19CSE311 - COMPUTER SECURITY
UNIT-1

January 13, 2022

Dr.Remya S/Mr. Sarath R
Assistant Professor
Department of Computer Science

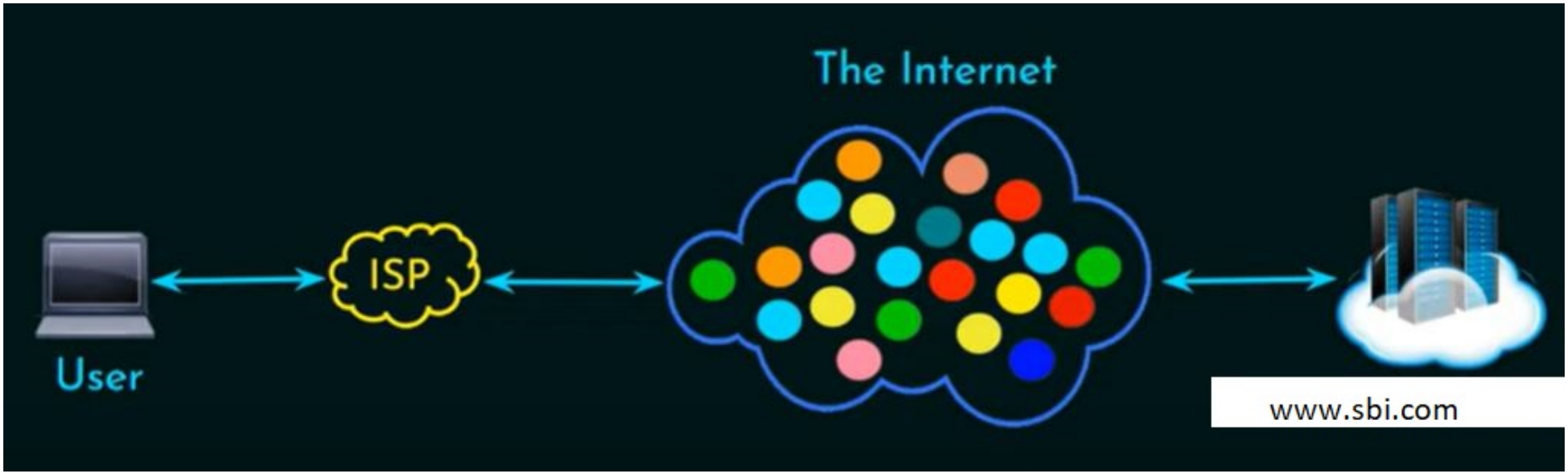
AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY
School of Engineering

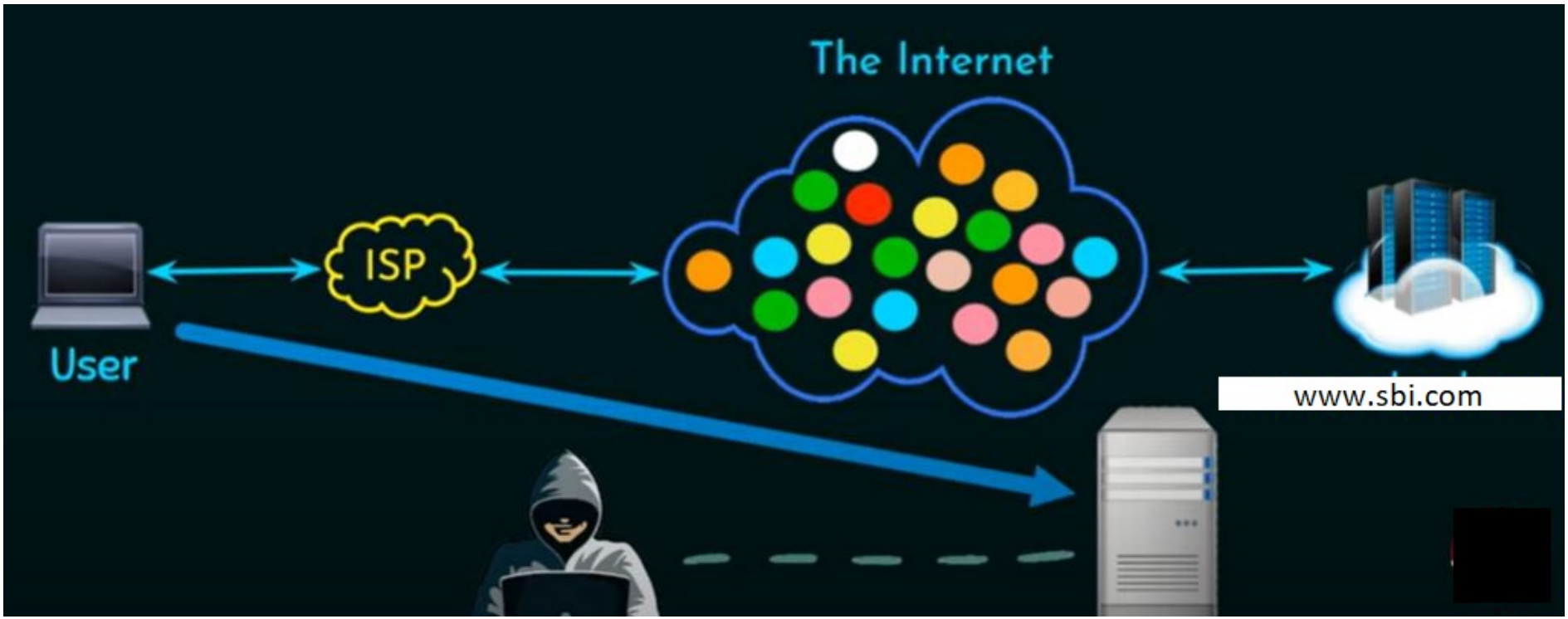
Agenda

- Introduction to cryptography
- Mathematical concepts-Algebra & Number Theory
- Block Cipher
- Public Key Cryptography
- Cryptographic Hash functions & Digital Signature
- Security Practices & System security
- Email, IP & Web security

Why Network Security and Cryptography?

- Why are we learning Network Security?
- What would we do with it?
- Understand information security services
- Be aware of vulnerabilities and threats
- Realize why network security is necessary
- What are the elements of a comprehensive security program

