Cryptography and Information Security Overview

Dr Shadi Masadeh
Isra University

2016-2017

Roadmap

- Cryptographic algorithms
  - symmetric ciphers
  - asymmetric encryption
  - hash functions
- Mutual Trust
- Network Security
- Computer Security

Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

Chapter 1 – Introduction

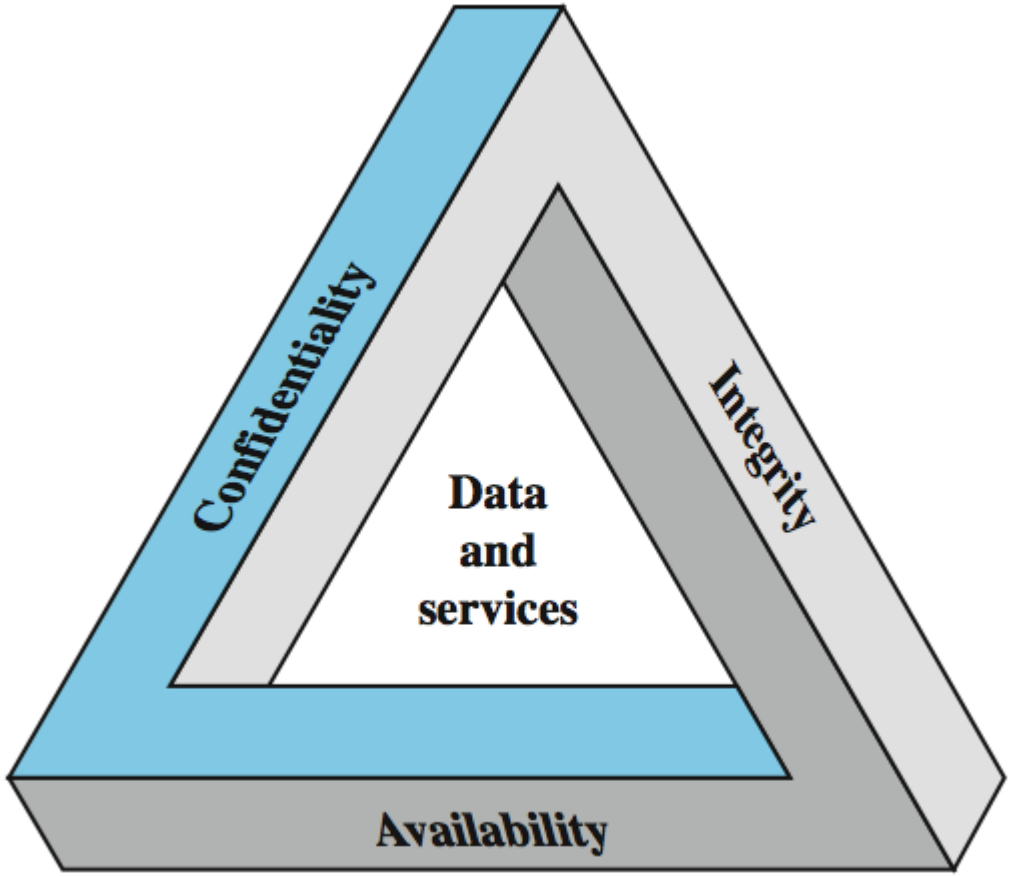
- *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure..*

  — On War, Carl Von Clausewitz

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



Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Examples of Security Requirements

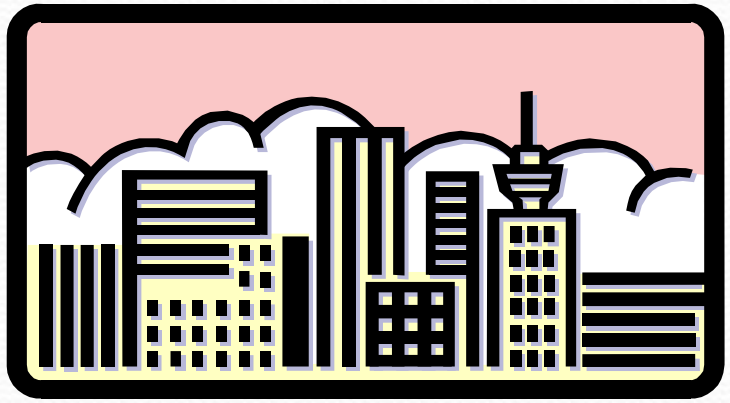
- confidentiality – student grades
- integrity – patient information
- availability – authentication service

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

OSI Security Architecture

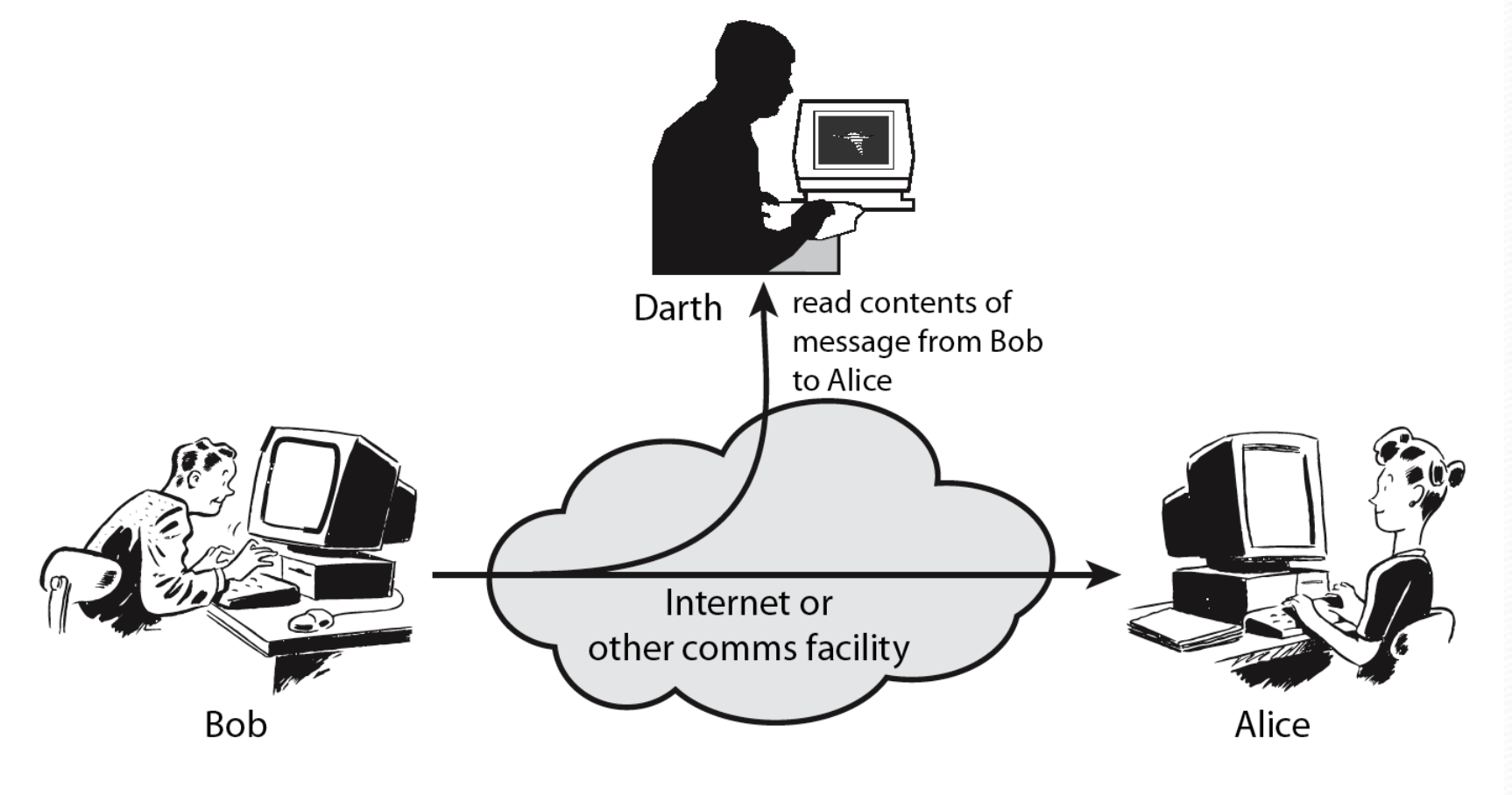
- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study



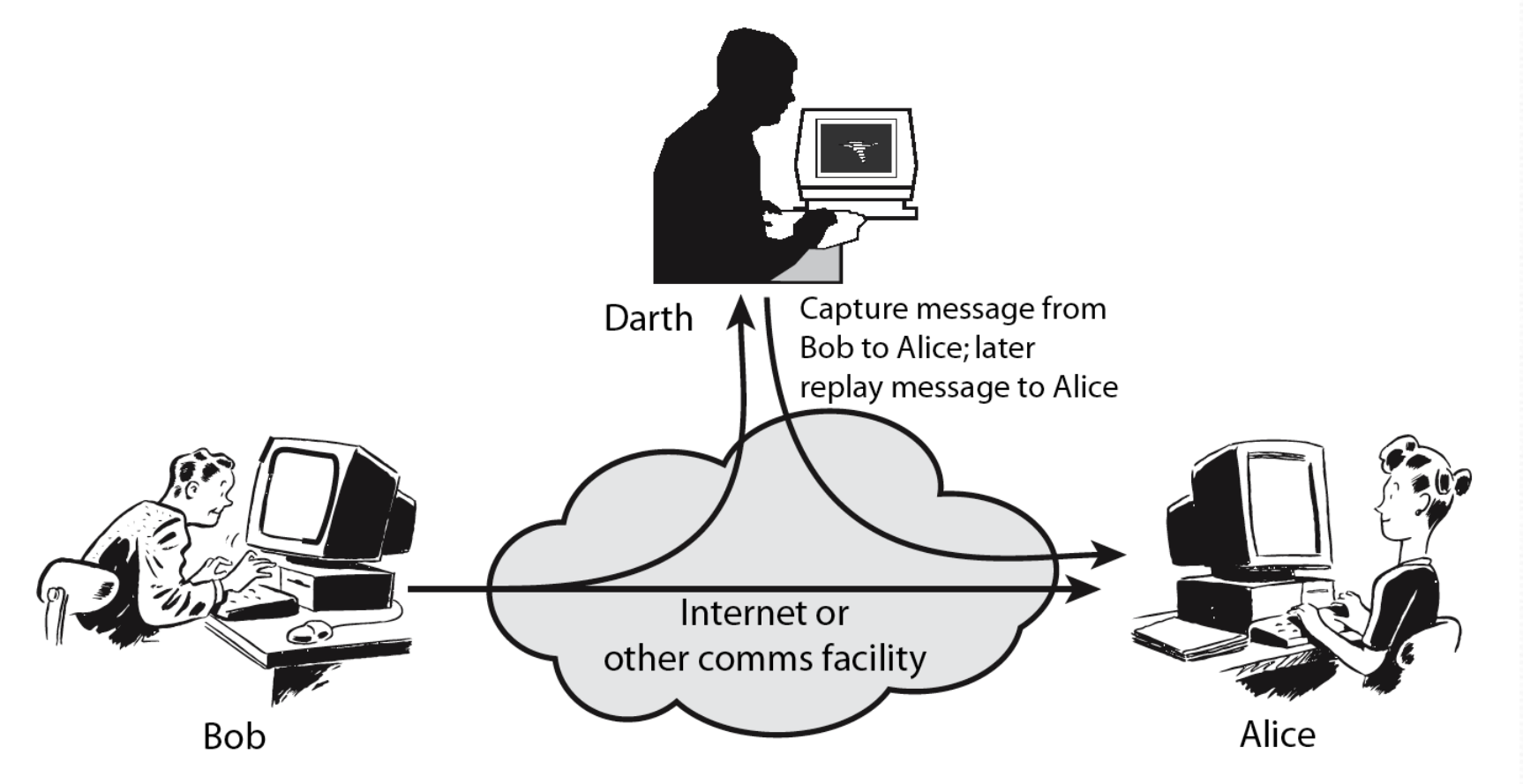
Aspects of Security

- 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



Active Attacks



Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:

