




# Chapter 1

Introduction



*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*

**—The Art of War, Sun Tzu**



# Background

- [[ In last several decades, the requirements of *information security* have undergone major changes.
- [[ The security was physical in the form of cabinets with combination of locks for sensitive documents.
- [[ The second change is the introduction of distributed systems and use of networks.
- [[ Use of networks and communications links requires measures to protect data during transmission



# Security

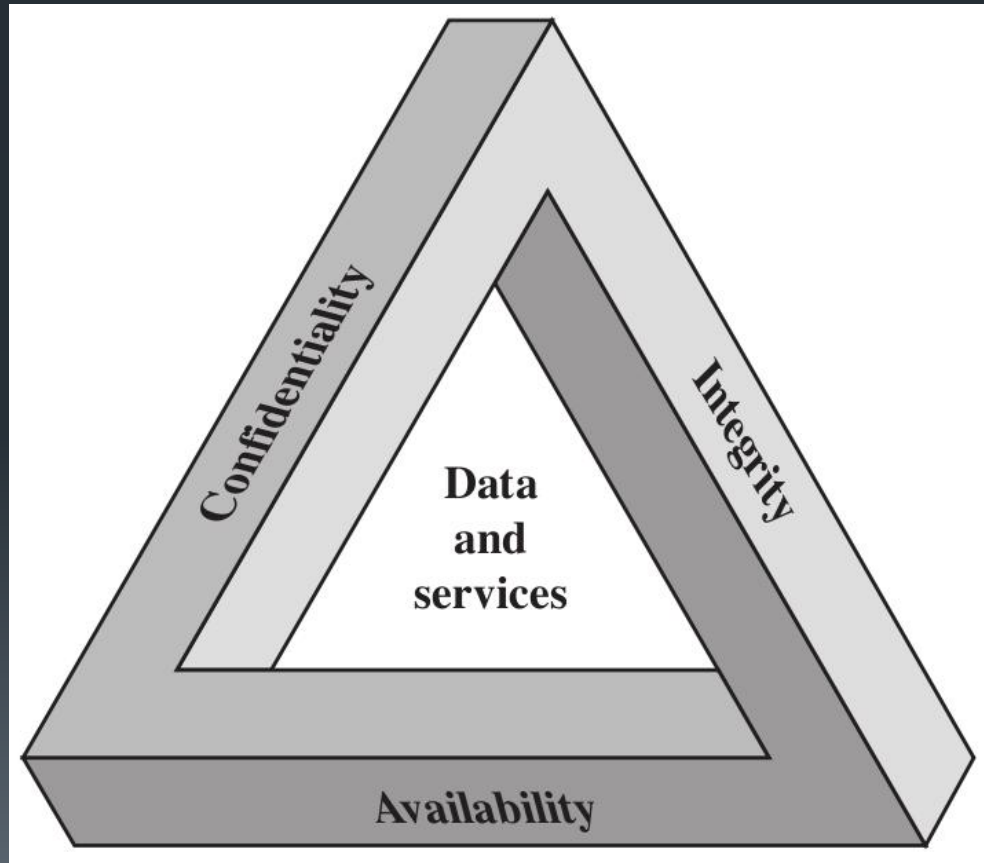
- [[ **Computer Security** - generic name for the collection of tools designed to protect data and to hide from hackers
- [[ **Network Security** - measures to protect data during their transmission
- [[ **Internet Security** - measures to protect data during their transmission over a collection of interconnected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



# Aim of Course

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

# Key Security Concepts





# Impact of Security Breaches

- [[ How do security breaches impact organizations?
  - [[ Effectiveness of primary operations are reduced
  - [[ Financial loss
  - [[ Damage to assets
  - [[ Harm to individuals



# OSI Security Architecture

- [[ To effectively access the resources of an organization, the network administrator has to define the requirements of security and characterize the approaches to satisfy those requirements
- [[ This is difficult enough in a centralized data processing environment.
- [[ ITU-T Recommendation X.800, Security Architecture for OSI, defines such a systematic approach.
- [[ The OSI security architecture is useful to administrators as a way of organizing the task of providing security.





