Cipher

Ch2. Classical Encryption Techniques

Department of Computer Science

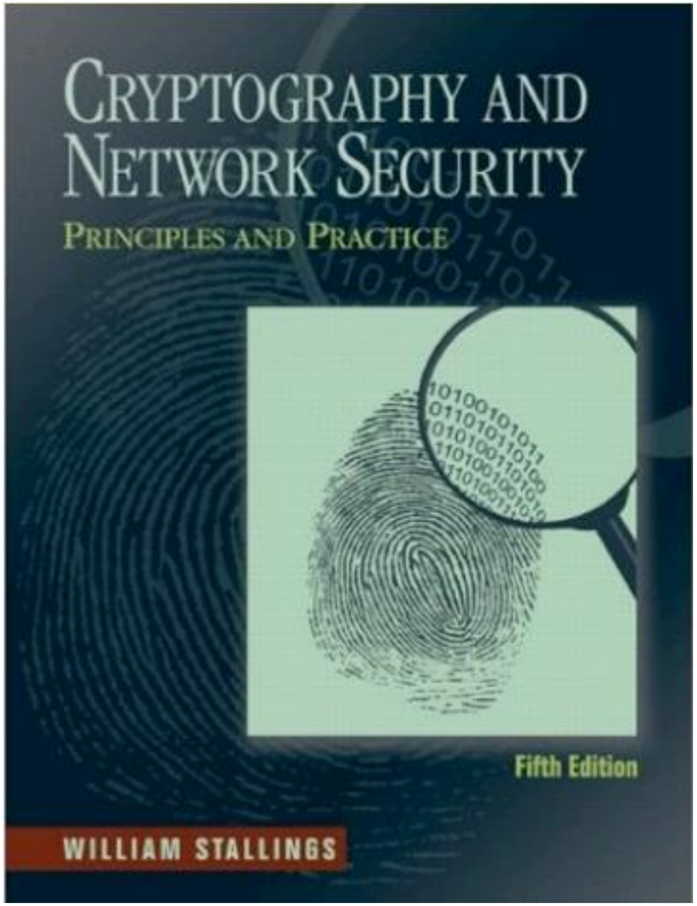
Academic Year: 2017-2018

Semester: One

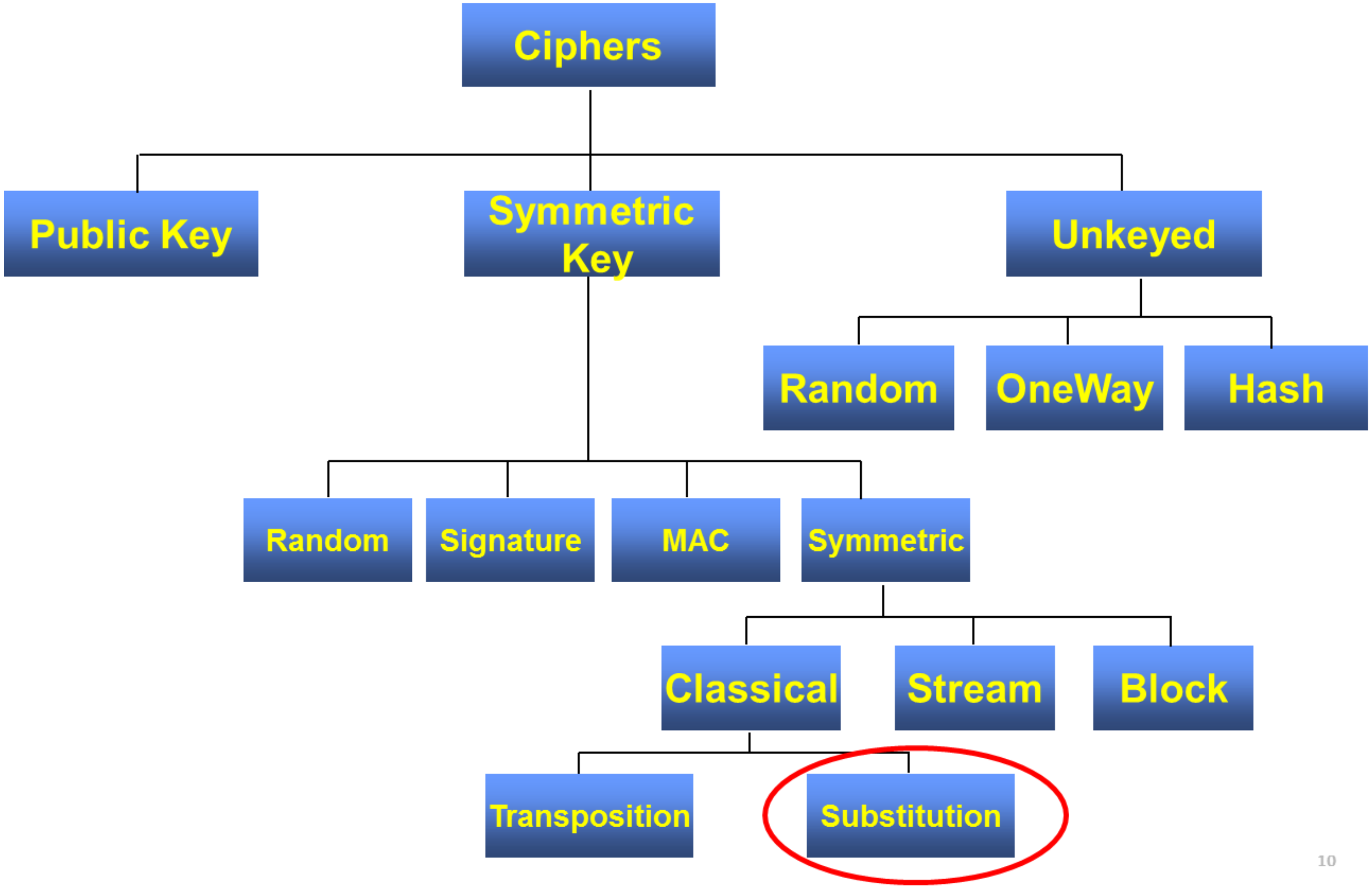
Dr. Maytham Mustafa Hammood

Textbook

- William Stallings, “Cryptography and Network Security Principles and Practice”, fifth edition, Prentice Hall