  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828:

  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

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

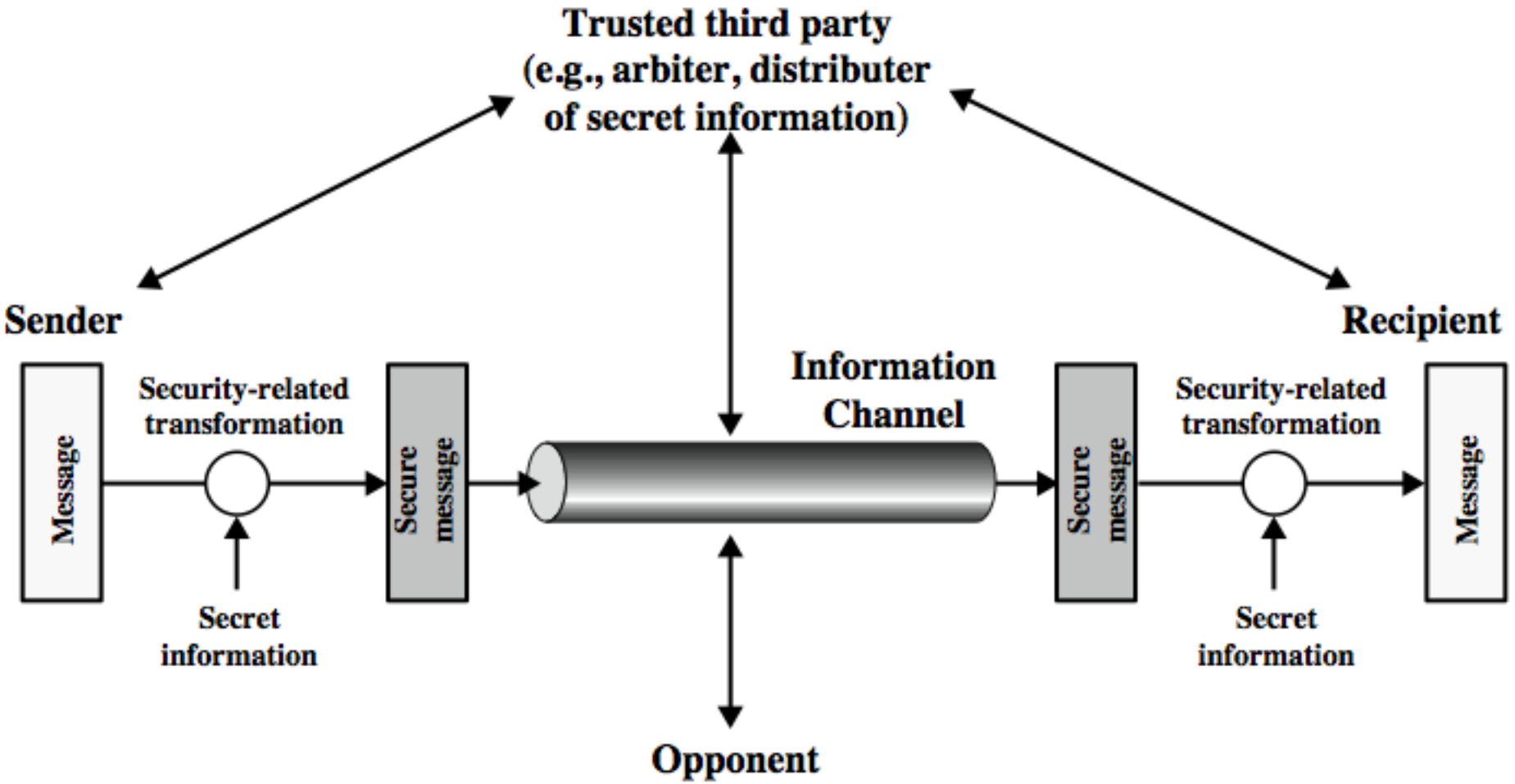
Security Mechanism

- 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**
- hence our focus on this topic

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

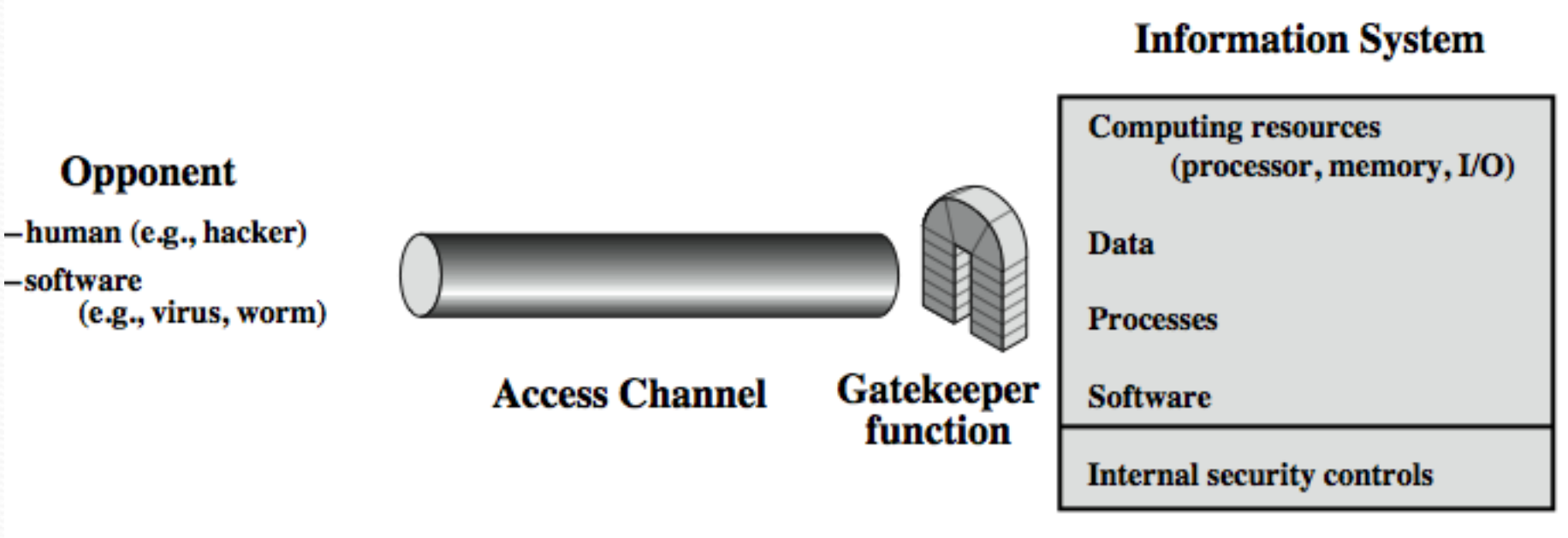
Model for Network Security



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

Summary

- topic roadmap & standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security

Dr. Shadi Masadeh and Dr.Hasan Kanaker

Cryptography

characterize cryptographic system by:

- type of encryption operations used
  - substitution / transposition / product
- number of keys used
  - single-key or private / two-key or public
- way in which plaintext is processed
  - block / stream

Cryptographic systems can be characterized along these three independent dimensions

Classical Substitution Ciphers

- Substitution
  Where letters of plaintext are replaced by other letters, or numbers, or symbols

- Transposition
  The plaintext is encrypted by changing the positions of the letters and/or symbols, by some sort of permutation

Classical Substitution Ciphers

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

Note

- In this section and the next, we examine a sampling of what might be called classical encryption techniques.
- A study of these techniques enables us to illustrate the basic approaches to symmetric encryption used today and the types of cryptanalytic attacks that must be anticipated.
- The two basic building blocks of all encryption technique are substitution and transposition.

substitution techniques

Caesar Cipher

- The algorithm can be expressed as follows. For each plaintext letter , substitute the ciphertext letter

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

- 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

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

Caesar Cipher

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
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

Encrypt the message P="Hello" using Caesar Cipher, given the key K=3.

Caesar Cipher

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
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

Encrypt the message P="Hello" using Caesar Cipher, given the key K=3.
C = (P + K) mod 26
C = 7 + 3 = 10 = K
4 + 3 = 7 = H
11 + 3 = O
= O
14 + 3 = 17 = R

C = "KHOOR"

Caesar Cipher

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
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

Decrypt the Cipher text C="KHOOR" using Caesar Cipher, given the key K=3.

M = (P-K) mod 26
10 - 3 = 7 = H
E
L

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- 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
- eg. break ciphertext "GCUA VQ DTGCM"

substitution techniques

Monoalphabetic Ciphers

- Caesar cipher is far from secure. WHY?
- Similar to Caesar cipher but the replacement is random.
- The key is changed for every message.
- This will increase the possibilities to 26!.
- Brute-force will not work.
- Is it secure?

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key 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

Monoalphabetic Cipher

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

Encrypt the message = "iteam" using Monoalphabetic Cipher given the key above.

M = iteam
C = RMWEA

Monoalphabetic Cipher

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

Encrypt the message = "iteam" using Monoalphabetic Cipher given the key above.