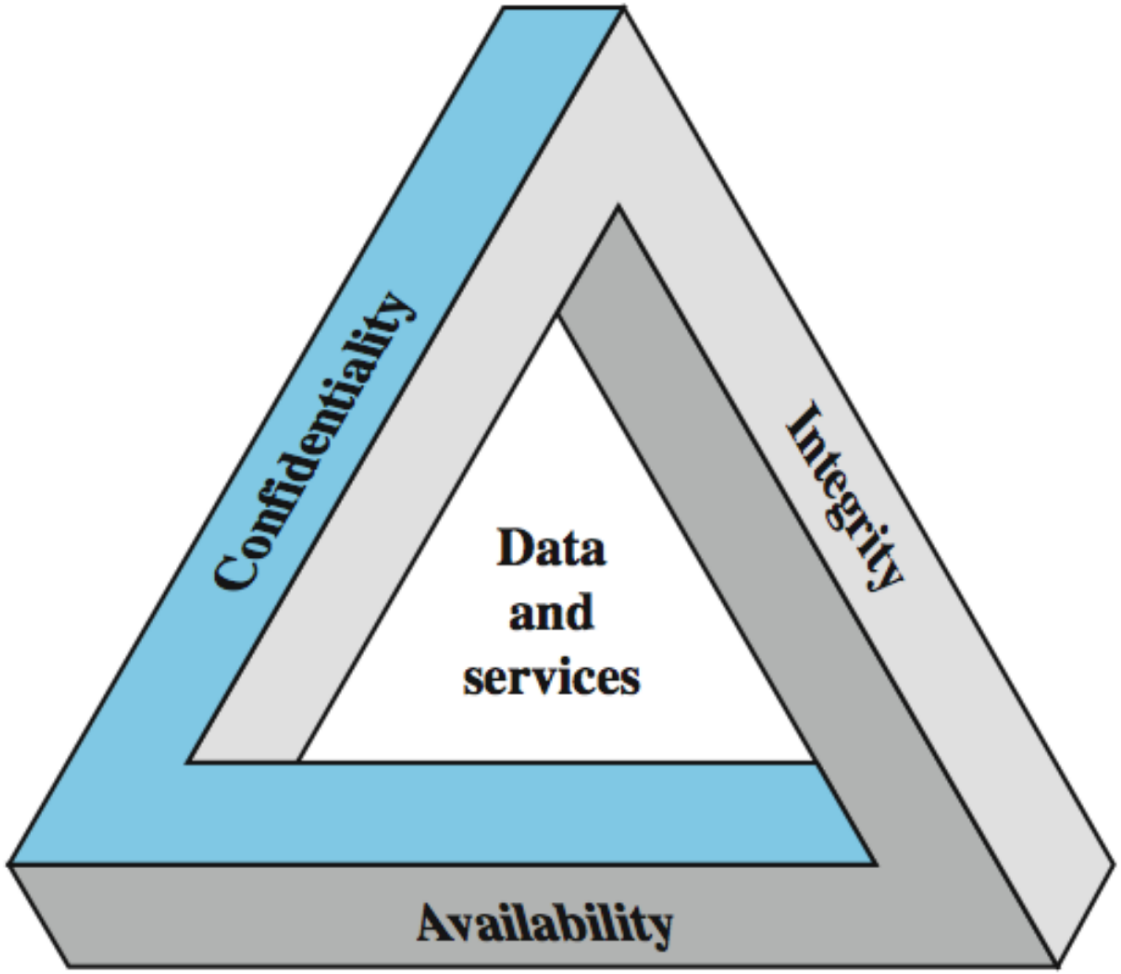



The Internet
ISP
User
www.sbi.com

CIA Triad
Computer Security -Definition

- 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)[NIST].
- 3 Key Objectives
  1. Confidentiality
     1. Data confidentiality
     2. Privacy
  2. Integrity
     1. Data integrity
     2. System integrity
  3. Availability

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

1. Confidentiality
   - Prevent unauthorized access and disclosure
   - Unauthorized access: Nobody else can access , except the right entities whom are involved in this transaction
   - Disclosure: The message should not be open enough
   - 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.
2. Integrity
   - Don't allow any modification of message by unauthorized people
   - sent = Received
   - 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.
3. Availability:
   - Ensure the timely and reliable access to the system

Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service

OSI Security Architecture

- 3 aspects of information security
  1. Security Attack:Any action that compromises the security of information owned by an organization
  2. Security Mechanism:detect, prevent, recover
  3. Security Service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- ITU-T X.800 "Security Architecture for OSI"
- It defines a systematic way of defining and providing security requirements
- 2 Terms
  1. threat – a potential for violation of security
  2. attack – an assault on system security, a deliberate attempt to evade security services

Threats & Attacks

- **Threats**: 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.

- Security Attack
  1. Passive Attack
  2. Active Attack
- Security services
  1. Authentication
  2. Access Control
  3. Data Confidentiality
  4. Non repudiation
- Security Mechanisms
  1. Encipherment
  2. Digital Signature
  3. Access Control
  4. Data Integrity
  5. Authentication Exchange
  6. Routing Control

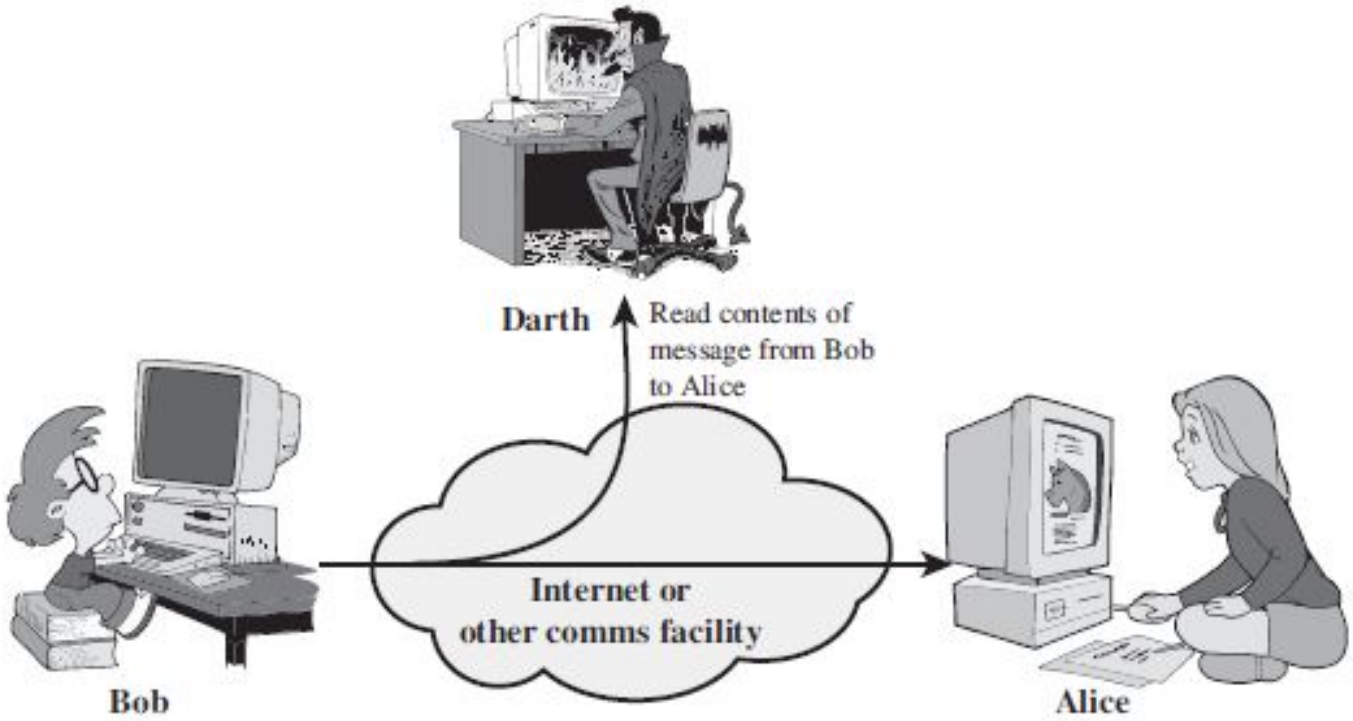
Security Attacks

- Action that comprises the security of an individual or an organization
- 2 Types
  1. Passive Attack: attempts to learn or make use of information from the system but does not affect system resources
     1. Release of message contents
     2. Traffic analysis
  2. Active Attack: attempts to alter system resources or affect their operation.
     1. Masquerade
     2. Replay
     3. Modification of messages
     4. Denial of service