Cipher Classification



Ciphers

Public Key

Symmetric Key

Unkeyed

Random

OneWay

Hash

Random

Signature

MAC

Symmetric

Classical

Stream

Block

Transposition

Substitution

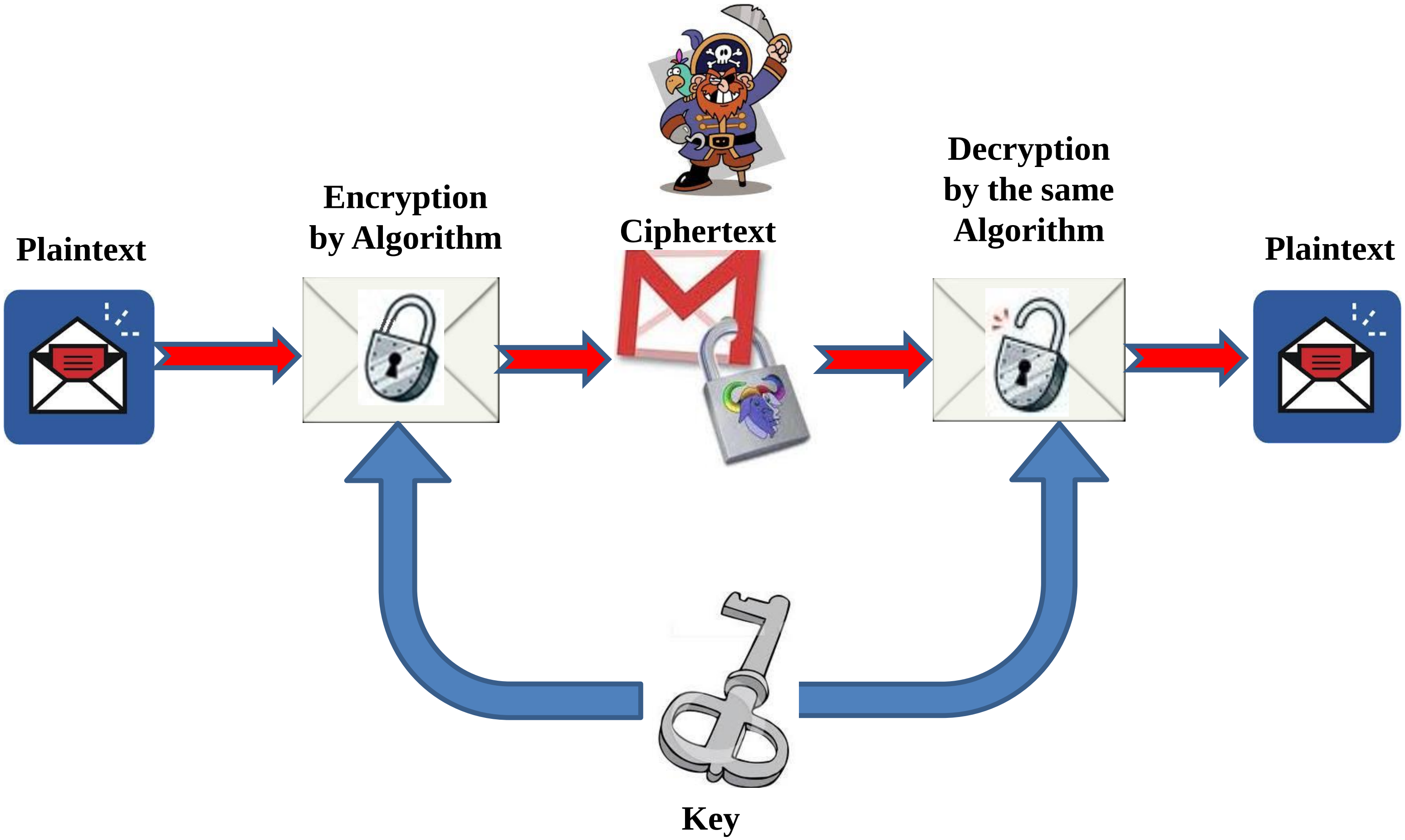
Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970’s
- and by far most widely used