C = RMWEA
M = iteam

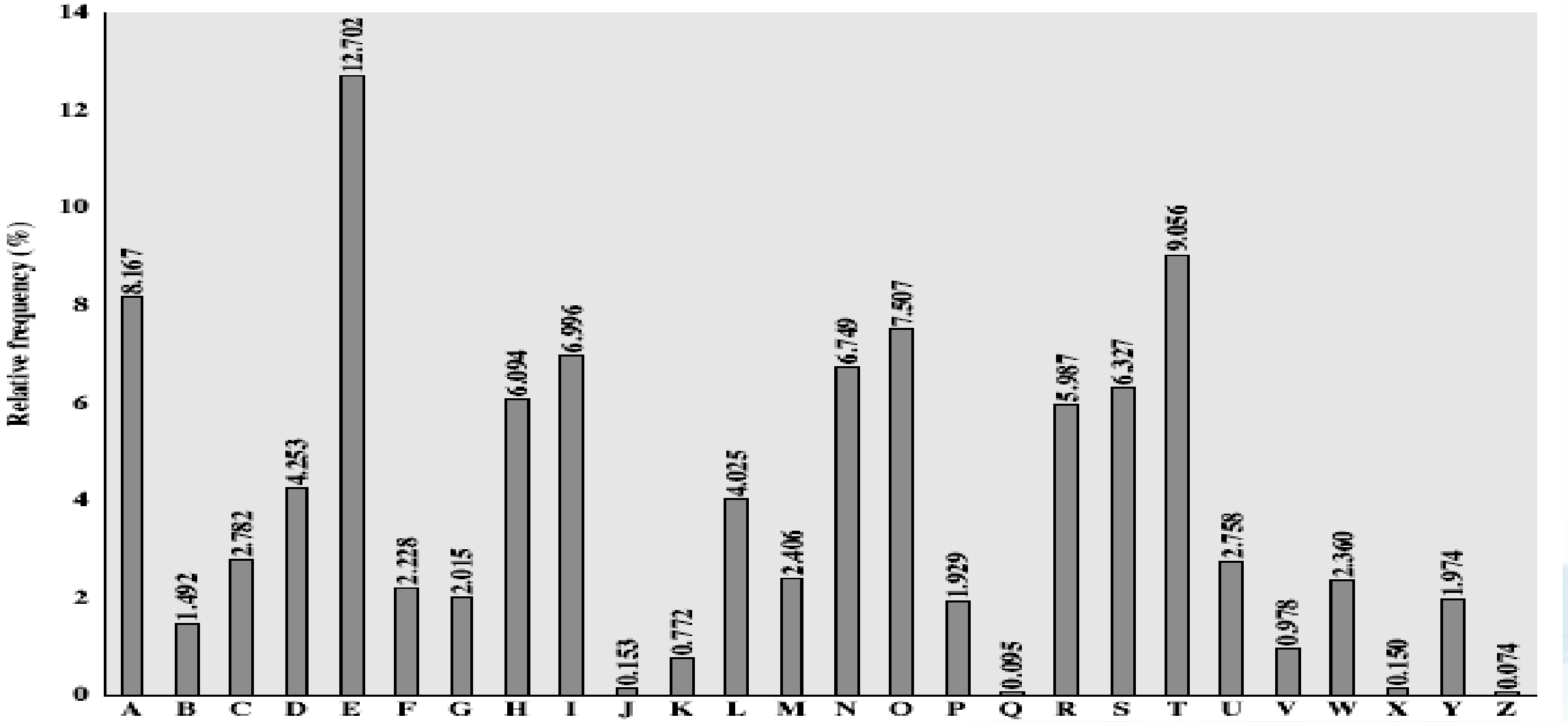
Monoalphabetic Cipher Security

- now have a total of $26! = 4 \times 10^{26}$ keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Language Redundancy and Cryptanalysis

- human languages are **redundant**
- E.g. "th ed s sh ph sh ll "
- letters are not equally commonly used
- In English E is by far the most common letter
  - followed by T,A,O,I,H, ..
- Other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html

Playfair Cipher

- not even the large number of keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- 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

Encrypting and Decrypting

- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

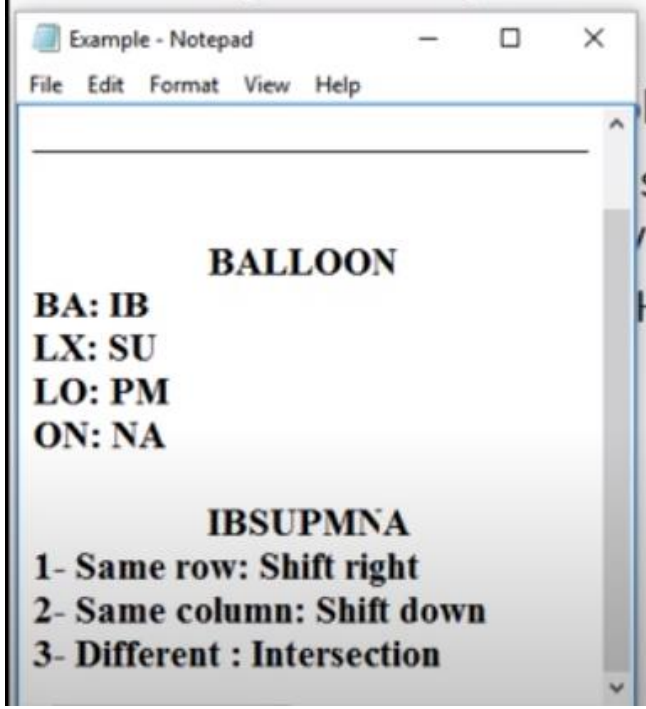
Playfair Cipher

Playfair Cipher

- The best-known multiple-letter encryption cipher
- The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.
- The keyword MONARCHY will produce the following matrix

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



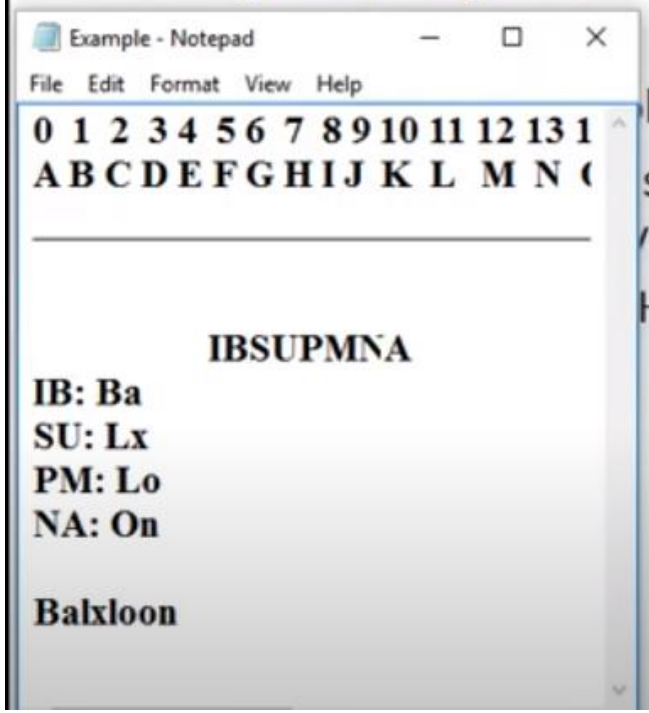
le-letter encryption cipher

s based on the use of a 5 × 5 matrix of letters
word.

HY will produce the following matrix

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



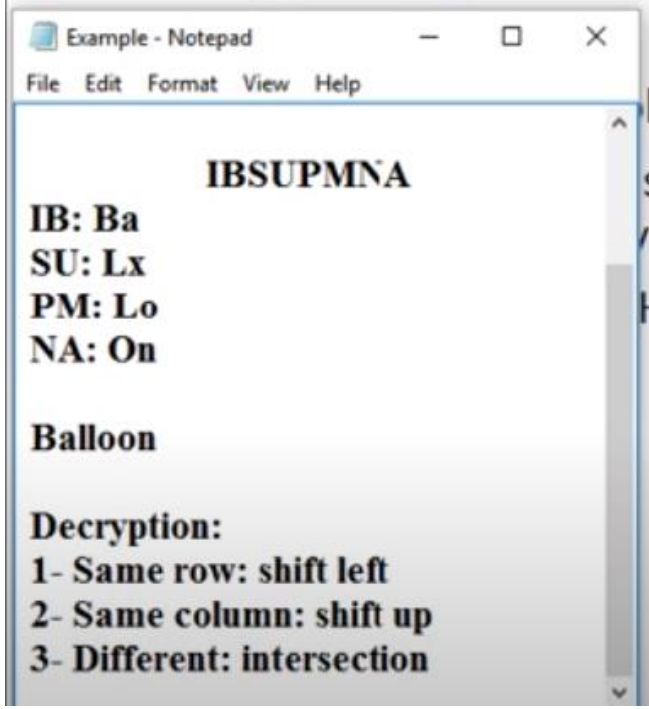
le-letter encryption cipher

s based on the use of a 5 × 5 matrix of letters
word.

HY will produce the following matrix

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



le-letter encryption cipher

s based on the use of a 5 × 5 matrix of letters
word.

HY will produce the following matrix

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

Security of Playfair Cipher

- security much improved over monoalphabetic
- since have 26 x 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. by US & British military in WW1
- it **can** be broken, given a few hundred letters
- since still has much of plaintext structure