Passive Attack

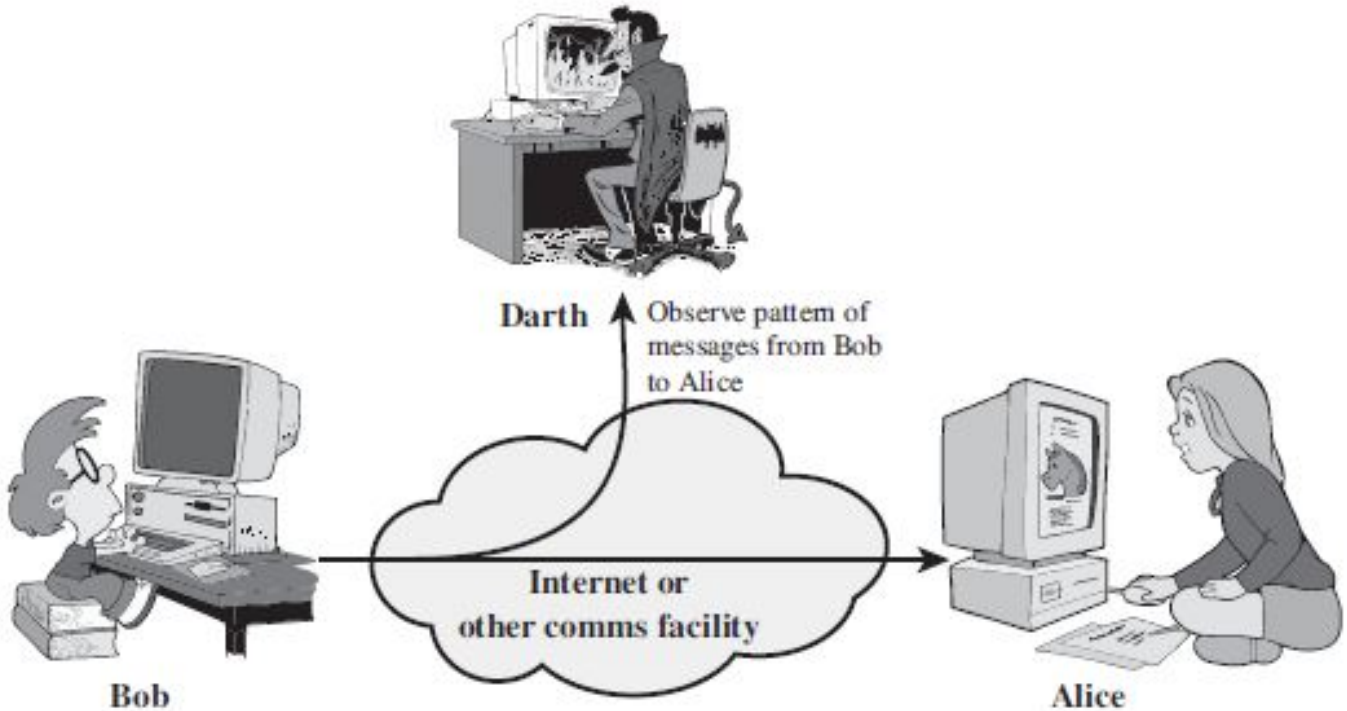
- Attempts to learn or make use of information from the system
- Does not affect system resources
- Eavesdropping or monitoring of transmissions
- Goal:Obtain information that is being transmitted

Passive Attack-Release of Message contents



(a) Release of message contents

Passive Attack-Traffic Analysis



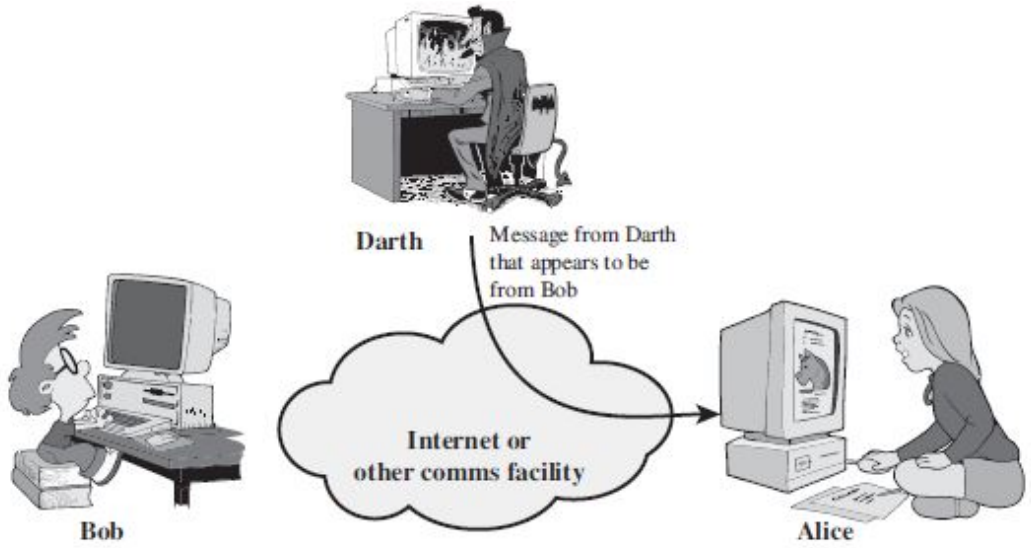
(b) Traffic analysis

Active Attack

- It involves some modification of the data stream or the creation of a false stream

Active Attack-Masquerade

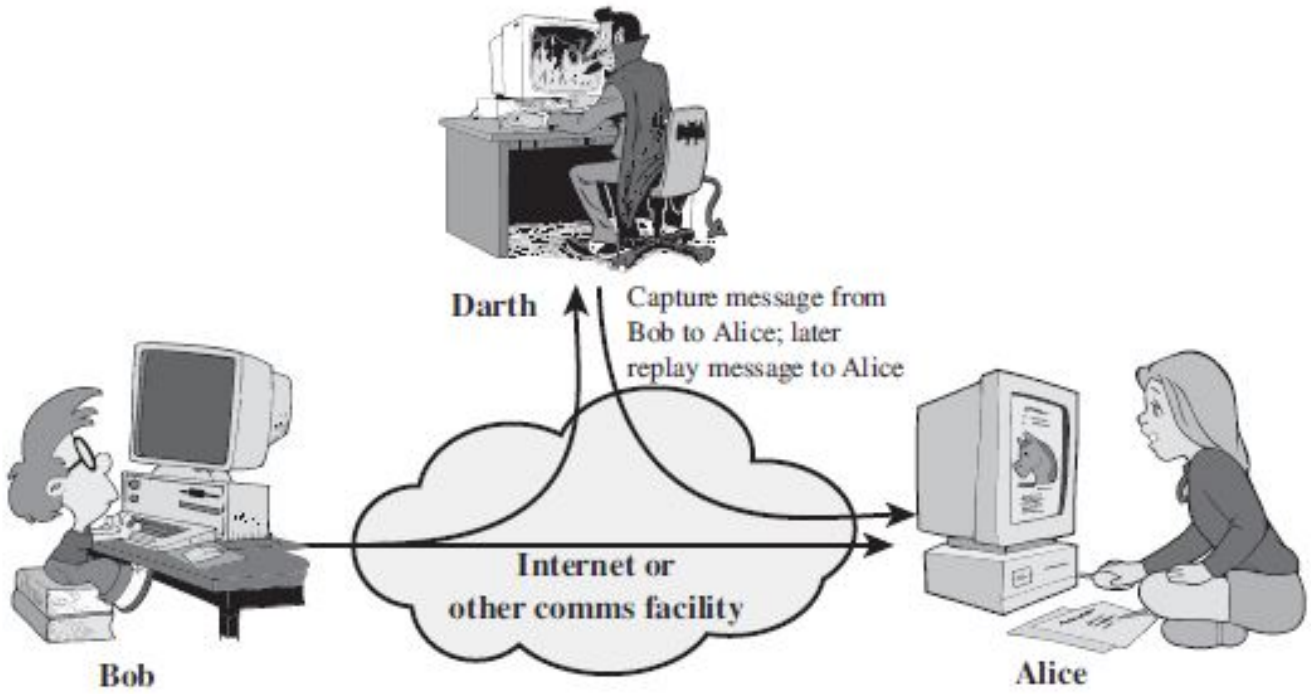
- Takes place when one entity pretends to be a different entity
- A masquerade attack usually includes one of the other forms of active attack.
- For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