# Aspects of Security

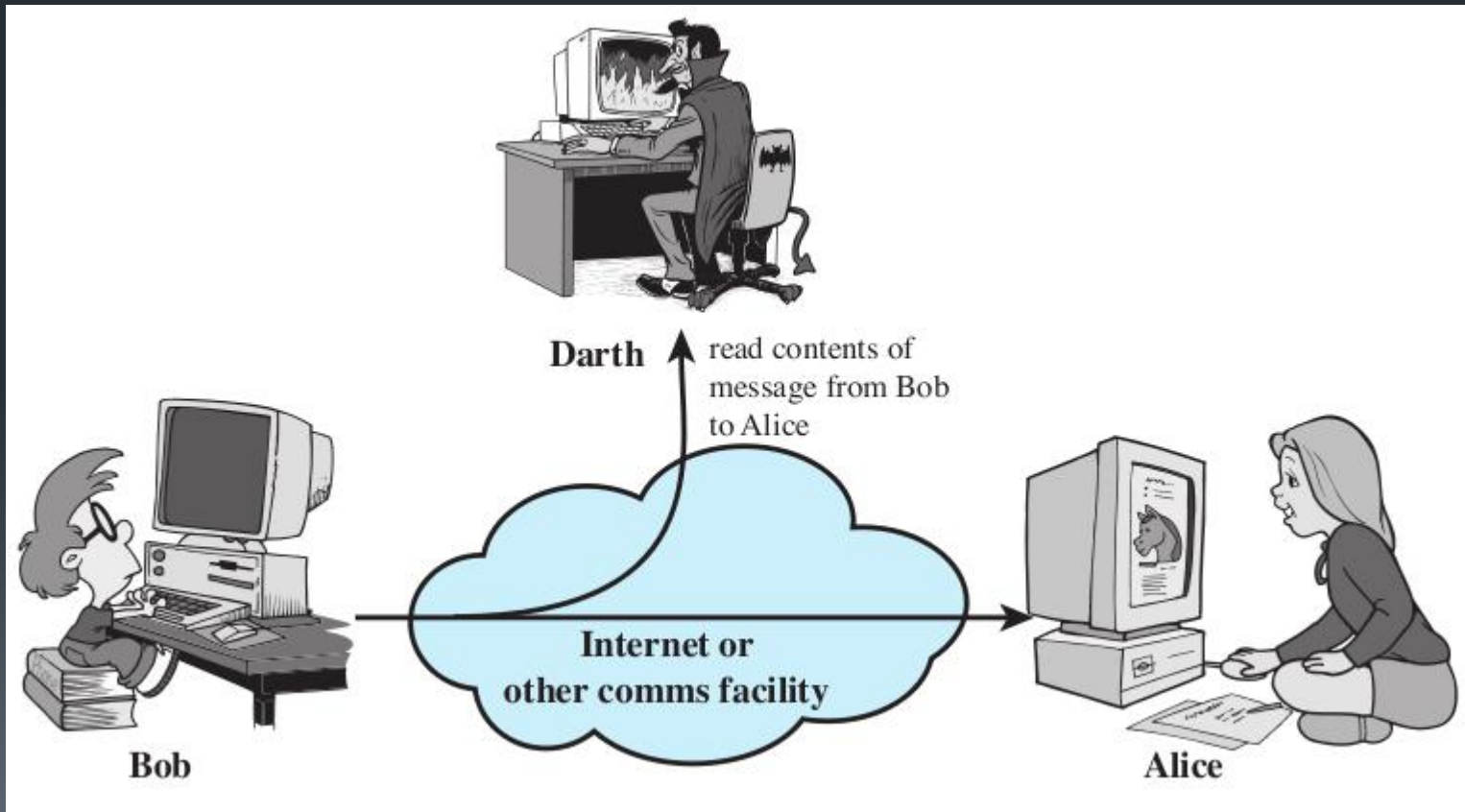
- [[ **Security attack:** Any actions that compromises the security of information owned by an organization (or a person)
- [[ **Security mechanism:** a mechanism that is designed to detect, prevent, or recover from a security attack
- [[ **Security service:** a service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service