Dr.Shadi Masadeh and Dr.Hasan Kanaker

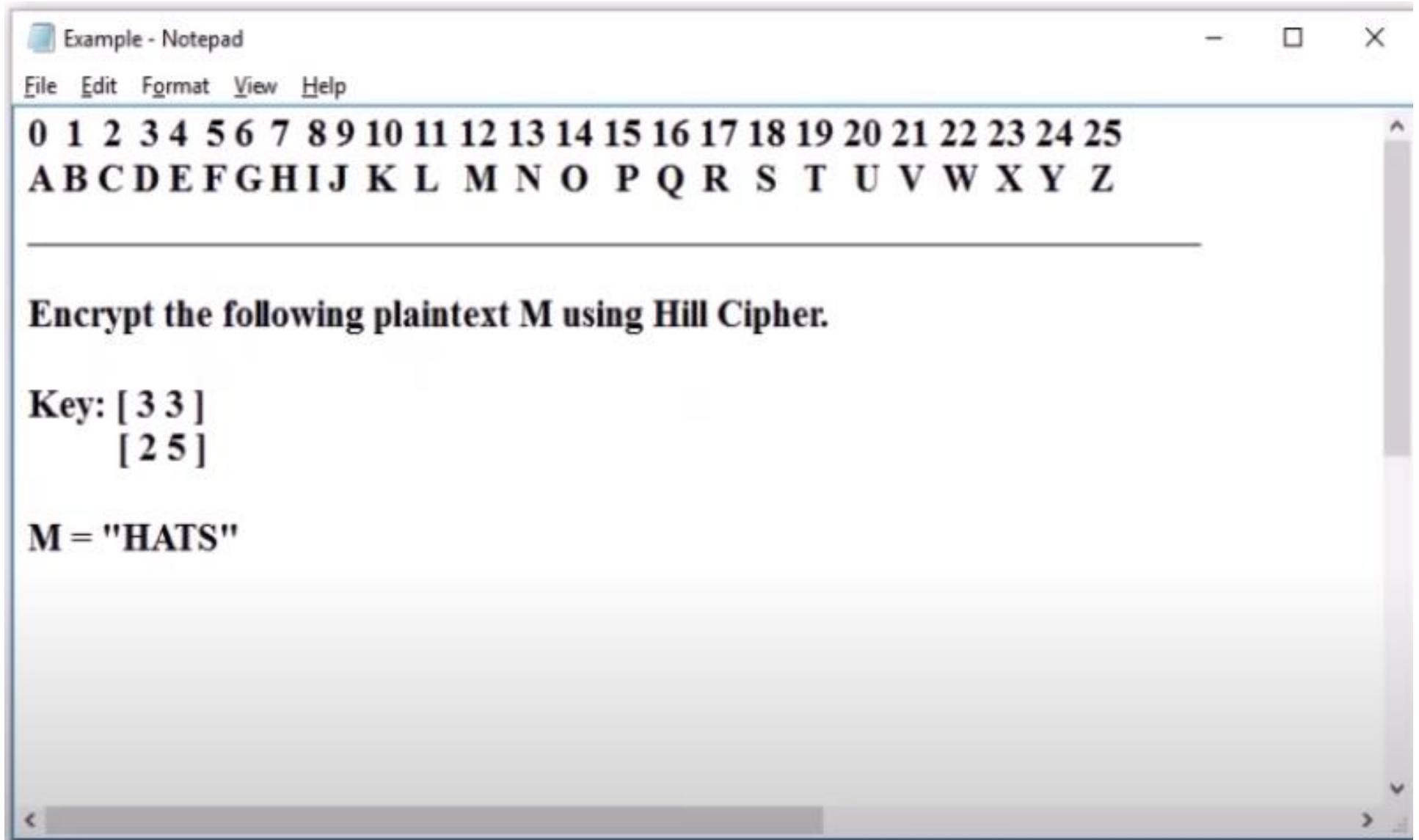
Hill Cipher

Hill cipher

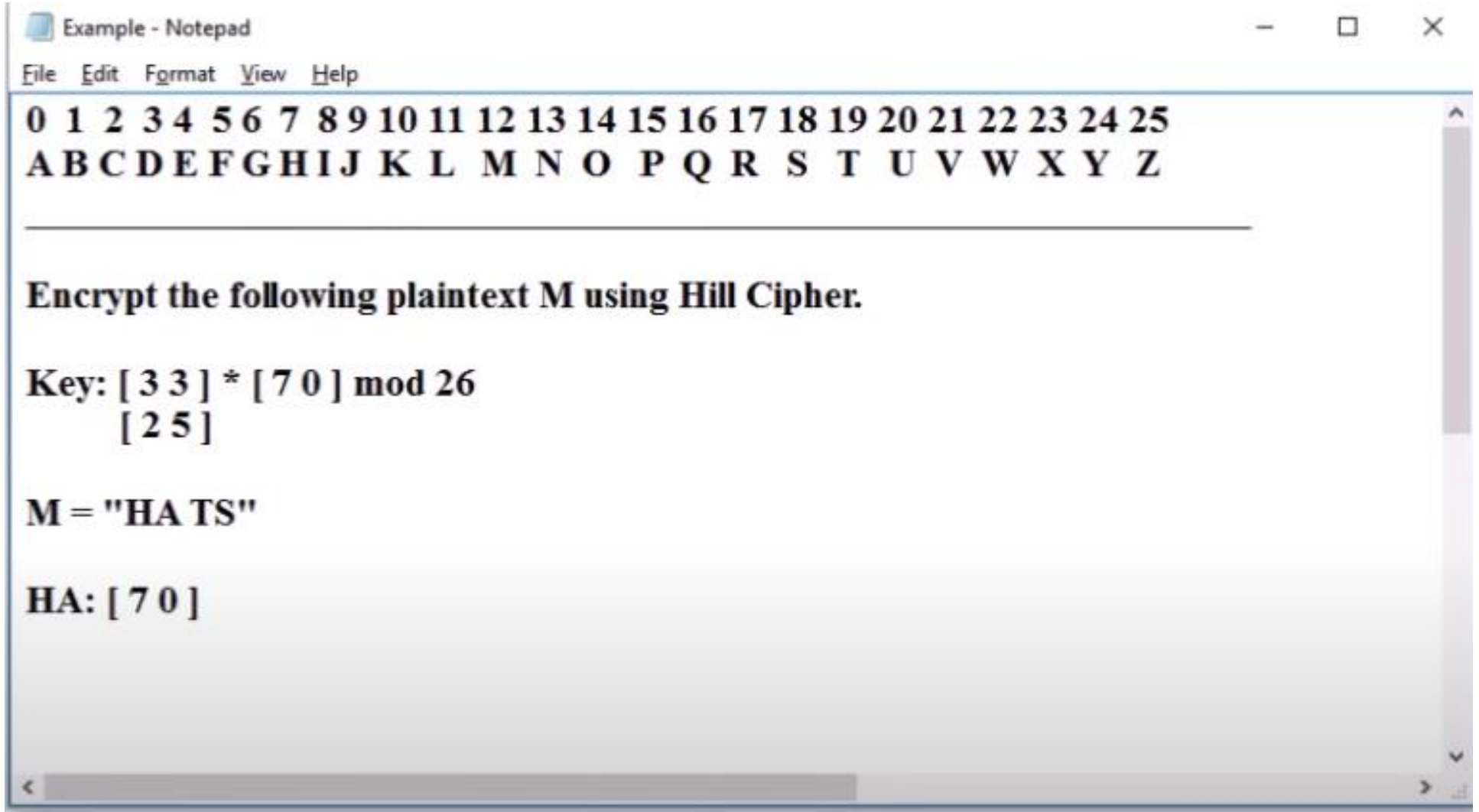
- This encryption algorithm takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters
- The substitution is determined by linear equations in which each character is assigned a numerical value (a=0, b=1,... z=25)
- Example

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

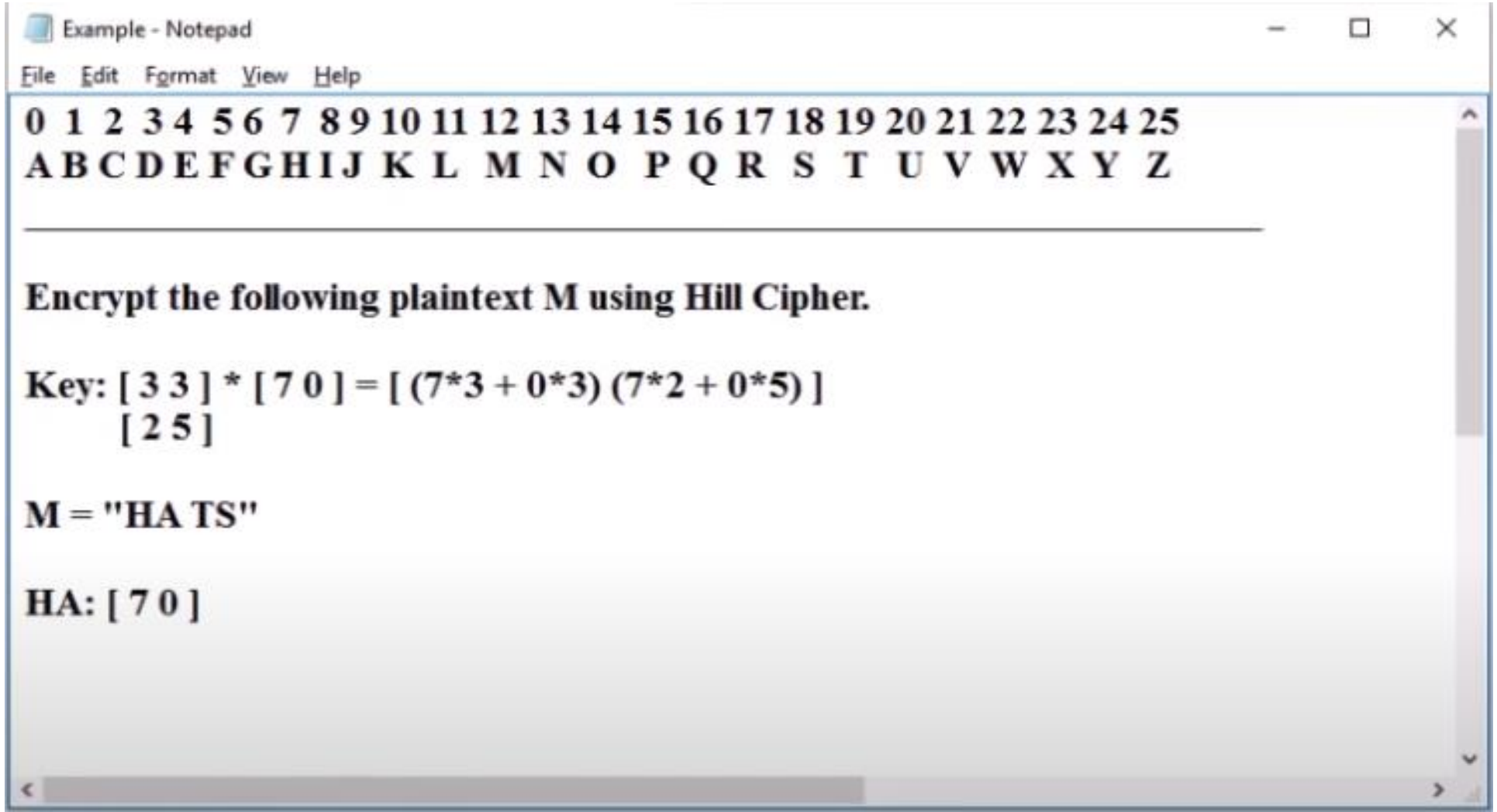
Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Encrypt the following plaintext M using Hill Cipher.
Key: [3 3]
[2 5]
M = "HATS"

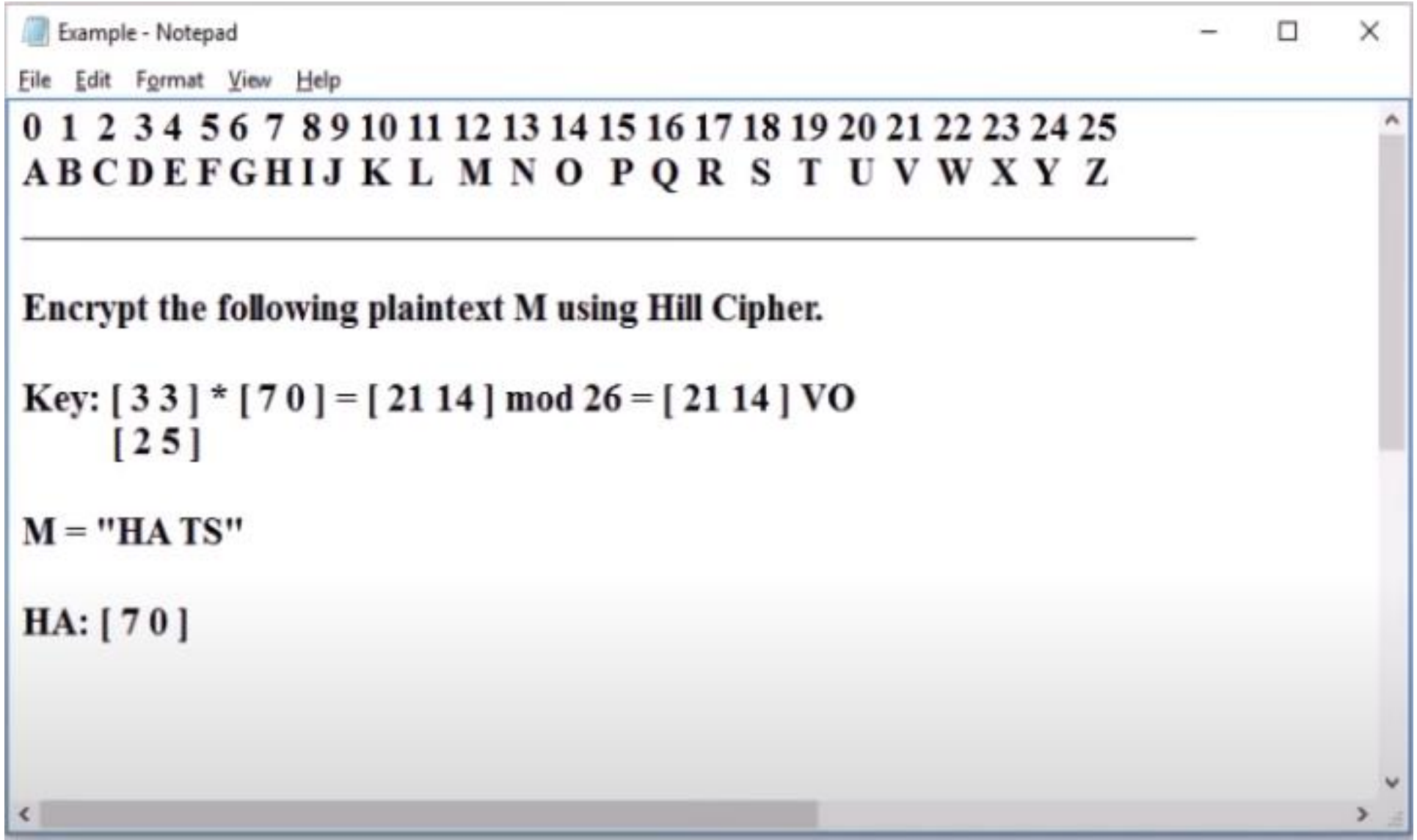
Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Encrypt the following plaintext M using Hill Cipher.
Key: [3 3] * [7 0] mod 26
[2 5]
M = "HA TS"
HA: [7 0]