(a) Masquerade

Active Attack-Replay

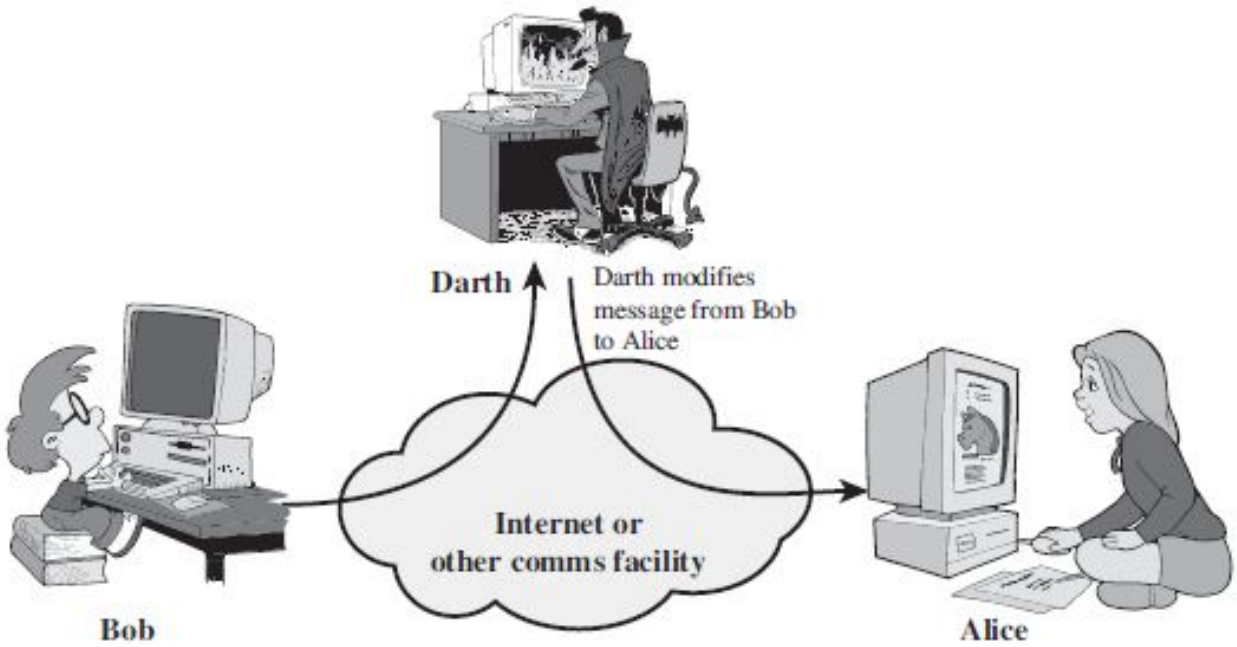
- involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



(b) Replay

Active Attack-Modification of messages

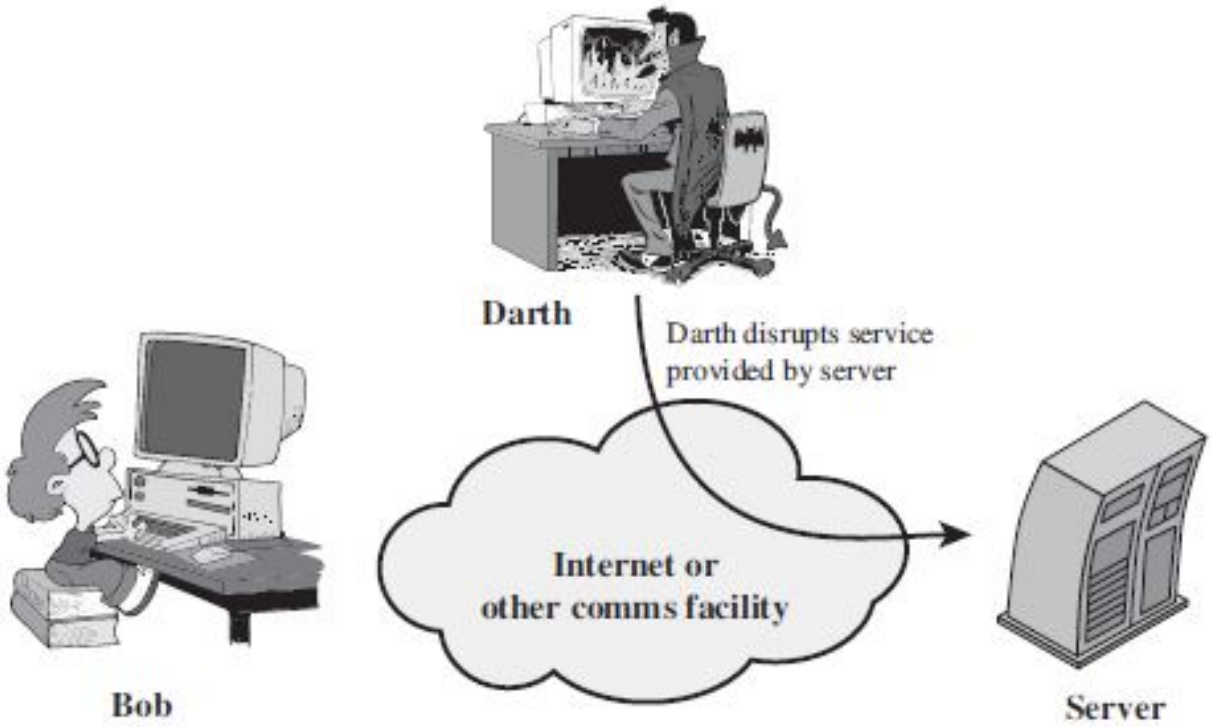
- means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect



(c) Modification of messages

Active Attack-Denial of Service(DoS)

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



(d) Denial of service

Passive Vs Active Attacks

No	Active Attack	Passive Attack
1	Attacker needs to have control media or network.	Attacker observe the communication in media or network.
2	It can be easily detected.	It cannot be easily detected.
3	It affects the system.	It does not affect the system.
4	It involves modification in data.	It involves in monitoring in data.
5	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
6	It is difficult to prevent network from active attack.	Passive attack can be prevented.
7	Types of active attack: Masquerade, replay, denial of service, modification of message.	Types of passive attack: release of message content, Traffic analysis.

Security Services

- A processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.[RFC-2828]
- **Authentication**:Proves the identity of the sender
- 2 types of authentication
  1. Peer entity authentication : Provides for the corroboration of the identity of a peer entity in an association
  2. Data origin authentication : : Provides for the corroboration of the source of a data unit.
- **Access Control**: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**:Protection of transmitted data from passive attacks
- **Data Integrity**:Send=Receive
- **Non repudiation**: Nonrepudiation prevents either sender or receiver from denying a transmitted message.

Security Mechanism:

- Security services implement security policies that are implemented by security mechanism
- 2 Types
  - Specific security mechanism: incorporated into the appropriate protocol layer in order to provide some of the OSI security services.Pervasive security mechanism:Mechanisms that are not specific to any particular OSI security service or protocol layer.
- **Specific Security Mechanism**
- **Encipherment**: Convert the plain text into cipher text before sending the data
- **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.