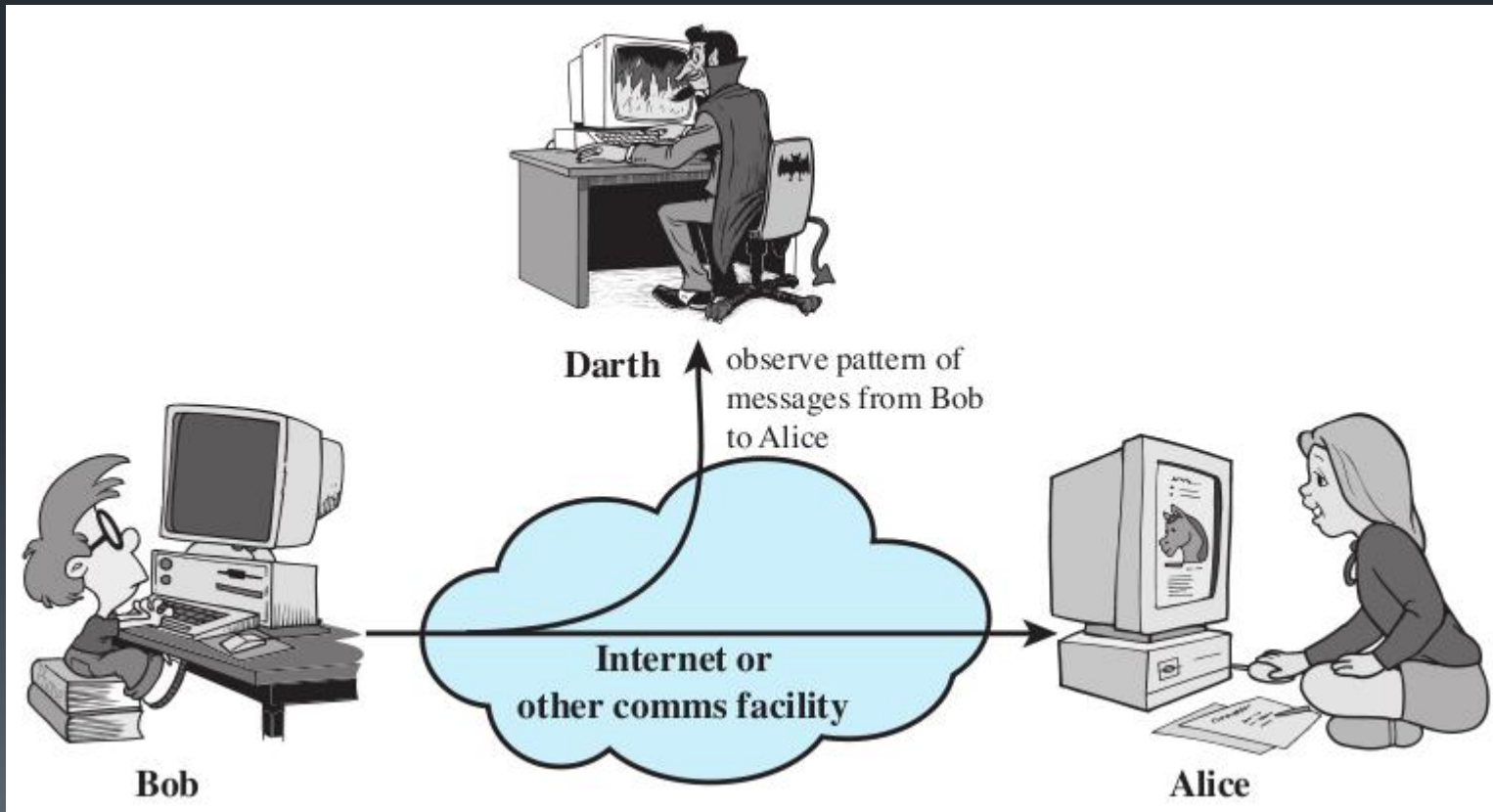
# Security Attacks

- [[ Passive Attack :Make use of information, but not affect system resources, e.g.
  - [[ Release message contents
  - [[ Traffic analysis
- [[ Relatively hard to detect, but easier to prevent
  
- [[ Active Attack ; I Alter system resources or operation, e.g.
  - [[ Masquerade
  - [[ Replay
  - [[ Modification
  - [[ Denial of service
- [[ Relatively hard to prevent, but easier to detect