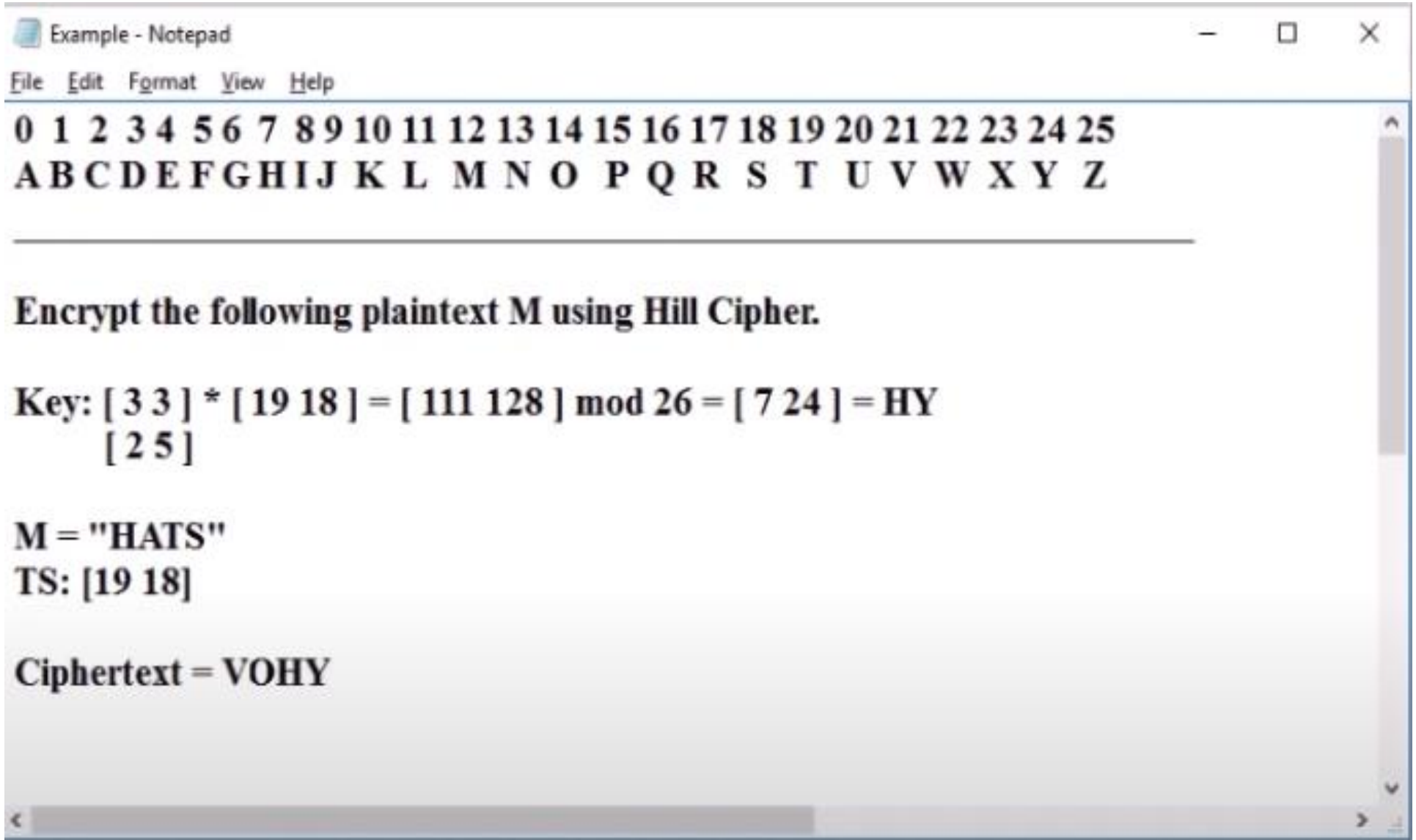
Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Encrypt the following plaintext M using Hill Cipher.
Key: [3 3] * [7 0] = [(7*3 + 0*3) (7*2 + 0*5)]
[2 5]
M = "HA TS"
HA: [7 0]

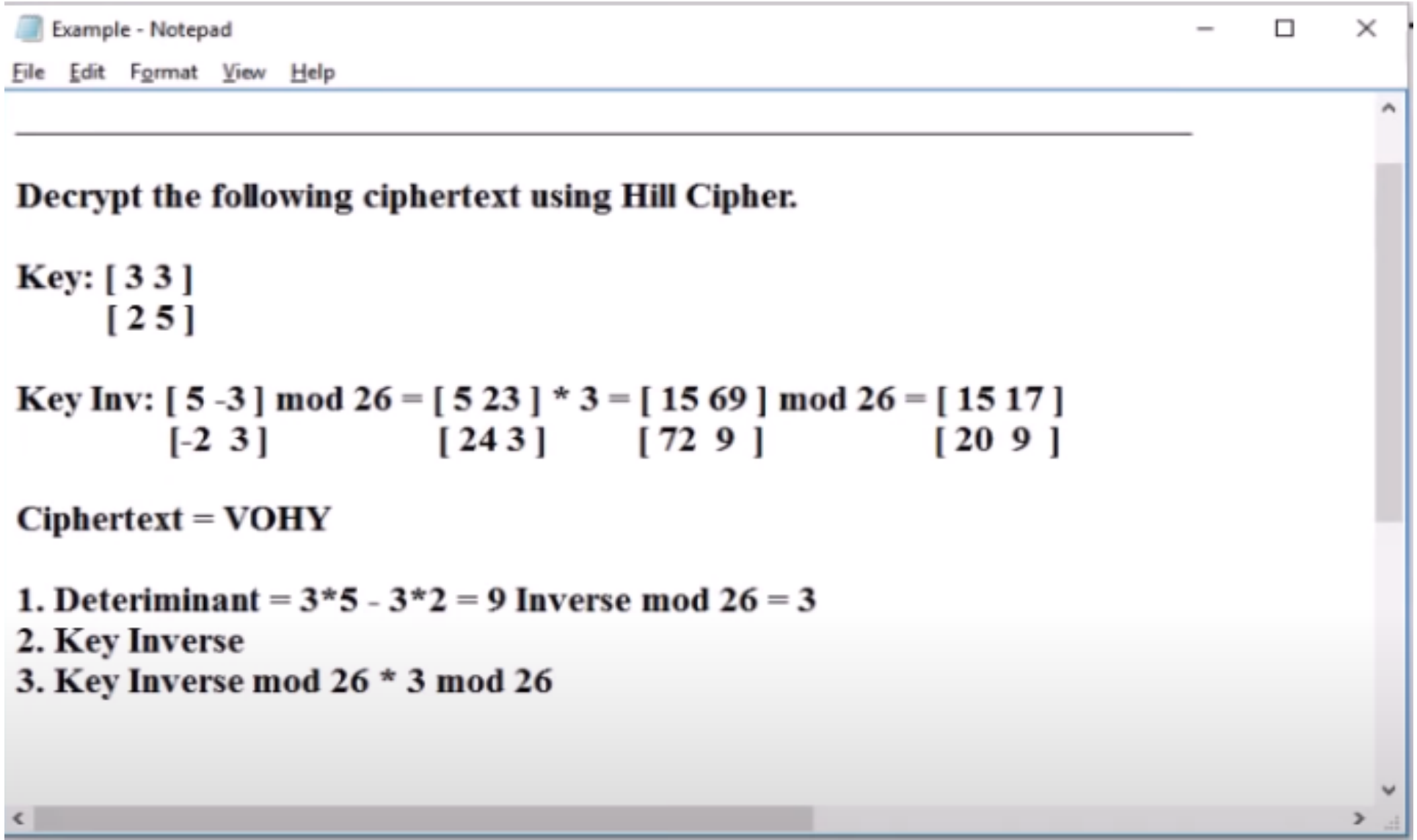
Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Encrypt the following plaintext M using Hill Cipher.
Key: [3 3] * [7 0] = [21 14] mod 26 = [21 14] VO
[2 5]
M = "HA TS"
HA: [7 0]

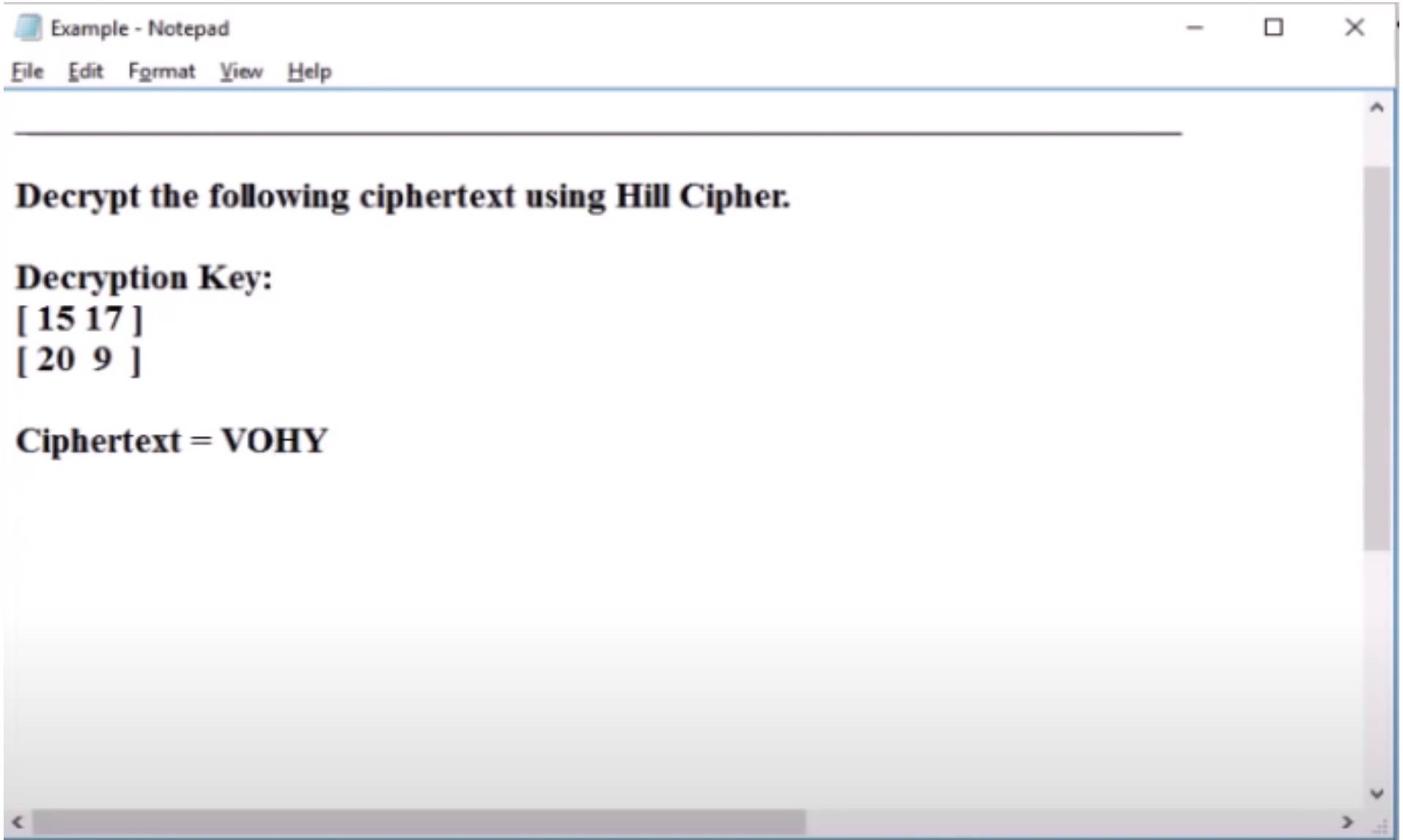
Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Encrypt the following plaintext M using Hill Cipher.
Key: [3 3] * [19 18] = [111 128] mod 26 = [7 24] = HY
[2 5]
M = "HATS"
TS: [19 18]
Ciphertext = VOHY

