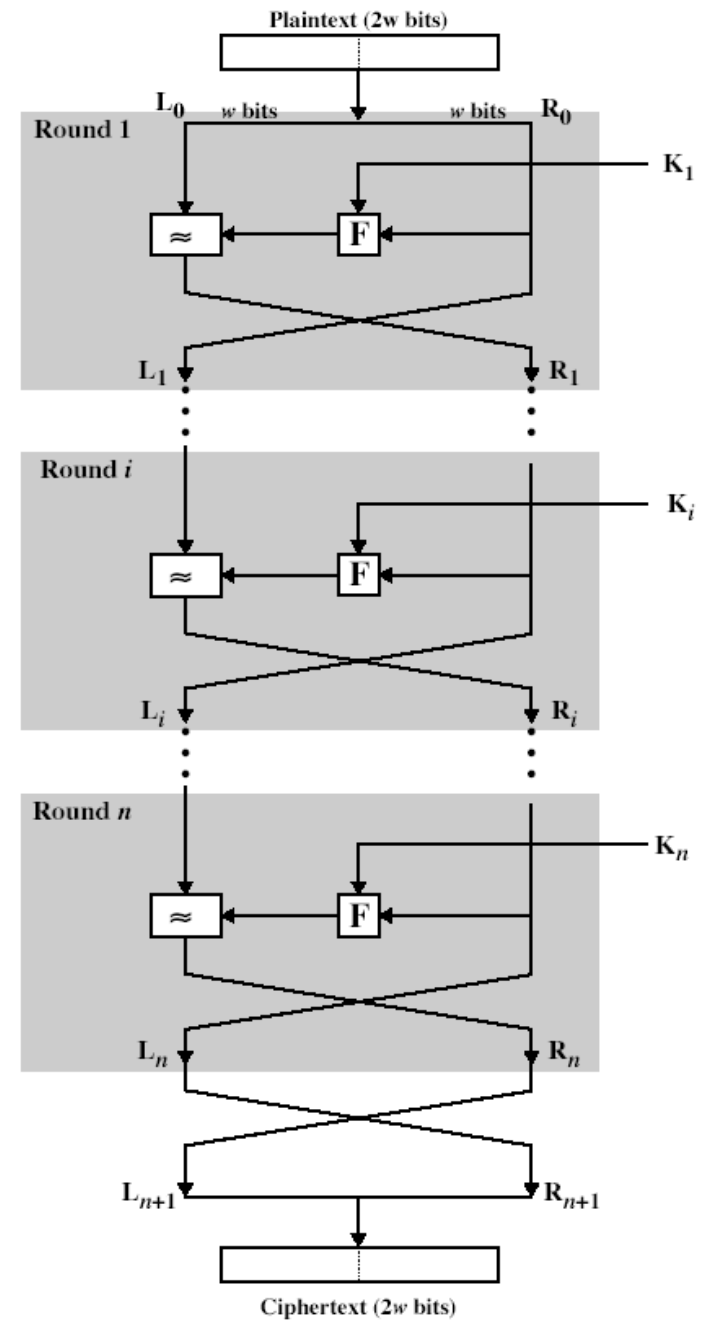
Diffusion and Confusion

- ▶ more practically Shannon suggested combining elements to obtain:
- ▶ **diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- ▶ **confusion** – makes relationship between ciphertext and key as complex as possible

Feistel Cipher Structure

- ▶ Horst Feistel devised the **feistel cipher**
 - ▶ implements Shannon's substitution-permutation network concept
- ▶ partitions input block into two halves
 - ▶ process through multiple rounds which
 - ▶ perform a substitution on left data half
 - ▶ based on round function of right half & subkey
 - ▶ then have permutation swapping halves

Feistel Cipher Structure



Feistel Cipher

- ▶ n sequential rounds
- ▶ A substitution on the left half L_i
 - ▶ 1. Apply a round function F to the right half R_i and
 - ▶ 2. Take XOR of the output of (1) and L_i
- ▶ The round function is parameterized by the subkey K_i
 - ▶ K_i are derived from the overall key K

Feistel Cipher Design Principles

- ▶ **block size**
 - ▶ increasing size improves security, but slows cipher
- ▶ **key size**
 - ▶ increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- ▶ **number of rounds**
 - ▶ increasing number improves security, but slows cipher
- ▶ **subkey generation**
 - ▶ greater complexity can make analysis harder, but slows cipher
- ▶ **round function**
 - ▶ greater complexity can make analysis harder, but slows cipher
- ▶ **fast software en/decryption & ease of analysis**
 - ▶ are more recent concerns for practical use and testing

F