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 attempting to break an encrypted message *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis
- **Mathematical attack**: analyzes characters in an encrypted text to discover the keys and decrypt the data

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = \mathrm{E}_K(X)$

  $X = \mathrm{D}_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- From two Greek words: *crypto*, meaning hidden, and *graph*, meaning writing.
- 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

Cryptography (continued)

- Success of cryptography depends on the robustness of encryption/decryption algorithms
- Encryption/decryption algorithm requires a key to encrypt/decrypt the message
- The security of the encryption is NOT rely on the secrecy of the algorithm but the secrecy of the key.
- Any mathematical key that creates a detectable pattern or structure is a **weak key** which provides an attacker with valuable information to break the encryption

Unconditional vs. Computational Security

- **Unconditional security**
  - No matter how much computer power is available, the cipher cannot be broken
  - The ciphertext provides insufficient information to uniquely determine the corresponding plaintext
  - Only one-time pad scheme qualifies
- **Computational security**
  - The cost of breaking the cipher exceeds the value of the encrypted info
  - The time required to break the cipher exceeds the useful lifetime of the info

Types of ciphers

- Private key cryptosystems/ciphers
  – The secret key is shared between two parties
- Public key cryptosystems/ciphers
  – The secret key is not shared and two parties can still communicate using their public keys

What is PKE used for?

Private Key Encryption (PKE) can be used:

- Transmitting data over an insecure channel
- Secure stored data (encrypt & store)
- Provide integrity check:
    - (Key + Mes.) -> MAC (message authentication code)

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

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- 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	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

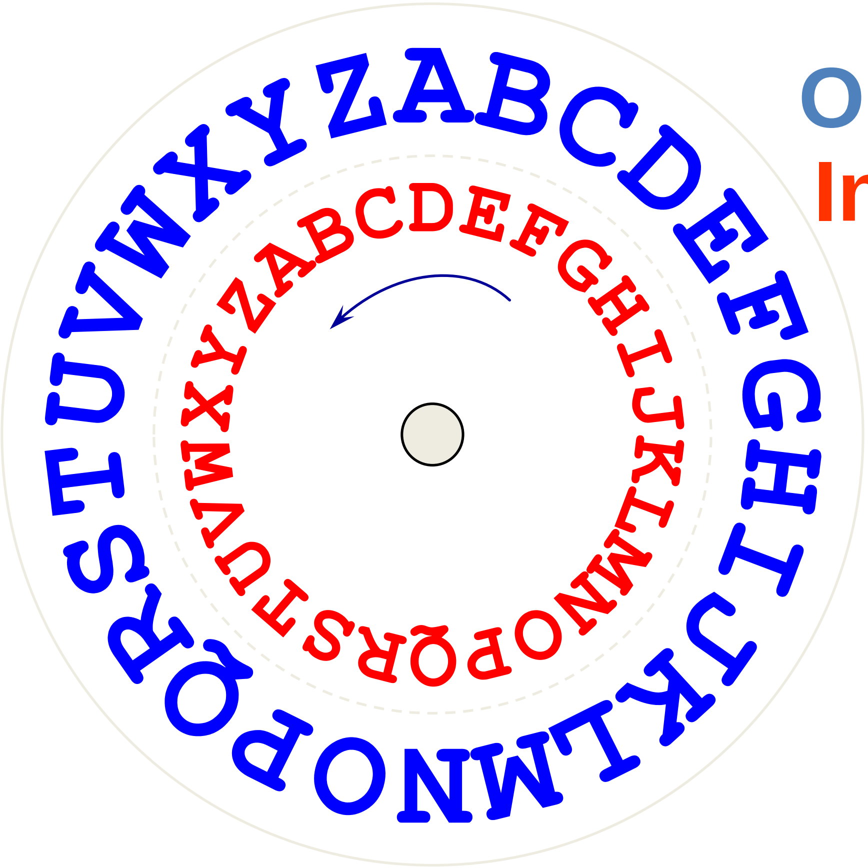
- then have Caesar cipher as:

$$c = \mathrm{E}(p) = (p + k) \bmod (26)$$

$$p = \mathrm{D}(\mathrm{c}) = (\mathrm{c} - k) \bmod (26)$$

The Caesar cipher (cont’d)

K=3



Outer: plaintext

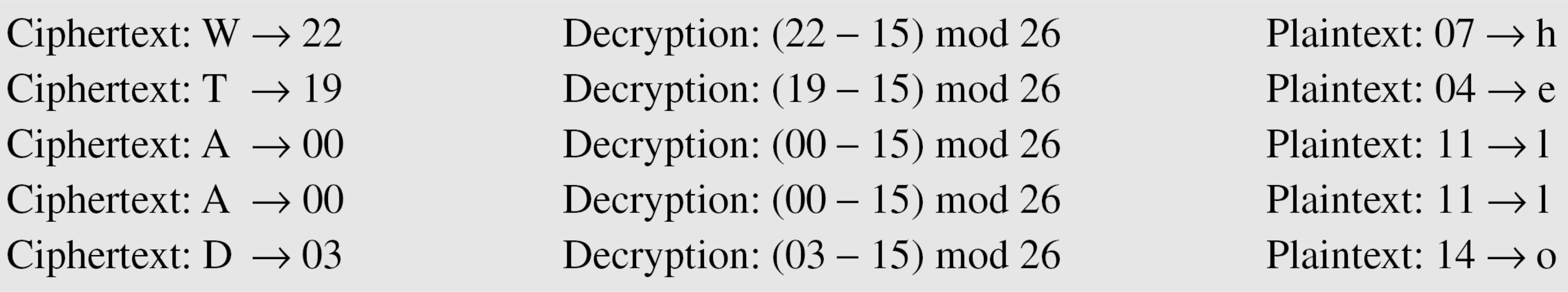
Inner: ciphertex

The Caesar cipher (cont’d)

Use the additive (Caesar) cipher with key = 15 to decrypt the message “WTAAD”.

Solution

We apply the decryption algorithm to the plaintext character by character:



Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

Cryptanalysis of Caesar Cipher

- Only have 25 possible ciphers
  - A maps to B,..Z
- Given ciphertext, just try all shifts of letters
- Do need to recognize when have plaintext
- E.g., break ciphertext "GCUA VQ DTGCM"

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’ If ‘X’ is a double letter, then insert another infrequent letter, say Q.
  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 Example

Use the following table: the Key is CHARLES

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

Encrypting the message: **THE SCHEME REALLY WORKS**

Playfair Example Cont.

- Break the plaintext in a two character diagram:
  - Plaintext is divided into 2-letter diagram
  - Use X to separate double letter
  - Use X to pad the last single letter

TH ES CH EM ER EA LL YW OR KS

TH ES CH EM ER EA L**X** LY WO RK S

TH ES CH EM ER EA L**X** LY WO RK S**X**

Playfair Encryption *Example Cont.*

- **TH -> PR**
- **ES -> SB**
- **CH -> HA**
- **EM -> DG**
- **ER -> DC**
- **EA -> BC**
- **LX -> AZ**
- **LY -> RZ**
- **WO -> VP**
- **RK -> AM**
- **SX -> BW**

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

Thus the message:
" THE SCHEME REALLY WORKS“
Becomes
"PR SB HA DG DC BC AX RZ VP AM BW “

Playfair Decryption Example Cont.