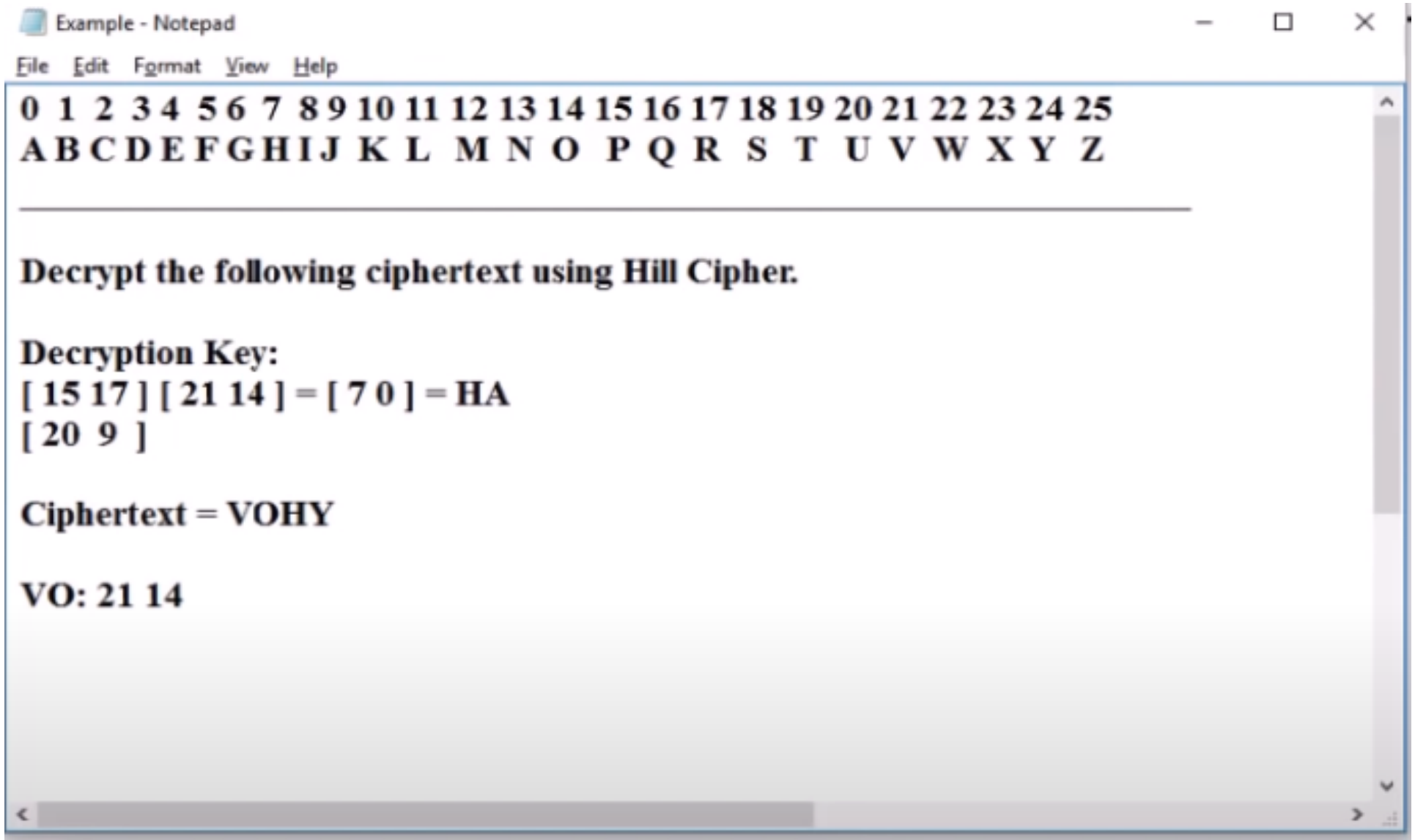
Hill Cipher


Example - Notepad
File Edit Format View Help
Decrypt the following ciphertext using Hill Cipher.
Key: [3 3]
[2 5]
Key Inv: [5 -3] mod 26 = [5 23] * 3 = [15 69] mod 26 = [15 17]
[-2 3] [24 3] [72 9] [20 9]
Ciphertext = VOHY
1. Deteriminant = 3*5 - 3*2 = 9 Inverse mod 26 = 3
2. Key Inverse
3. Key Inverse mod 26 * 3 mod 26

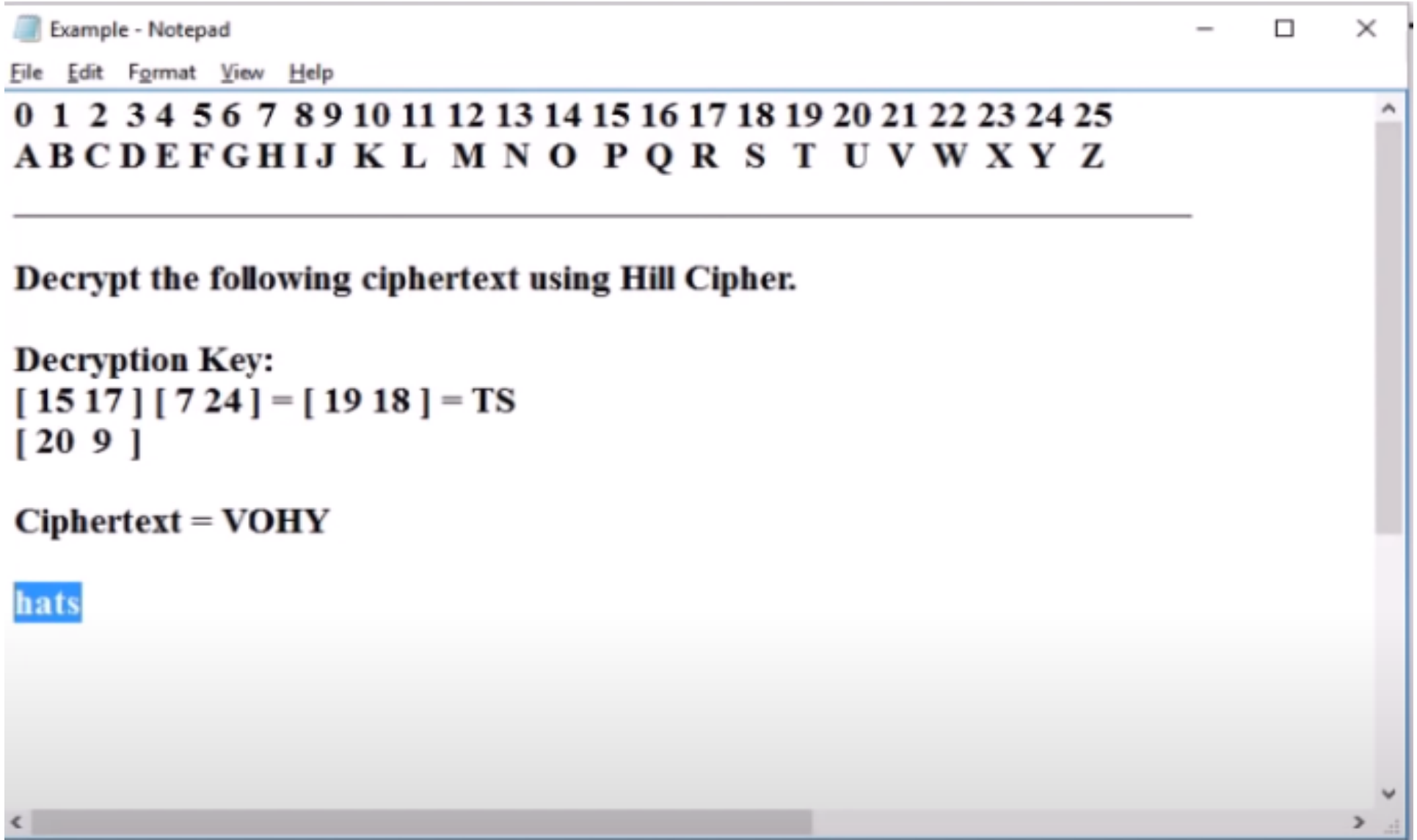
Hill Cipher


Example - Notepad
File Edit Format View Help
Decrypt the following ciphertext using Hill Cipher.
Decryption Key:
[15 17]
[20 9]
Ciphertext = VOHY

Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Decrypt the following ciphertext using Hill Cipher.
Decryption Key:
[15 17] [21 14] = [7 0] = HA
[20 9]
Ciphertext = VOHY
VO: 21 14

Hill Cipher


Example - Notepad
File Edit Format View Help
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
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
Decrypt the following ciphertext using Hill Cipher.
Decryption Key:
[15 17] [7 24] = [19 18] = TS
[20 9]
Ciphertext = VOHY
hats

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
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- have problem of safe distribution of key

One-time Pad: Encryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

Transposition Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text

Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message out as:

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

- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

Rail Fence cipher

Rail fence Technique

- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- Consider M = “meet me after the toga party”

  with a rail fence of depth 2, we 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

Rail Fence cipher

Consider M = “meet me after the party”
with a rail fence of depth = 2, encrypt using Rail fence:

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

C = MEMATRHPRYETEFETEAT

Rail Fence cipher

Consider M = "meet me after the party"
with a rail fence of depth = 2, encrypt using Rail fence:

C = MEMATRHPRY ETEFETEAT

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

M = meet me after the party

Row Transposition Ciphers

- 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.

```
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
```