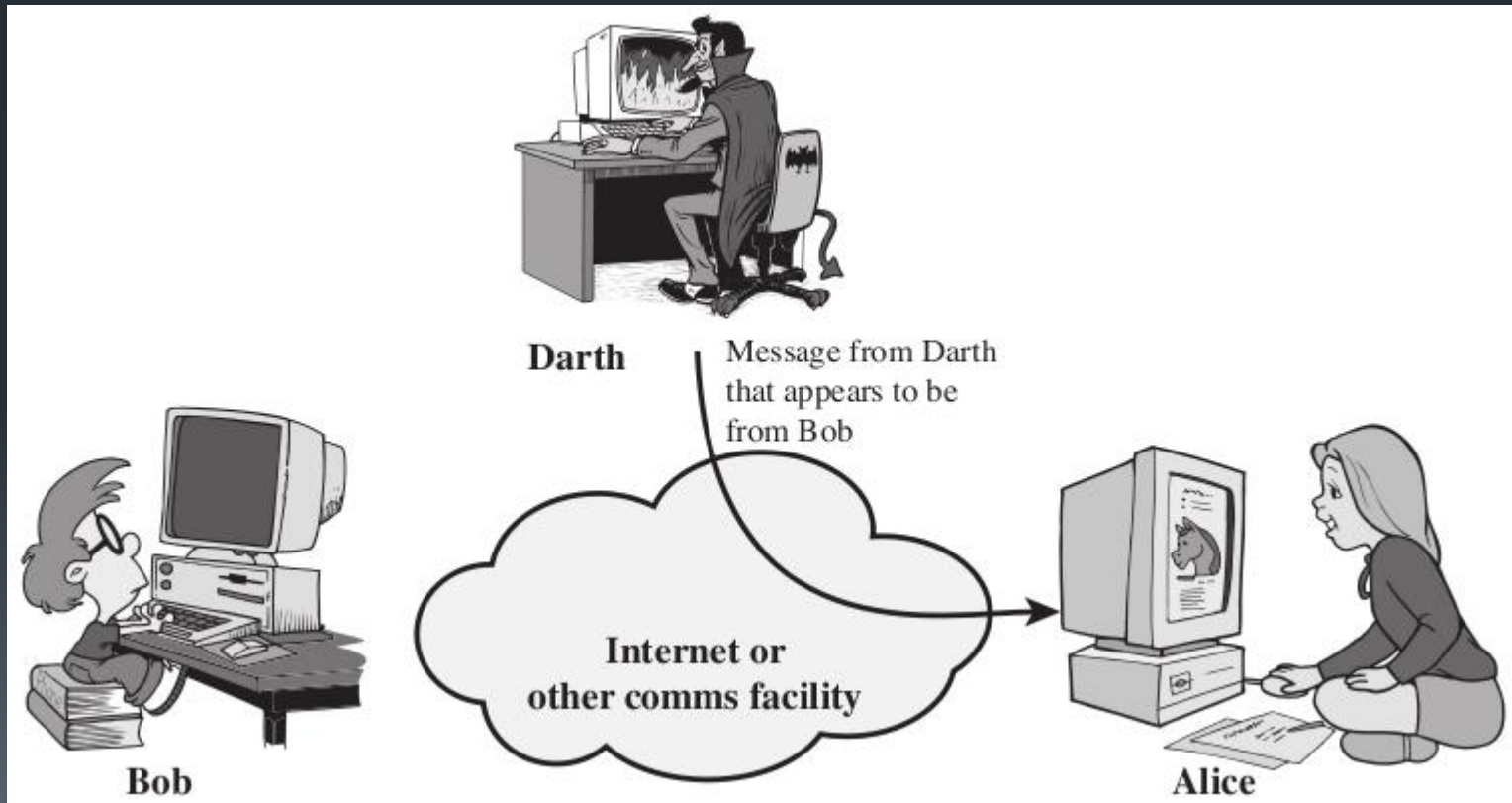
# Release Message Contents



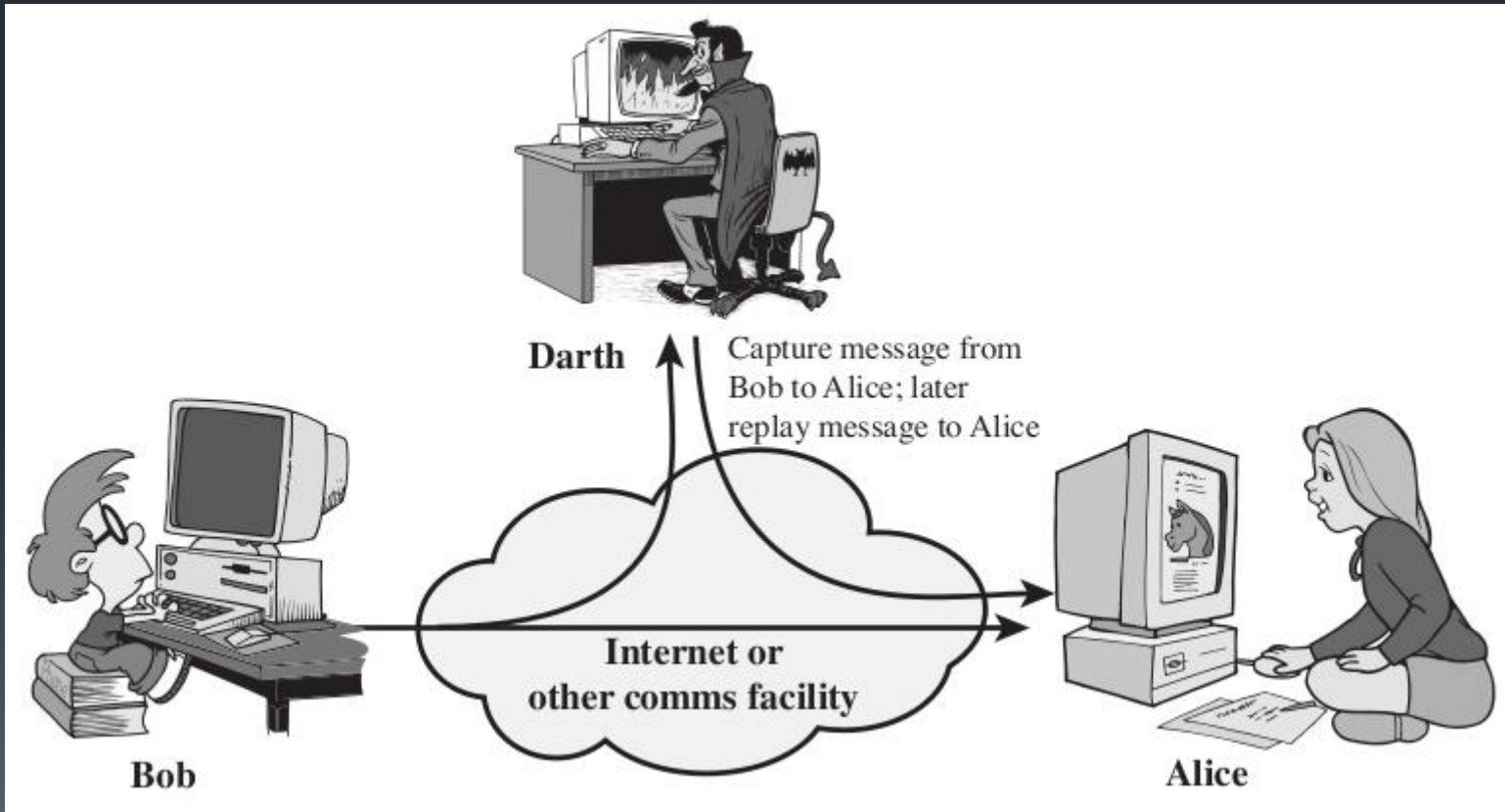
# Traffic Analysis



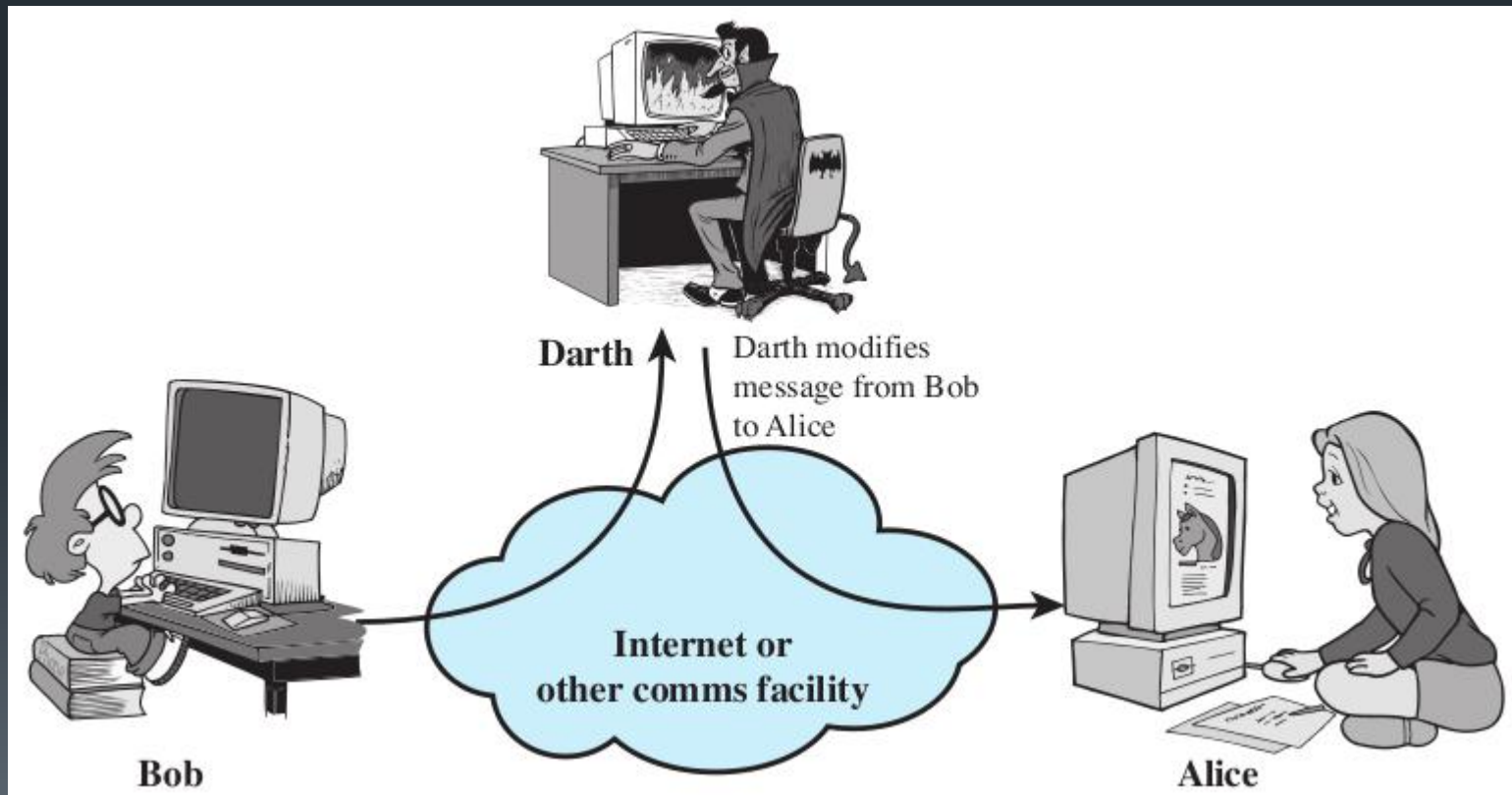
# Masquerade Attack



# Replay Attack

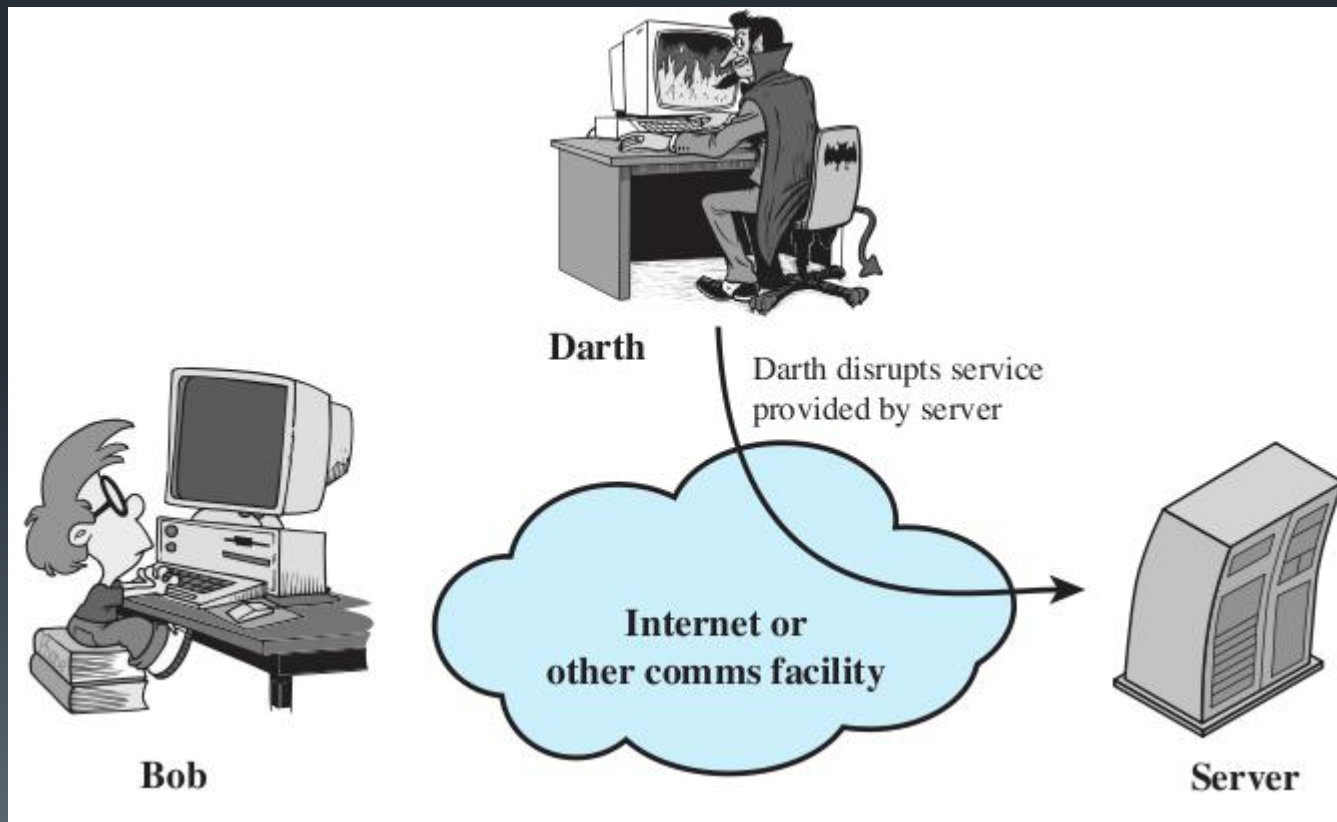


# Modification Attack





# Denial Of Service Attack







# Security Service

- [[ Security service is a service which ensures adequate security of the systems or of data transfers
- [[ X.800 Recommendation divides security services into 5 categories:
  - [[ Authentication
  - [[ Access control
  - [[ Data confidentiality
  - [[ Data integrity
  - [[ Nonrepudiation
  - [[ *Availability service*



# Authentication

- [[ The authentication service is concerning with assuring that a communication is authentic:
- [[ The recipient of the message should be sure that the message came from the source that it claims to be
- [[ All communicating parties should be sure that the connection is not interfered with by unauthorized party.
- [[ **Example:** consider a person, using online banking service. Both the user and the bank should be assured in identities of each other



# Access control

- [[ This service controls
  - [[ who can have access to a resource;
  - [[ under what conditions access can occur;
  - [[ what those accessing are allowing to do.
- [[ **Example:** in online banking a user may be allowed to see his balance, but not allowed to make any transactions for some of his accounts



# Data confidentiality

- [[ The protection of data from unauthorized disclosure (from passive attacks).
  - [[ Connection confidentiality (*protection of all user data on a connection*)