- Decryption the Ciphertext :-

"PRSBHA DGDC BCAX RZVP AMBW “

"PR SB HA DG DC BC AX RZ VP AM BW “

- PR ->TH
- SB ->ES
- HA ->CH
- DG ->EM
- DC ->ER
- BC ->EA
- AZ ->LX
- RZ ->LY
- VP ->WO
- AM ->RK
- BW ->SX

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

Playfair second Example

Prepare specific information

E.g. Shi Sherry loves Heath Ledger

Choose encryption key

E.g. Sherry

All the letters should be written in capital letter, in pairs, without punctuation, All Js are replaced with Is.

→**SH IS HE RR YL OV ES HE AT HL ED GE R**

Playfair second Example Cont.

- double letters which occur in a pair must be divided by an **X**
- E.g. LI TE RA LL Y→LI TE RA LX LY

→SH IS HE RR YL OV ES HE AT HL ED GE R

→SH IS HE RX RY LO VE SH EA TH LE DG ER

Playfair second Example Cont.

KEY: SHERRY→

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

Encryption
Or
Ciphering

Plaintext: SH IS HE RX RY LO VE SH EA TH LE DG ER

Ciphertext: HE GH ER DR YS IQ WH HE SC OY KR AL RY

Decipher

- Shift up and left instead of down and right
- Drop extra X
- Locate any missing any “I”s that should be “J”s
- Back into the original readable message

Playfair second Example Cont.

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

Decryption

or

Decipher

Ciphertext: HE GH ER DR YS IQ WH HE SC OY KR AL RY

Plaintext: SH IS HE RX RY LO VE SH EA TH LE DG ER

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

https://www.youtube.com/watch?v=quKhvu2tPy8

Vigenère Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ ...\ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

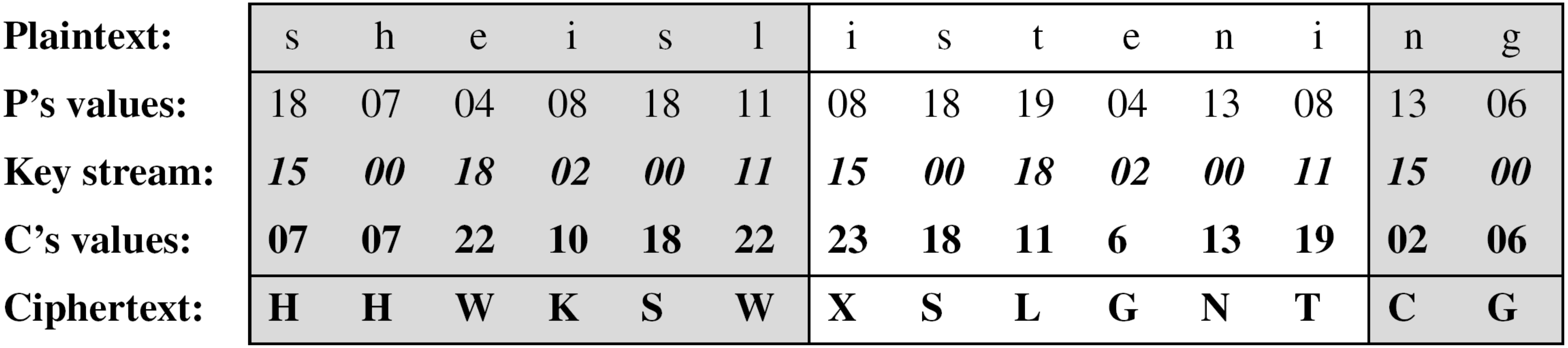
Example of Vigenère Cipher

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

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

Example of Vigenère Cipher

Let us see how we can encrypt the message “**She is listening**” using the 6-character keyword “**PASCAL**”. The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).



Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C’s values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Security of Vigenère Ciphers

- have multiple ciphertext letters for each plaintext letter
- hence letter frequencies are obscured
- but not totally lost
- start with letter frequencies
  - see if look monoalphabetic or not
- if not, then need to determine number of alphabets, since then can attach each

One-Time Pad

- **Developed by Gilbert Vernam in 1918, another name: *Vernam Cipher***
- **The key**
  - **a truly random sequence of 0’s and 1’s**
  - **the same length as the message**
  - **use one time only**
- **The encryption**
  - **adding the key to the message modulo 2, bit by bit.**

Encryption

$$c_i = m_i \oplus k_i \qquad i = 1,2,3,\ldots$$

Decryption

$$m_i = c_i \oplus k_i \qquad i = 1,2,3,\ldots$$

m_i : plain-text bits.

k_i : key (key-stream) bits

c_i : cipher-text bits.