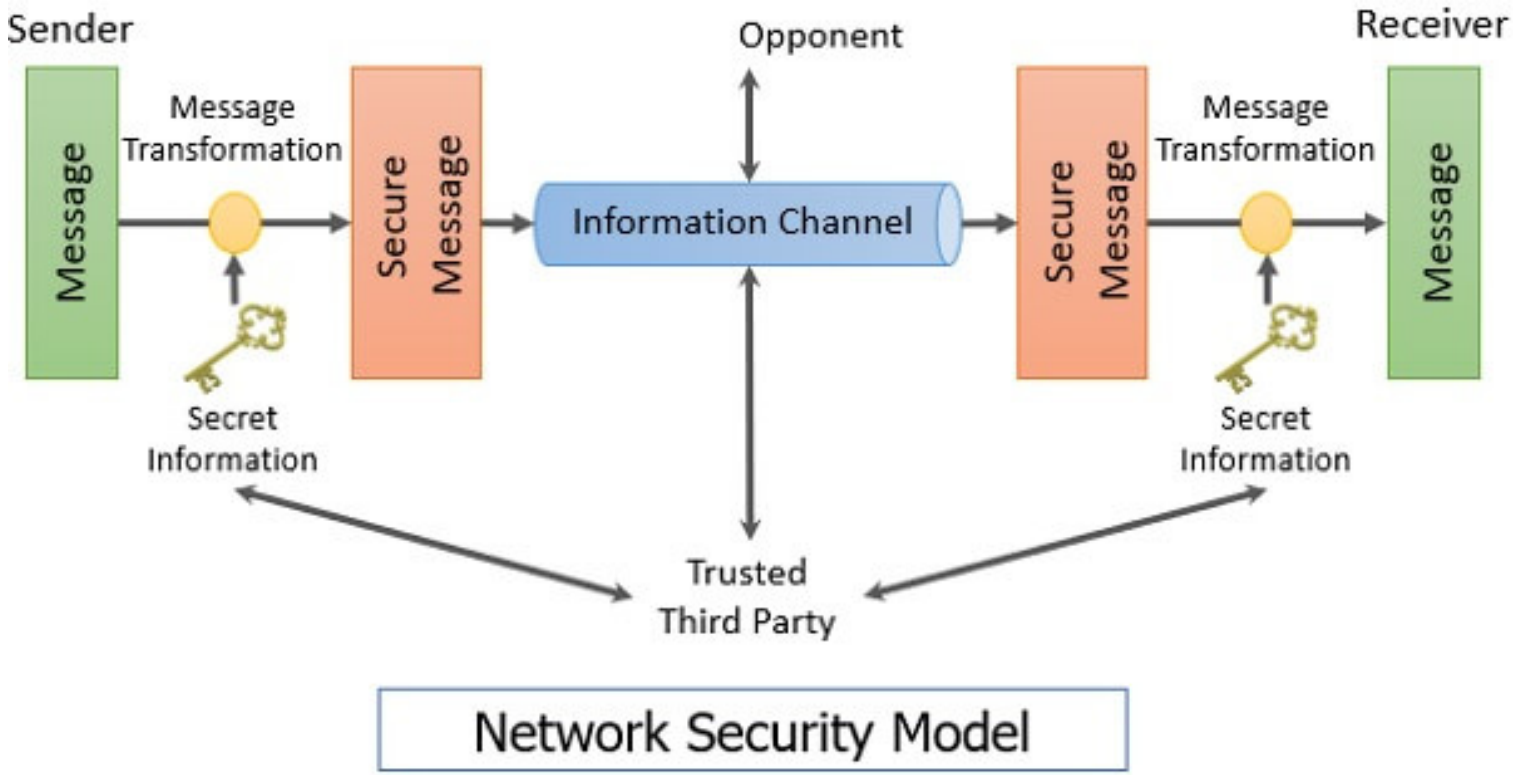
Frame Title

- **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.

Pervasive Security Mechanism

- **Trusted Functionality**: perceived to be correct with respect to some criteria
- **Security Label**: The marking bound to a resource that names or designates the security attributes of that resource.
- **Event Detection**: Detection of security-relevant events.
- **Security Recovery**: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Network Security Model

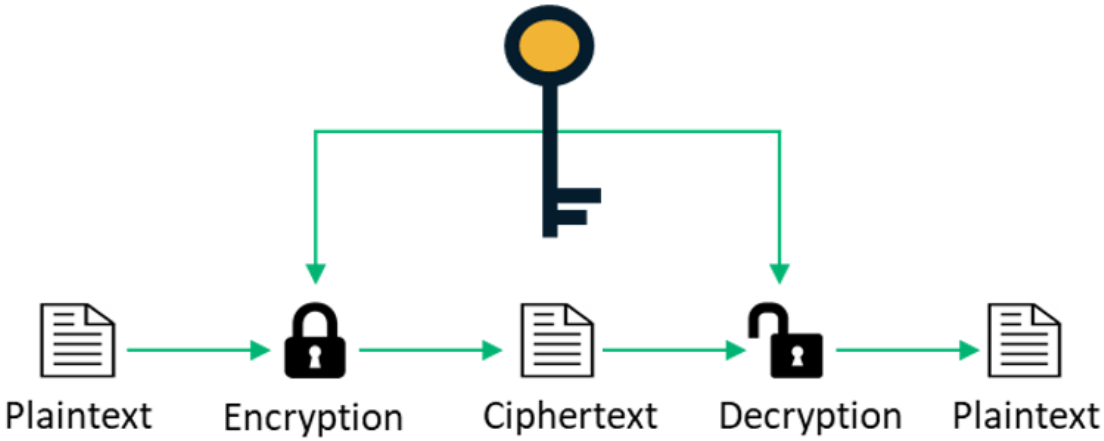


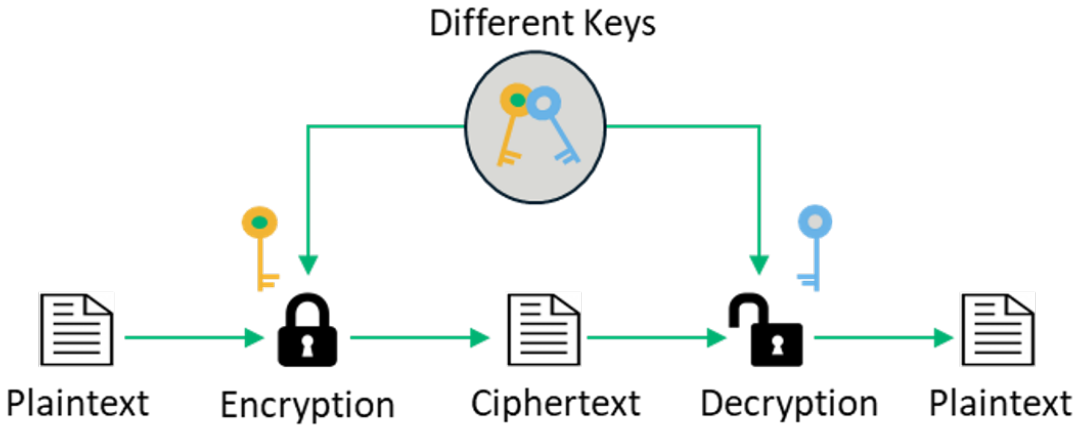
This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Cryptography

1. Symmetric Cryptography(Private key cryptography)
2. Asymmetric Cryptography(Public key cryptography)





Some Basic Terminology

- Plaintext - original message
- Ciphertext - coded message
- Cipher - algorithm for transforming plaintext to ciphertext
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to ciphertext
- Decipher (decrypt) - recovering plaintext from ciphertext
- Cryptography - study of encryption principles/methods
- Cryptanalysis (codebreaking) - study of principles/ methods of deciphering ciphertext without knowing key
- Cryptology - field of both cryptography and cryptanalysis

Cryptography

- can characterize cryptographic system by:
  1. Type of encryption operations used
     - substitution
     - transposition
     - product
  2. Number of keys used
     - single-key or private
     - two-key or public
  3. Way in which plaintext is processed
     - block
     - stream

Classical Encryption Techniques

1. Substitution Techniques
    1. Caesar Cipher
    2. Mono alphabetic Cipher
    3. Play fair Cipher
    4. Hill Cipher
    5. Polyalphabetic Cipher
    6. One-Time pad
2. Transposition Techniques

Classical Substitution Ciphers

- Substitution technique is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.
- If the plain text (original message) is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text.