Row Transposition Ciphers

Plaintext: attack postponed untill two am
Key: 4312567

4 3 1 2 5 6 7
a t t a c k p
o s t p o n e
d u n t i l l
t w o a m

C = TTNOAPTATSUWAODTCOIMKNLPEL

Row Transposition Ciphers

Key: 4312567 -> 7
C = TTNOAPTA TSUW AODT COIM KNL PEL -> 26

4 3 1 2 5 6 7
A T T A C K P
O S T P O N E
D U N T I L L
T W O A M

M = Attack Postponed Untill Two AM

Row Transposition Ciphers

Key: iTeam
C = TTNOAPTA TSUW AODT COIM KNL PEL -> 26

ITEAM
3521 4

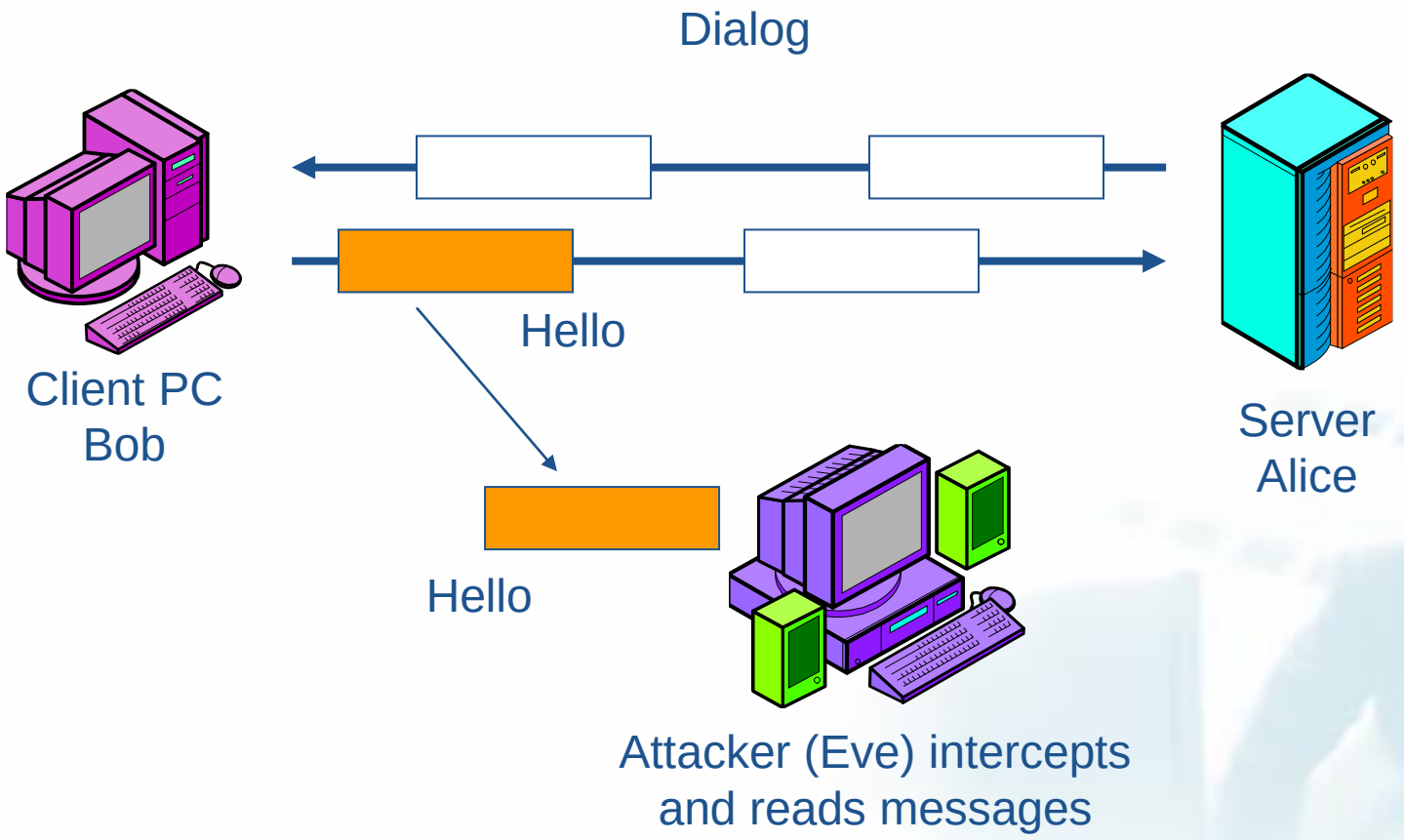
4312 5 67
ATTAC KP
OSTPO NE
DUNTI LL
TWOAM