  - [[ Connectionless confidentiality (*protection of all user data in a single block*)
  - [[ Selective field confidentiality
  - [[ Traffic-Flow Confidentiality



# Data Integrity

- [[ The assurance that data received are exactly as sent by an authorized entity, i.e. contain
  - [[ no modification
  - [[ no insertion
  - [[ no deletion
  - [[ no replay
- [[ Connection integrity with recovery
- [[ Connection integrity without recovery
- [[ Selective field connection integrity
- [[ Connectionless integrity



# Nonrepudiation

- [[ Protection against denial by one of the entities involved in a communication of having participated in the communication.
- [[ Nonrepudiation can be related to
  - [[ Origin: proof that the message was sent by the specified party
  - [[ Destination: proof that the message was received by the specified party
- [[ **Example:** Imagine a user of online banking who has made a transaction, but later denied that. How the bank can protect itself in a such situation?



# Security Mechanism

- [[ Feature designed to detect, prevent, or recover from a security attack
- [[ No single mechanism that will support all services required
- [[ Specific security mechanisms :
  - [[ Encipherment, Digital signatures, Access Controls, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control, Notarization



# Practical sides of Attacks

- [[ The attacks discussed earlier can come in number of forms in real life. They can be classified in two categories:
  - [[ Application Level Attacks: the attacker attempts to access, modify or prevent access to information or application. Like obtains' someone's credit card information or changing the amount in financial transaction.
  - [[ Network Level Attacks: attacker attempt to slow down or completely make the network inaccessible.





# Programs that Attack

- [[ Virus: It is a program code that attaches itself to a legitimate program and runs when the legitimate program runs.
- [[ Viruses can be classified in following categories:
  - [[ **Parasitic virus**: attaches itself to executable files and keeps replicating
  - [[ **Memory resident** : attaches to main memory and infects every executable program that is executable
  - [[ **Boot sector virus**: infects master boot record of the disk
  - [[ **Stealth virus**: prevents antivirus from detecting it
  - [[ **Polymorphic virus**: keeps changing its signature on every execution
  - [[ **Metamorphic virus**: in addition to changing signature, it keeps rewriting every time



# Worm

- [[ A worm replicates itself again and again
- [[ The replication grows so much that ultimately the computer or the network on which the worm resides, become very slow and finally stops.
- [[ A worm attack attempts to make the computer or the network unusable by eating its all resources



# Trojan Horse

- [[ It attempts to reveal confidential information to attacker.
- [[ A Trojan horse can silently sit in the code for a login screen by attaching itself to it.
- [[ When the user enters the user id and password, the Trojan horse can capture the details and send this details to attacker without knowledge of the user.
- [[ The attacker can then misuse the details.