Caesar Cipher

- This the simplest substitution cipher by Julius Caesar.
- In this substitution technique, to encrypt the plain text, each alphabet of the plain text is replaced by the alphabet three places further it.
- And to decrypt the cipher text each alphabet of cipher text is replaced by the alphabet three places before it.
- Assign a numerical equivalent to each letter

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 the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:[2]

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

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

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26 \quad \textbf{(2.1)}$$

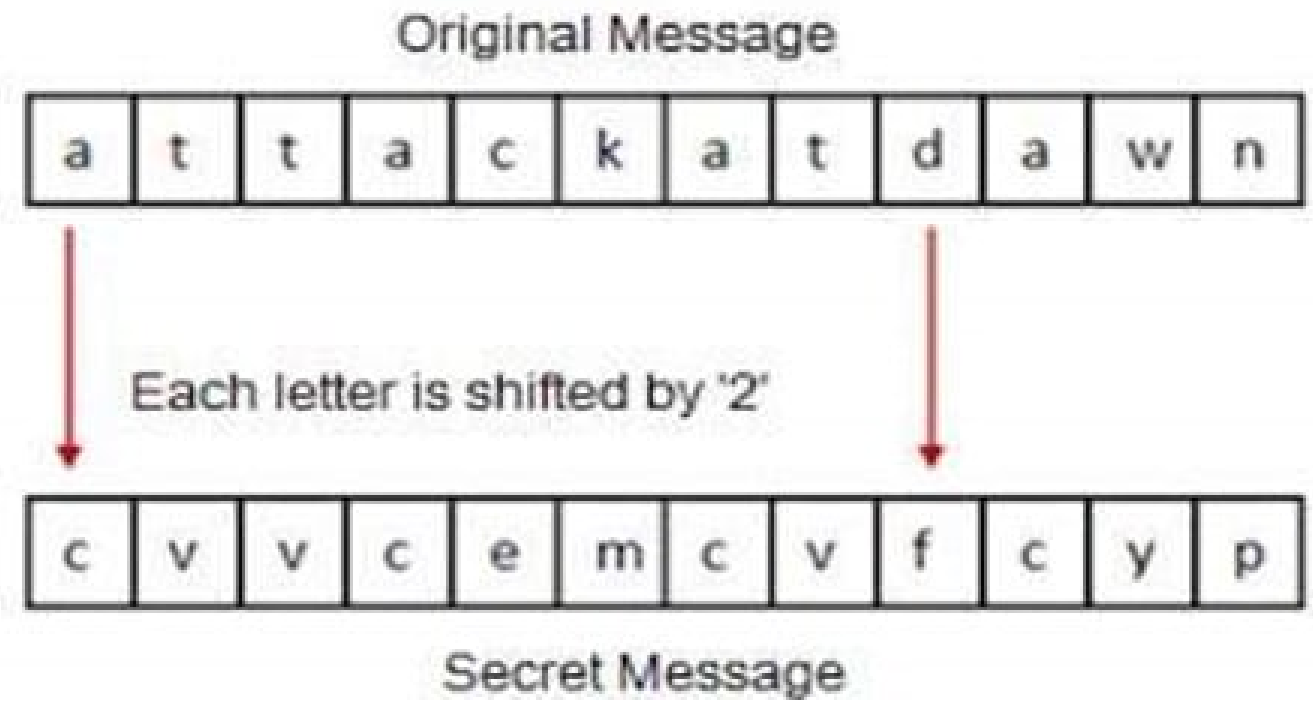
where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26 \quad \textbf{(2.2)}$$

```
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
```

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

- Shift cipher:key=2,3,4,5.....
- Shift cipher with key value=3 is called Caesar Cipher
- Example with key = 2



Caesar cipher-Pros & cons

- Pros
  1. Simple
  2. easy to implement
- Cons
  1. The encryption and decryption algorithms are known.
  2. There are only 25 keys to try(Vulnerable to Brute Force Attack).
  3. The language of the plaintext is known and easily recognizable

Brute Force Attack in Caesar Cipher

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 ydrcp rfc 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 hsjlq
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	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

Brute force attack

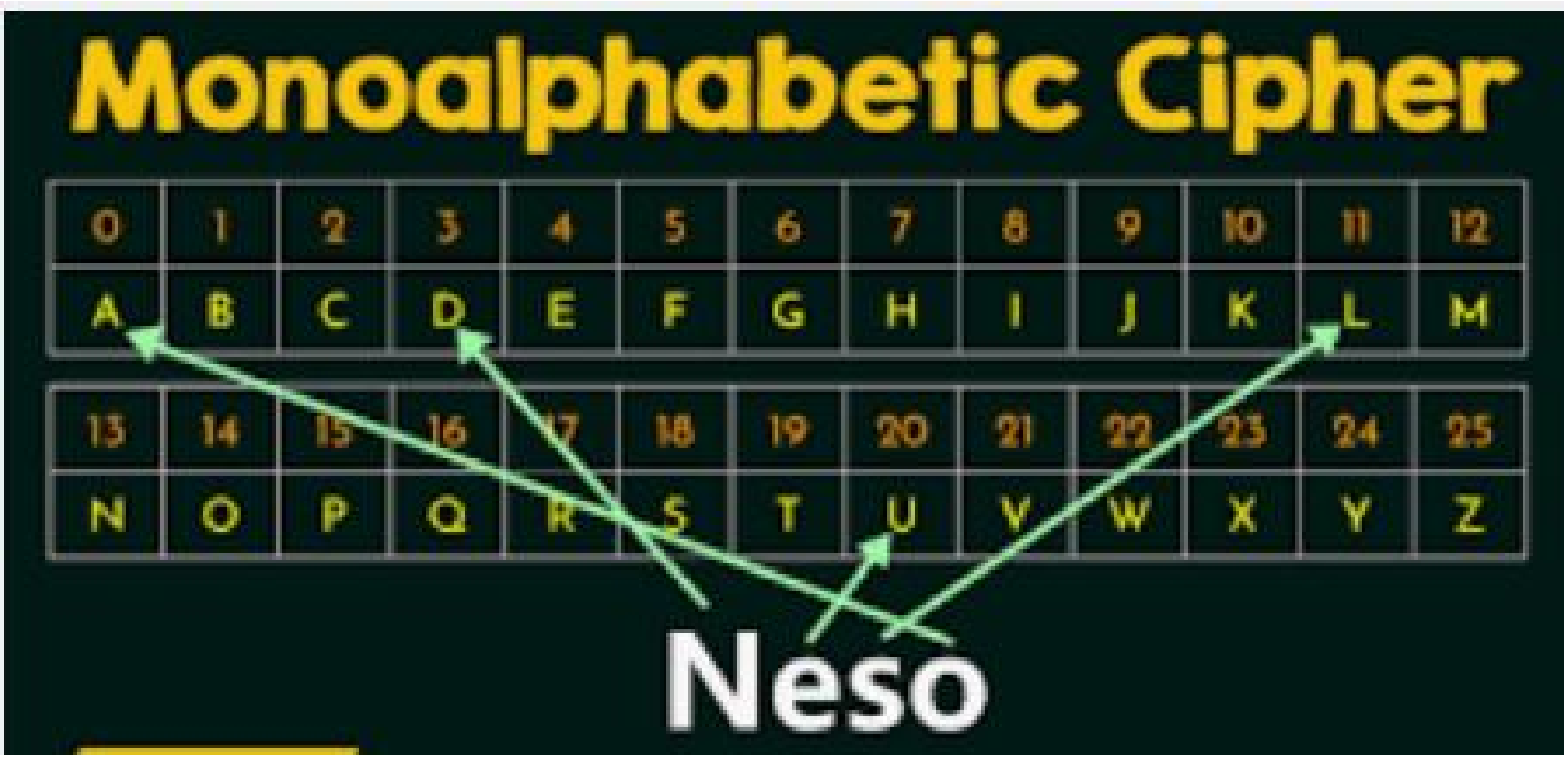
Ciphertext: SQDYMZK

Shifts	Back	Result
0	[26]	SQDYMZK
1	[25]	TREZNAL
2	[24]	USFAOBM
3	[23]	VTGBPCN
4	[22]	WUHCQDO
5	[21]	XVIDREP
6	[20]	YWJESFQ
7	[19]	ZXKFTGR
8	[18]	AYLGUHS
9	[17]	BZMHVIT
10	[16]	CANIWJU
11	[15]	DBOJXKV
12	[14]	ECPKYLW
13	[13]	FDQLZMX