Threats and Vulnerabilities

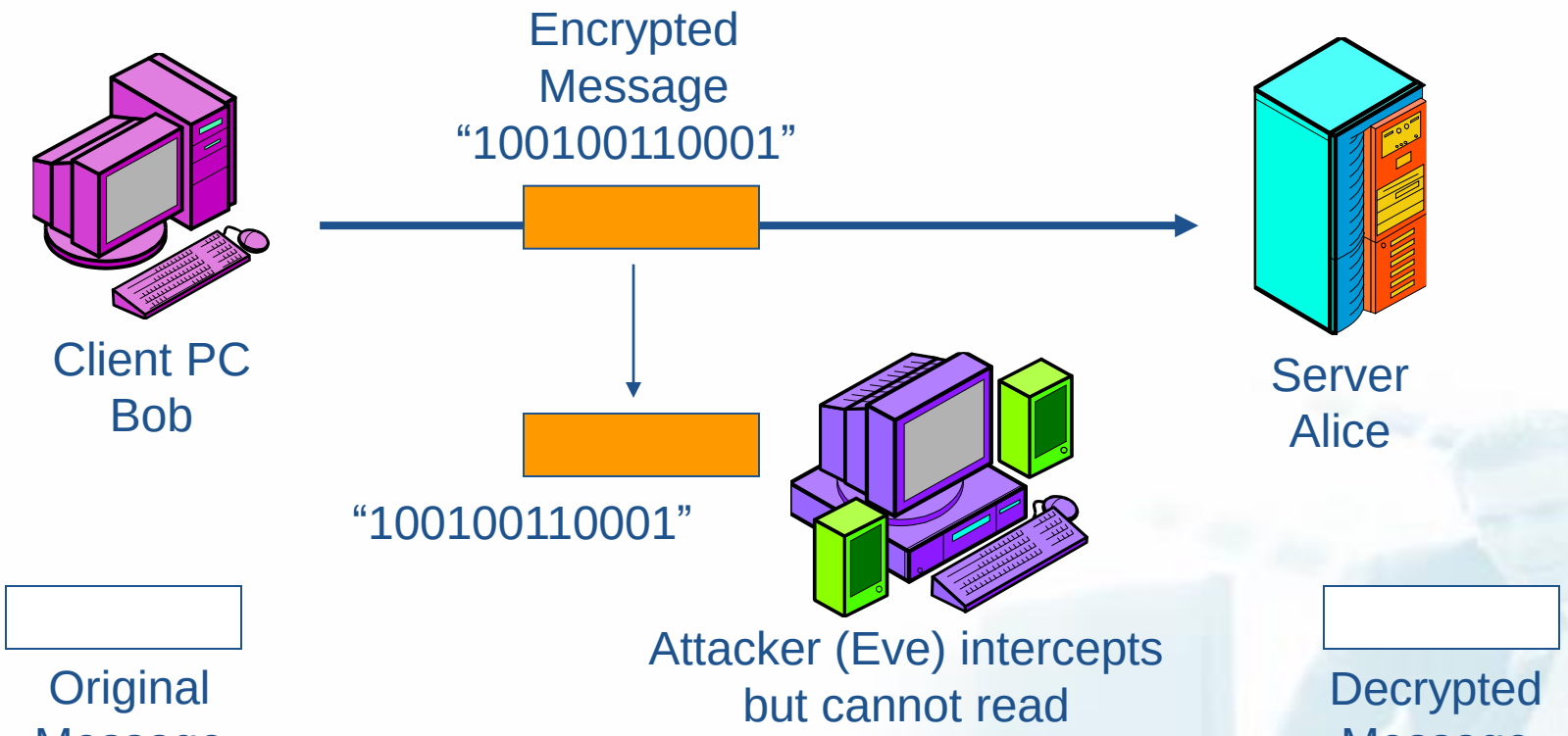
By Dr. Dr. Shadi Masadeh

Company
LOGO

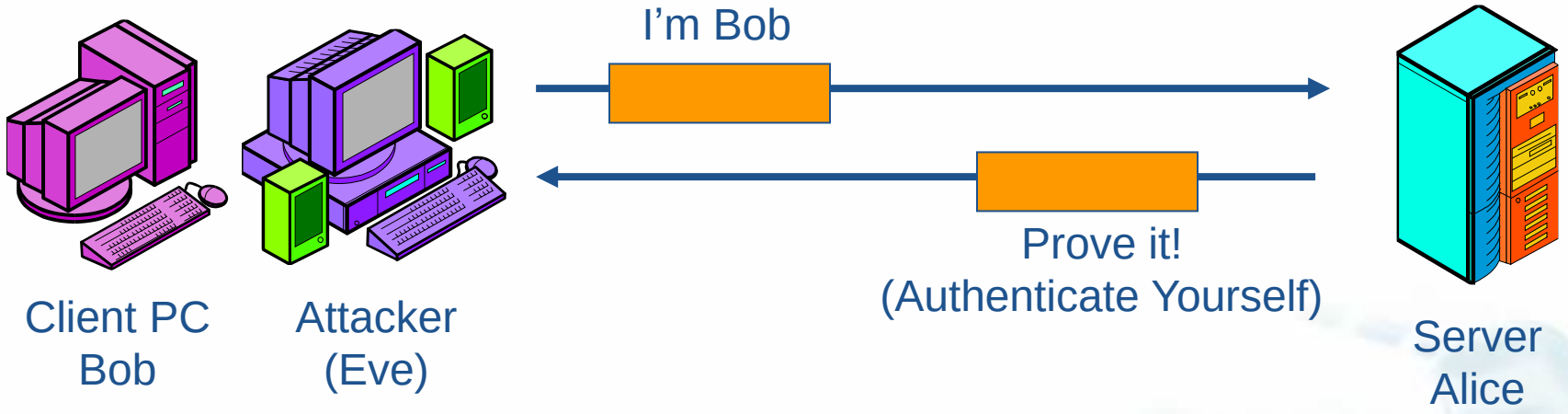
Eavesdropping on a Dialog



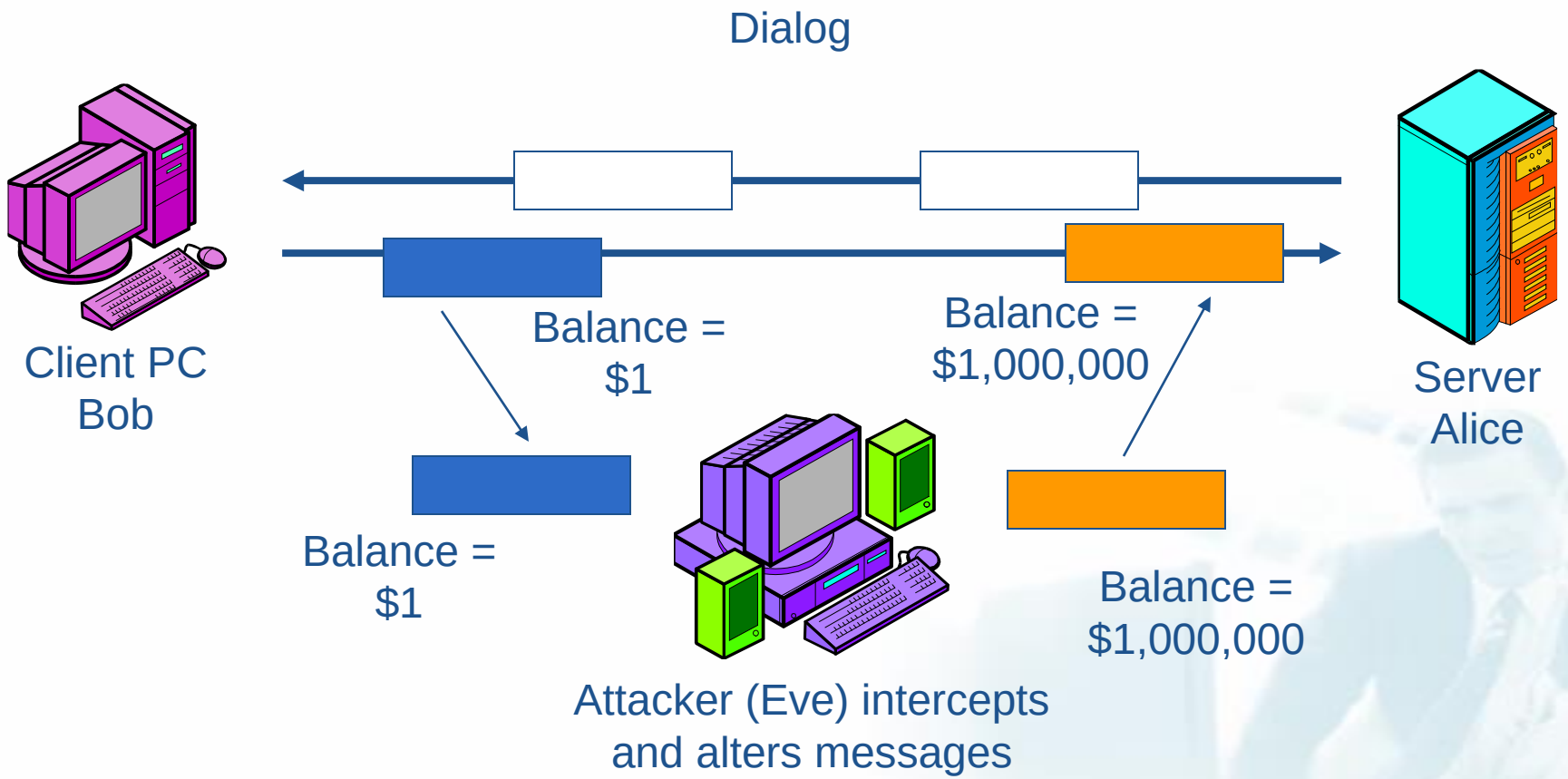
Encryption for Confidentiality



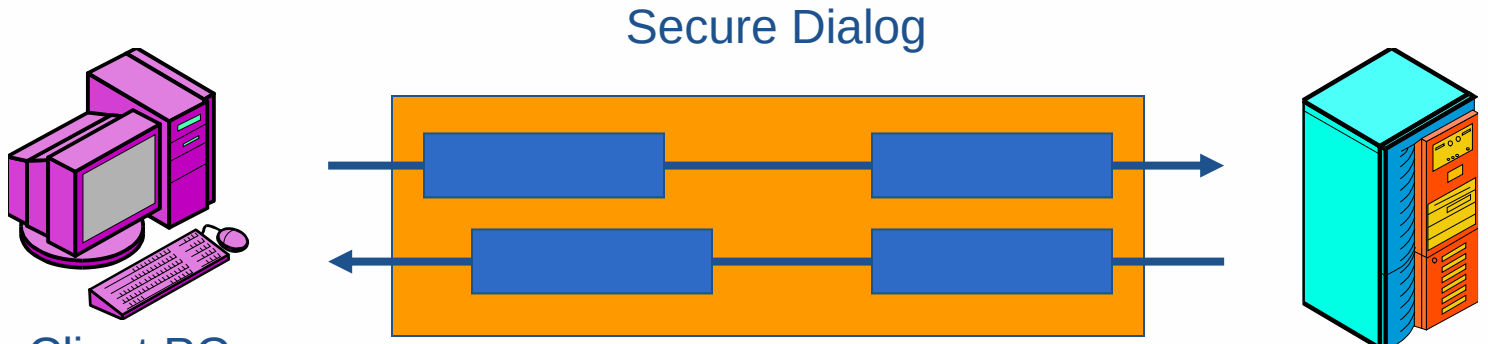
Impersonation and Authentication



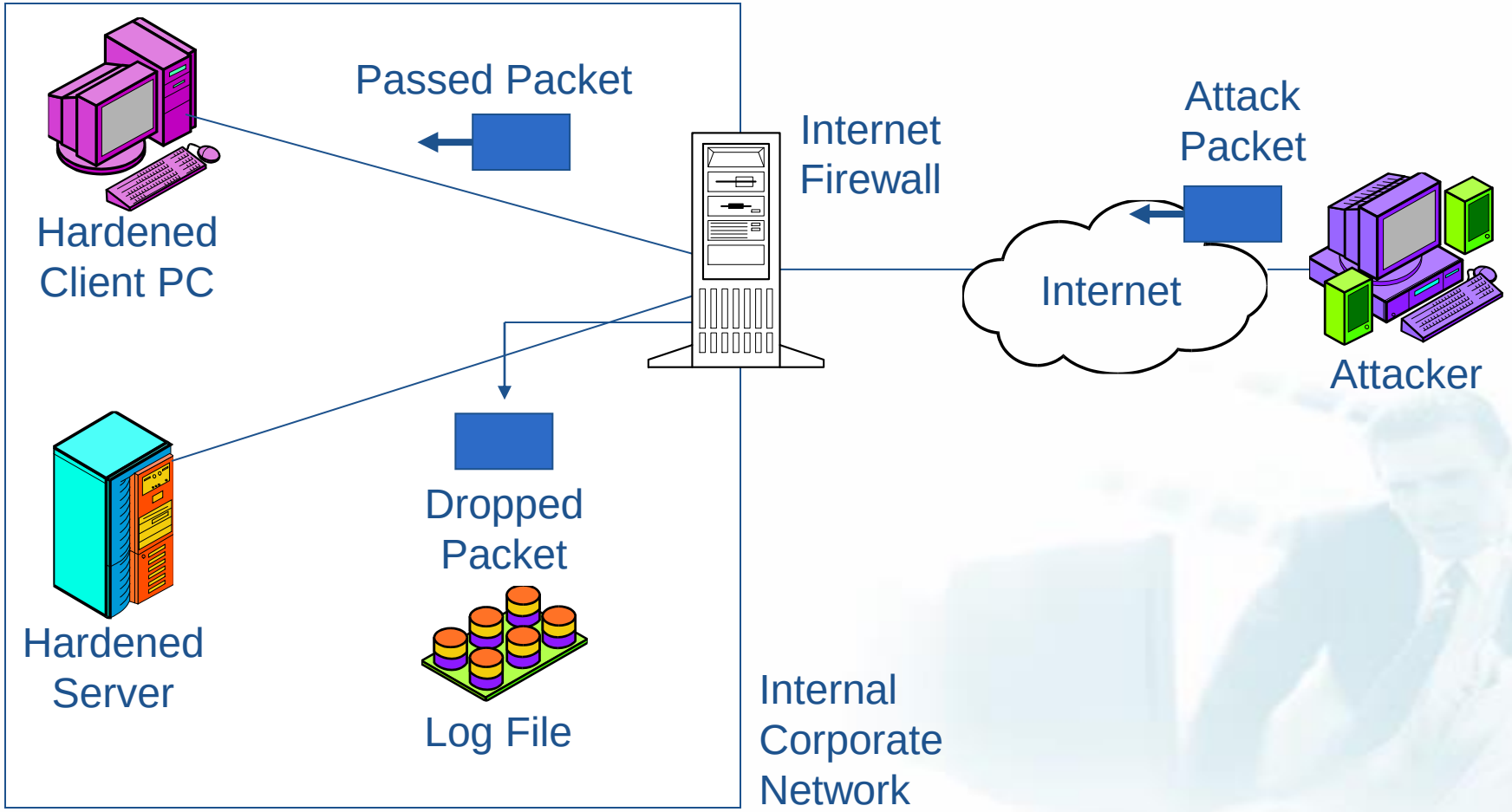
Message Alteration



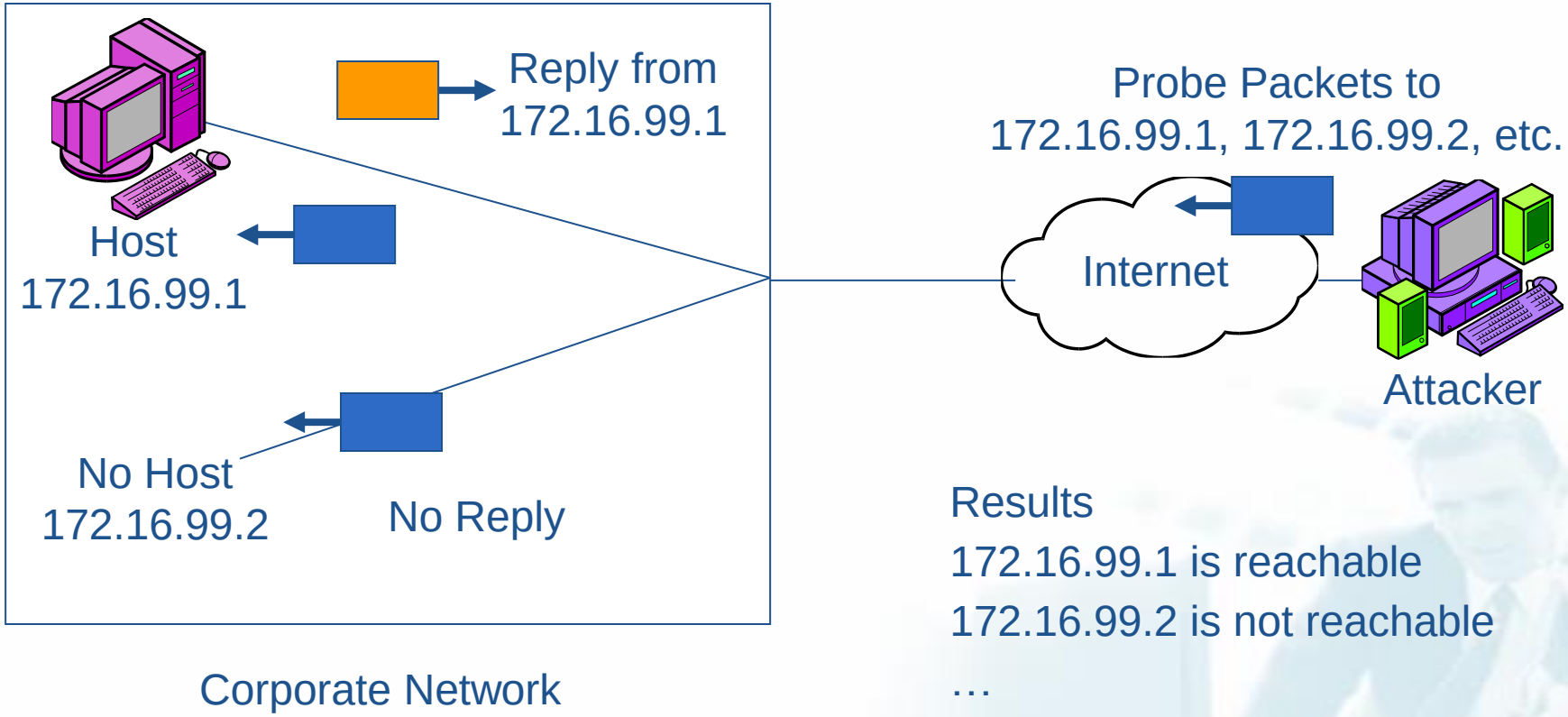
Secure Dialog System



Network Penetration Attacks and Firewalls

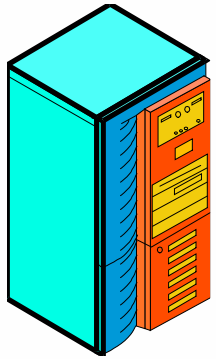


Scanning (Probing) Attacks

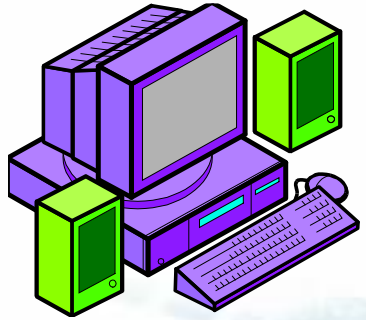


Results
172.16.99.1 is reachable
172.16.99.2 is not reachable
…

Single-Message Break-In Attack



1.
Single Break-In Packet



2.
Server
Taken Over
By Single Message

Attacker

Denial-of-Service (DoS) Flooding Attack

Intrusion Detection System (IDS)