# Applets and ActiveX Controls

- [[ Some web pages contain small programs that get downloaded onto the client along with the web page, these program then get execute inside the browser.
- [[ Sun Microsystems provide Java Applets and Microsoft provide ActiveX control for this purpose
- [[ These programs are used to periodically request for information from a web server.
- [[ Such programs may work as virus and can cause damage to computer



# Sniffing and Spoofing

- [[ Attacker targets the packets as they travel from source to destination on Internet.
- [[ These attacks take two main forms:
  - [[ Packet Sniffing: It is a passive attack on an on going conversation
  - [[ Packet Spoofing: The attacker sends packet with a false source address



# Phishing

- [[ In 2006, the estimated losses due to phishing were 2.8 billion USD.
- [[ The attacker sets up fake website which looks like real website and get the user credentials which can be misused later.



# Caesar Cipher

- [[ earliest known substitution cipher
- [[ by Julius Caesar
- [[ first attested use in military affairs
- [[ replaces each letter by a letter *three* places down the alphabet
- [[ example:  
meet me after the toga party  
PHHW PH DIWHU WKH WRJD SDUWB

# Caesar Cipher

[[ 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  
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

[[ then have Caesar cipher as:

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

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

[[ **modulo arithmetic:**  $1 = 27 \bmod 26$ ,  $3 = 29 \bmod 26$



# Brute Force Search of Caesar Cipher

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	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	geb	qldx	mxxoqv
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	hsjllq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	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	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	umnb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzcx	znc	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qlix	qi	ejxiv	xli	xske	tevxc



# Cryptanalysis of Caesar Cipher

- [[ only have 26 possible keys
  - [[ Could shift  $K = 0, 1, 2, \dots, 25$  slots
- [[ could simply try each in turn
- [[ a **brute force search**
- [[ given ciphertext, just try all shifts of letters
- [[ do need to recognize when have plaintext
- [[ Test: break ciphertext  
GCUA VQ DTGCM