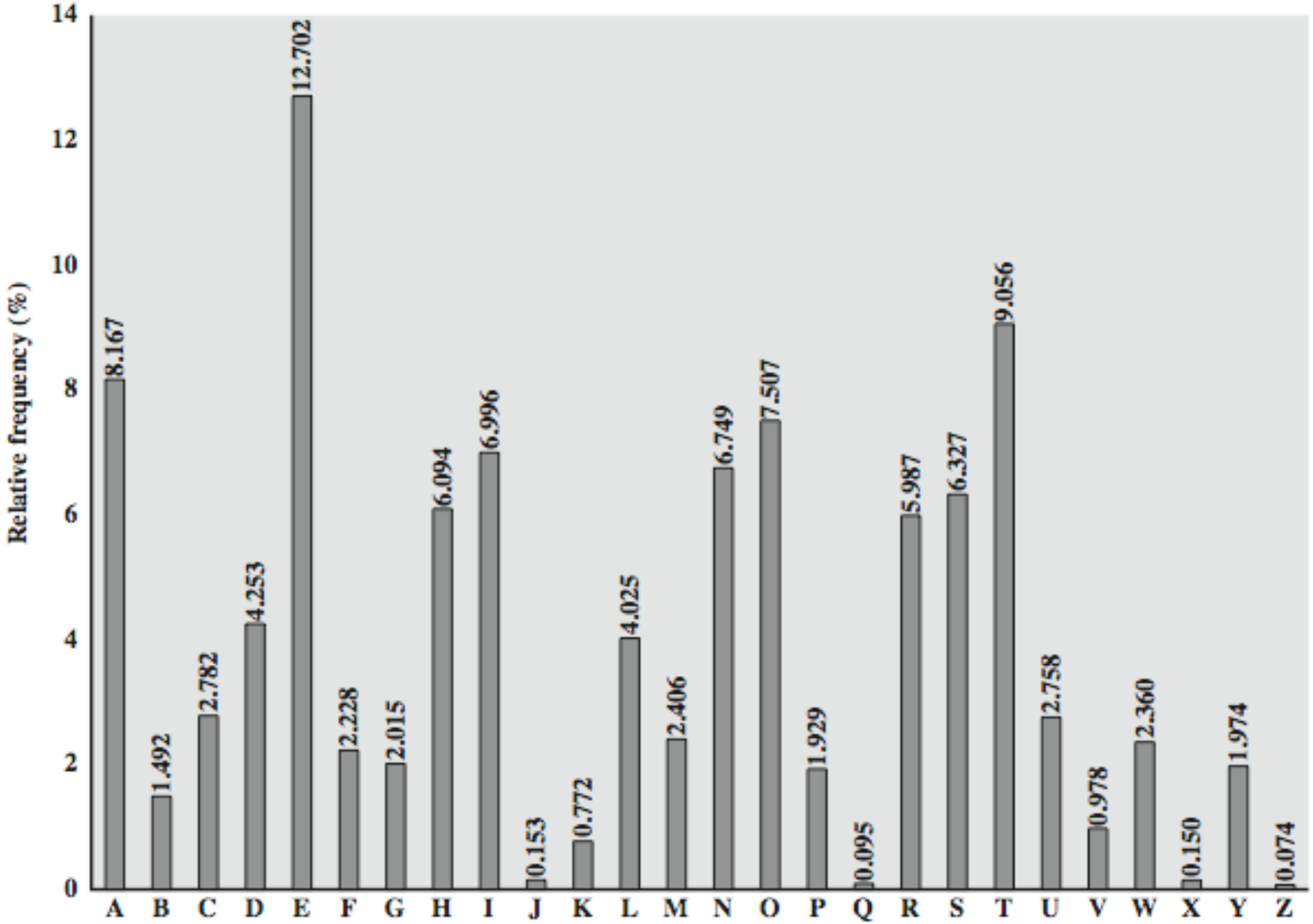
Shifts	Back	Result
13	[13]	FDQLZMX
14	[12]	GERMANY
15	[11]	HFSNBOZ
16	[10]	IGTOCPA
17	[9]	JHUPDQB
18	[8]	KIVQERC
19	[7]	LJWRFSD
20	[6]	MKXSGTE
21	[5]	NLYTHUF
22	[4]	OMZUIVG
23	[3]	PNAVJWH
24	[2]	QOBWKXI
25	[1]	RPCXLYJ

Monoalphabetic Cipher

- The cipher line can be any permutation of the 26 alphabetic characters
- A permutation of a finite set of elements 'S' is an ordered sequence of all the elements of S with each element appearing exactly once
- For example, if S=a,b,c , there are six permutations of : abc, acb, bac, bca, cab, cba
- Monoalphabetic cipher would seem to eliminate brute-force techniques for cryptanalysis
- A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message
- English Language-Nature of plain text is known


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

Relative frequency of English letters



Example

CT	G	Z	G	E	W	V	G	R	N	C	P
PT	E		E				E				
PT	E		E			T	E				
PT	E		E			T	E			A	
PT	E		E			T	E		L	A	N
PT	E		E			T	E	P	L	A	N
PT	E	X	E	C	U	T	E	P	L	A	N

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

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

```
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
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e   e e tat   e    the    t
```

Only four letters have been identified, but already we have quite a bit of the message. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. The complete plaintext, with spaces added between words, follows:

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

Monoalphabetic Cipher-Pros & Cons

- Pros
  1. Better security than Caesar cipher
- Cons
  1. Monoaphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
  2. countermeasure is to provide multiple substitutes, known as homophones, for a single letter

Playfair Cipher

- Manual symmetric encryption technique
- Multiple-letter encryption cipher
- It treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- 5 X 5 matrix constructed using a keyword(Ex: 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

Rules for encryption using palyfair cipher

1. Digrams
2. Repeating/Missing Letters-Filler Letter
3. Same column- wrap around
4. Same row- wrap around
5. Rectangle-swap

Example

Plaintext: attack

Digrams: at ta ck

Plaintext: academy

Digrams: ac ad em yx

Plaintext: balloon

Digrams: ba ll oo n

Digrams: ba lx lo on

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

Example 1: attack

Digrams: at ta ck

at	ta	ck
RS	SR	DE

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

Plaintext: attack

Digrams: RSSRDE

Example 2: mosque

mo	sq	ue
ON	TS	ML

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

Plaintext: mosque

Digrams: ONTSML

PT: instruments

in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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

Hill Cipher

- Multi letter cipher
- developed by Lester hill in 1929
- Encrypt a group of letters: digraph, trigraph or polygraph-depending on the key

Hill Cipher-Mathematical aspects

- linear algebra
- matrix arithmetic modulo 26
- Square matrix
- determinant
- multiplicative inverse

Hill Cipher-Algorithm

- $C = E(K,P) = P * K \bmod 26$
- $P = D(K,C) = C * K^{-1} \bmod 26 = P * K * K^{-1} \bmod 26$
  This can be expressed in terms of row vectors and matrices

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

Encryption

$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Question: Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

Key = 3 x 3 matrix.