Example

- **Encryption:**
- 1001001 1000110 plaintext
- 1010110 0110001 key
- 0011111 1110110 ciphertext

- **Decryption:**
- 0011111 1110110 ciphertext
- 1010110 0110001 key
- 1001001 1000110 plaintext

One-Time pad practical Problem

- Key-stream should be as long as plain-text
- Difficult in Key distribution & Management
- **Solution :**
  - Stream Ciphers
  - Key-stream is generated in pseudo-random fashion form Relatively short secret key

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 depend on the key
- then read off cipher row by row
- Plaintext= ***meet me after the toga party***
- 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

- **Example 1: Encipher “CHUCK NORRIS IS A TOUGH GUY”**
  - **Row 1: CUKORSSTUHU**
  - **Row 2: HCNRIIAOGGY**
  - **ciphertext: CUKORSSTUHUHCNRIIAOGGY**

Rail Fence cipher

- To decipher a rail fence cipher, we divide the ciphertext in half and reverse the order of the steps of encipherment, that is, write the ciphertext in two rows and read off the plaintext in zig-zag fashion. (Note: if there are an odd number of letters, the first row has one more letter then the second)
- Example 2: Decipher the message “CITAT ODABT UHROE ELNES WOMYE OGEHW VR
  - There are 32 letters:
  - Row 1: C I T A T O D A B T U H R O E E
  - Row 2: L N E S W O M Y E O G E H W V R
  - Solution: CLINTEASTWOODMAYBETOUGHERHOWEVER

  or

  - *Ciphertext: CLINT EASTWOOD MAY BE TOUGHER HOWEVER*

Rail Fence Cipher

Example:

WE ARE DISCOVERED FLEE AT ONCE

W E C R L T E

E R D S O E E F E A O C

A I V D E N

The message:

Ciphertext: WECRLTEERDSOEEFEAOCAIVDEN

…Decrypted

ITIAGOAIGTSHSSODSTES

I T I A G O A I G T

S H S S O D S T E S

Message: IS THIS AS GOOD AS IT GETS

Columnar Transposition Ciphers

- a more complex transposition
- write letters of message out in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

```
Key:3 4 2 1 5 6 7

                1   2   3   4   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: TTNA    APTM   TSUO   AODW    COIX
  KNLY    PETZ
```

Key Columnar Transposition

The message: WE ARE DISCOVERED FLEE AT ONCE

Example: Let the key word be: ZEBRA.

ZEBRA=53241

1	2	3	4	5
W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
F	L	E	E	A
T	O	N	C	E

CIPHERTEXT: EODAE ASREN EIELO RCEEC WDVFT.

Product Ciphers

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

RC4

- **Consists of 2 parts:**
  - **Key Scheduling Algorithm (KSA)**
    - **Generates State array**
  - **Pseudo-Random Generation Algorithm (PRGA)**
    - **Generates keystream**
- **XOR-ed keystream with the plaintext to generate ciphertext**

KSA

PRGA

RC4

- starts with an array S of numbers: 0..255
- use key to well and truly shuffle
- S forms **internal state** of the cipher

```
for i = 0 to 255 do
    S[i] = i
    T[i] = K[i mod keylen])
j = 0
for i = 0 to 255 do
    j = (j + S[i] + T[i]) (mod 256)
    swap (S[i], S[j])
```

RC4

- encryption continues shuffling array values
- sum of shuffled pair selects "stream key" value from permutation
- XOR S[t] with next byte of message to en/decrypt

```
i = j = 0
for each message byte $M_i$
    i = (i + 1) (mod 256)
    j = (j + S[i]) (mod 256)
    swap(S[i], S[j])
    t = (S[i] + S[j]) (mod 256)
    $C_i$ = $M_i$ XOR S[t]
```