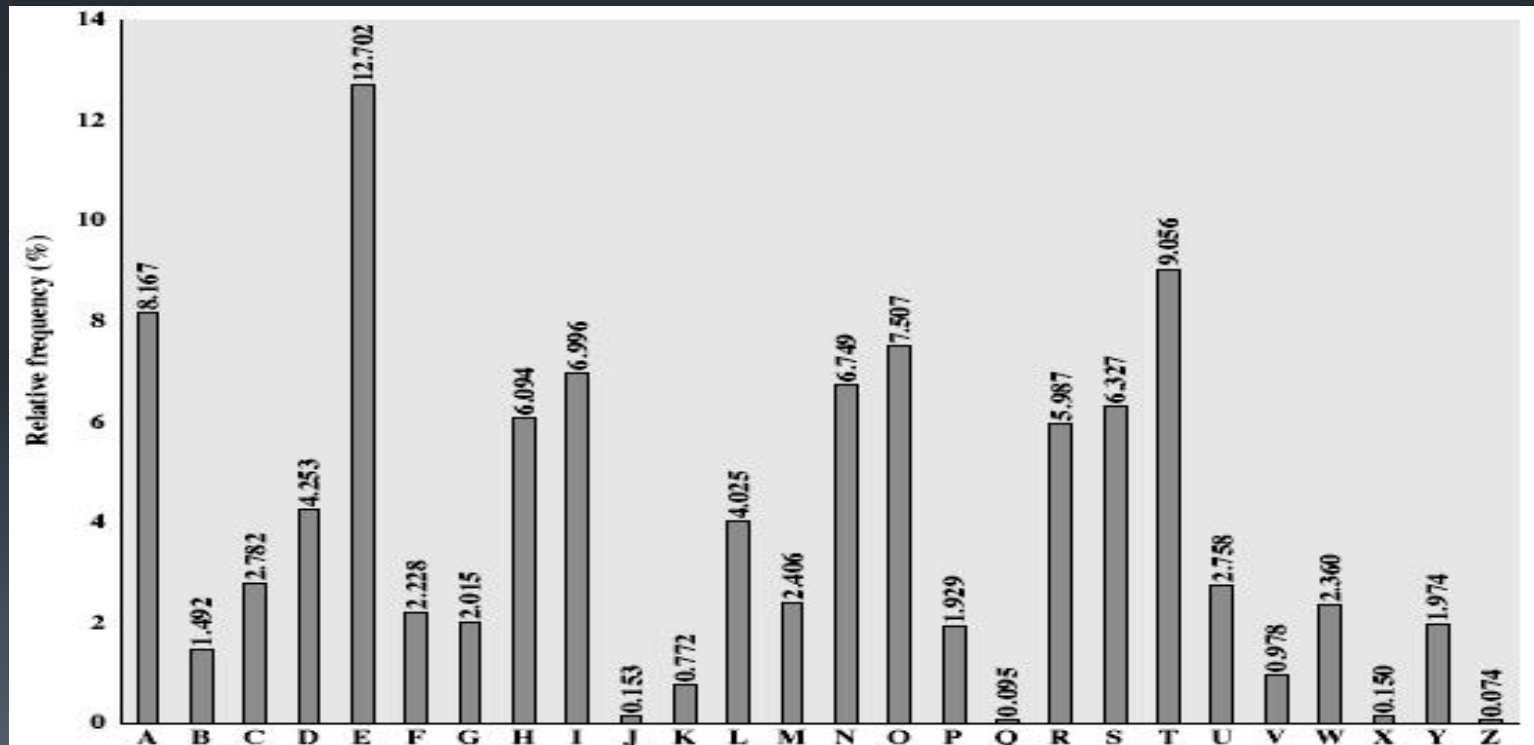
# Monoalphabetic Cipher

- Rather than just shifting the alphabet
- Could shuffle (jumble) the letters arbitrarily
- May call a permutation of letters from A to Z
- Each plaintext letter maps to a different random ciphertext letter
- Hence, the key K is 26 letters long
- 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 K V Q F I B J W P E S C X H T M Y A U O L R G Z  
N
- Plaintext: ifwewishtoreplaceletters
- Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

# Frequency Analysis

- [[ letters are not equally commonly used
- [[ in English **e** is by far the most common letter
- [[ then T,R,N,I,O,A,S
- [[ other letters are fairly rare
- [[ cf. Z,J,K,Q,X
- [[ have tables of single, double & triple letter frequencies

# English Letter Frequencies



# Example Cryptanalysis

[ given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ  
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX  
EPYEPOPDSZUFPOMBZWPFUPZHMDJUDTMOHMQ

[ count relative letter frequencies (see text)

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  t a           e e te a that e e a           a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  e t   ta t ha e ee a e th   t a|
EPYEPOPDSZUFPOMBZWPFUPZHMDJUDTMOHMQ
  e e e tat e   the   t
```

[ guess P & Z are e and t

[ guess ZW is th and hence ZWP is 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

# Playfair Cipher

- [[ A 5X5 matrix of letters based on a keyword
- [[ Fill in letters of keyword
- [[ Fill rest of matrix with other letters
- [[ eg. 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

# Playfair Cipher

- [[ plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert a filler like 'X',  
eg. "balloon" encrypts as "ba lx lo on"
  2. 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"
  3. 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"
  4. 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)





# Playfair Cipher

- [[ Perform encryption using Playfair cipher
  - [[ It is very easy subject.
  - [[ Key: playfair



# Polyalphabetic Ciphers

- [[ another approach to improving security is to use multiple cipher alphabets
- [[ called **polyalphabetic substitution ciphers**
- [[ makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- [[ use a key to select which alphabet is used for each letter of the message
- [[ use each alphabet in turn
- [[ repeat from start after end of key is reached

# Example

key:       deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

- [ write the plaintext out
- [ write the keyword repeated above it
  - [ eg using keyword *deceptive*
- [ use each key letter as a caesar cipher key
- [ encrypt the corresponding plaintext letter



# Vigenère Cipher


- [[ Simplest polyalphabetic substitution cipher
- [[ Effectively multiple caesar ciphers
- [[ Key is multiple letters long  $K = k_1 k_2 \dots k_d$
- [[  $i^{\text{th}}$  letter specifies  $i^{\text{th}}$  alphabet to use
- [[ Use each alphabet in turn

# Vigenère Cipher

message

keyword

<b>h</b>	<b>i</b>	<b>s</b>	<b>b</b>	<b>o</b>	<b>w</b>	<b>t</b>	<b>i</b>	<b>e</b>	<b>i</b>	<b>s</b>	<b>a</b>	<b>c</b>	<b>a</b>	<b>m</b>	<b>e</b>	<b>r</b>	<b>a</b>	
<b>c</b>	<b>o</b>	<b>d</b>	<b>e</b>	<b>c</b>	<b>o</b>	<b>d</b>	<b>e</b>	<b>c</b>	<b>o</b>	<b>d</b>	<b>e</b>	<b>c</b>	<b>o</b>	<b>d</b>	<b>e</b>	<b>c</b>	<b>o</b>	
<b>7</b>	<b>8</b>	<b>18</b>	<b>1</b>	<b>14</b>	<b>22</b>	<b>19</b>	<b>8</b>	<b>4</b>	<b>8</b>	<b>18</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>12</b>	<b>4</b>	<b>17</b>	<b>0</b>	
<b>+</b>	<b>2</b>	<b>14</b>	<b>3</b>	<b>4</b>	<b>2</b>	<b>14</b>	<b>3</b>	<b>4</b>	<b>2</b>	<b>14</b>	<b>3</b>	<b>4</b>	<b>2</b>	<b>14</b>	<b>3</b>	<b>4</b>	<b>2</b>	<b>14</b>

Wolfram  Demonstrations Project demonstrations.wolfram.com



# One-Time Pad

- [[ If a truly random key as long as the message is used, the cipher will be secure , called a One-Time pad
- [[ It is implemented using a random set of non repeating characters
- [[ Can only use the key **once** though
- [[ Problems in generation & safe distribution of key



# Transposition Techniques

[[ A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters, referred to as a transposition cipher

[[ For example, to encipher the message "meet me after the toga party" write the following:

```
m e m a t r h t g p r y  
e t e f e t e o a a t
```

[[ The encrypted message is:  
MEMATRHTGPRYETEFETEOAAT

# Transposition Techniques

- [[ A more complex scheme is to 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
  - [[ Message is : attack postponed until two am

```
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
```