PT = pay mor emo ney

Encrypting: pay

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (15\ 0\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (15\text{x}17+0\text{x}21+24\text{x}2 \quad 15\text{x}17+0\text{x}18+24\text{x}2 \quad 15\text{x}5+0\text{x}21+24\text{x}19) \bmod 26$$

$$= (303\ 303\ 531) \bmod 26$$

$$= (17\ 17\ 11)$$

$$= (R\ R\ L)$$

Encrypting: mor

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (12\ 14\ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (12\text{x}17+14\text{x}21+17\text{x}2 \quad 12\text{x}17+14\text{x}18+17\text{x}2 \quad 12\text{x}5+14\text{x}21+17\text{x}19) \bmod 26$$

$$= (532\ 490\ 677) \bmod 26$$

$$= (12\ 22\ 1)$$

$$= (M\ W\ B)$$

Encrypting: emo

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (4\ 12\ 14) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (4\text{x}17+12\text{x}21+14\text{x}2 \quad 4\text{x}17+12\text{x}18+14\text{x}2 \quad 4\text{x}5+12\text{x}21+14\text{x}19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (10\ 0\ 18)$$

$$= (K\ A\ S)$$

Encrypting: ney

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (13\ 4\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (13\text{x}17+4\text{x}21+24\text{x}2 \quad 13\text{x}17+4\text{x}18+24\text{x}2 \quad 13\text{x}5+4\text{x}21+24\text{x}19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (15\ 3\ 7)$$

$$= (P\ D\ H)$$

PT	p	a	y	m	o	r	e	m	o	n	e	y
CT	R	R	L	M	W	B	K	A	S	P	D	H

Polyalphabetic Cipher-Vigenere Cipher

- To improve on the mono alphabetic technique
- A set of related mono alphabetic substitution rules is used
- A key determines which particular rule is chosen for a given transformation
- Example:Vigenere Cipher
- 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
- To encrypt a message, a key is needed that is as long as the message.
- Usually, the key is a repeating keyword.

Vigenere Cipher

We can express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters $P = p_0, p_1, p_2, \ldots, p_{n-1}$ and a key consisting of the sequence of letters $K = k_0, k_1, k_2, \ldots, k_{m-1}$, where typically $m < n$. The sequence of ciphertext letters $C = C_0, C_1, C_2, \ldots, C_{n-1}$ is calculated as follows:

$$\begin{aligned} C = C_0, C_1, C_2, \ldots, C_{n-1} &= \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})] \\ &= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26, \\ &\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots \end{aligned}$$

Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first m letters of the plaintext. For the next m letters of the plaintext, the key letters are repeated. This process continues until all of the plaintext sequence is encrypted. A general equation of the encryption process is

$$C_i = (p_i + k_{i \bmod m}) \bmod 26 \qquad \textbf{(2.3)}$$

$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

- KEY : deceptive
- Plain Text: “we are discovered save yourself”

```
key:            deceptivedeceptivedeceptive
plaintext:      wearediscoveredsaveyourself
ciphertext:     ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenere Cipher-Cryptanalysis

- As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.
- Determining the length of the keyword
- Key and the Plaintext share the same frequency distribution of letters, a statistical technique can be applied
- **Autokey System:** The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself.
- Vigenère proposed what is referred to as an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key.

```
key:          deceptivewearediscoveredsav
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Polyalphabetic Cipher-Vernam Cipher

- Need of ultimate defense against such a cryptanalysis
- Introduced by Gilbert Vernam in 1918.
- This system works on binary data (bits) rather than letters
- Length of Keyword=Length of Plaintext
- no statistical relationship to it.
- This system can be expressed as follows:

$$c_i = p_i \oplus k_i$$

where

p_i = ith binary digit of plaintext
k_i = ith binary digit of key
c_i = ith binary digit of ciphertext
$\oplus$ = exclusive-or (XOR) operation

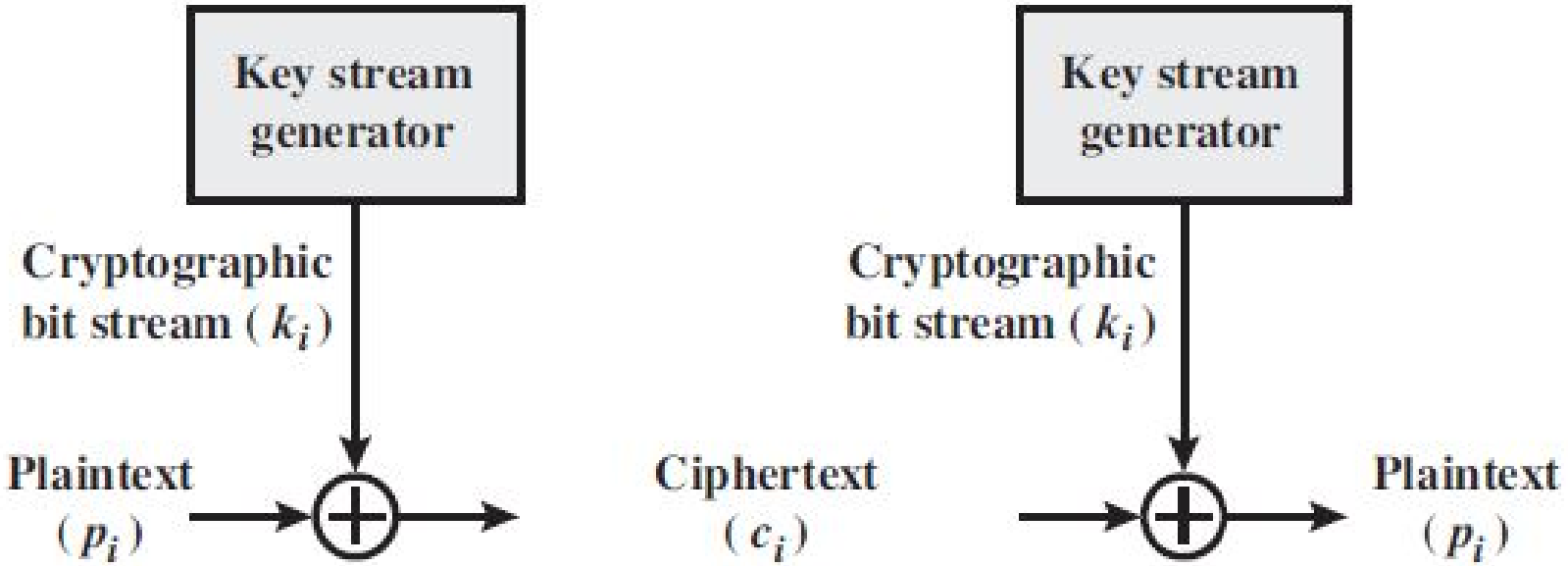


Figure 2.7 Vernam Cipher

Vernam Cipher-Cryptanalysis

- Construction of the key
- Vernam proposed the use of a running loop of tape that eventually repeated the key
- The system worked with a very long but repeating keyword.
- It can be broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.

One-Time Pad

- Improvement to the vernam Cipher
- Yield ultimate aim in security
- Random key that is as long as the message
- The key need not be repeated
- In addition the key is to be 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
- Such a scheme, known as a one-time pad, is unbreakable
- It produces random output
- 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
- The security of the one time pad is entirely due to the randomness of the key

Example

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall
```

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        mfugpmiydgaxgoufhkllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

Two fundamental difficulties

- Making large quantities of random keys
- Key distribution and protection
- Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security
- The one-time pad is the only cryptosystem that exhibits what is referred to as perfect secrecy

Transposition Cipher

- some sort of permutation on the plaintext letters
- 2 methods
  1. Rail fence method
  2. Row Column Transposition

Rail Fence Technique

- The simplest method
- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example, to encipher the message "**meet me after the toga party**" with a rail fence of **depth 2**

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

Row Column Transposition

- More complex
- Rectangle
- Write: Row by row
- Read: Column by column
- Key: Order of the column
- PT: 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
```

- To encrypt, start with the column that is labeled 1, in this case column 3.
- Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.