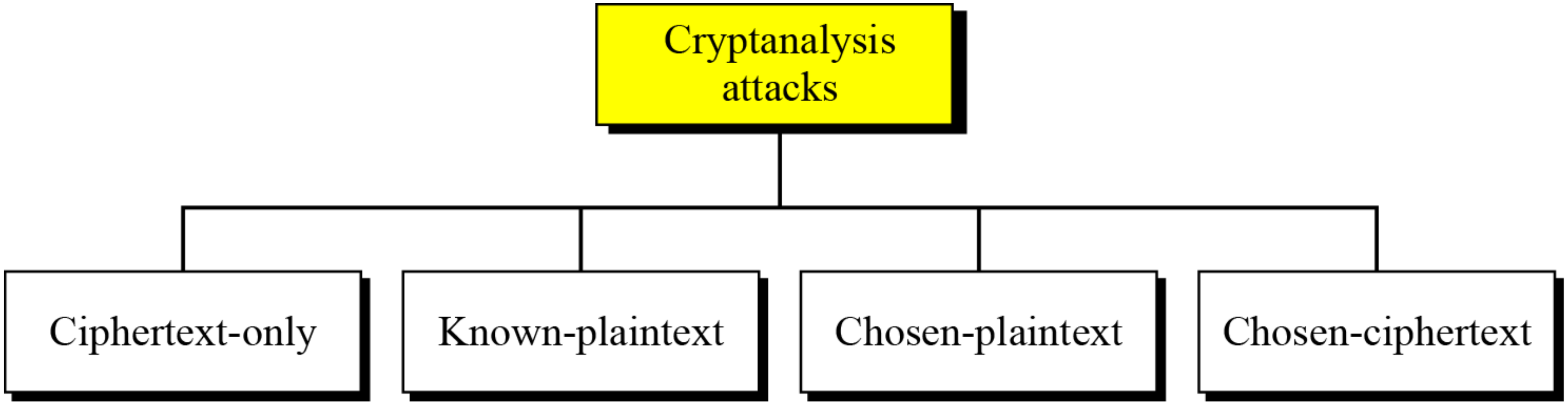
https://www.youtube.com/watch?v=VuC9PJ1ZUzk

Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext

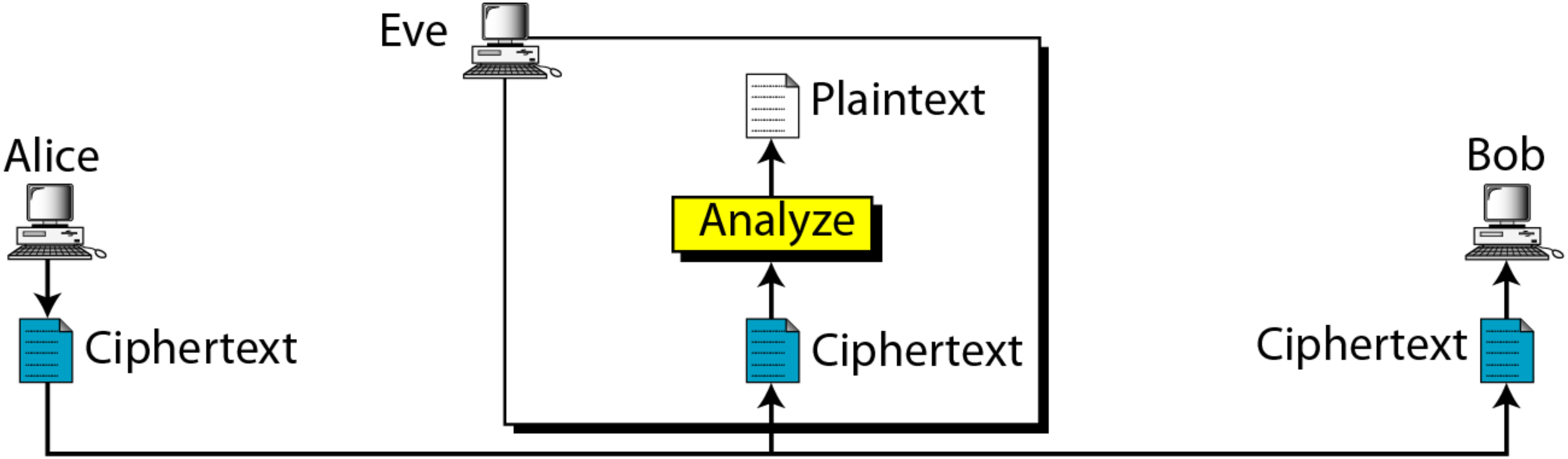
As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.

Figure 3.3 Cryptanalysis attacks



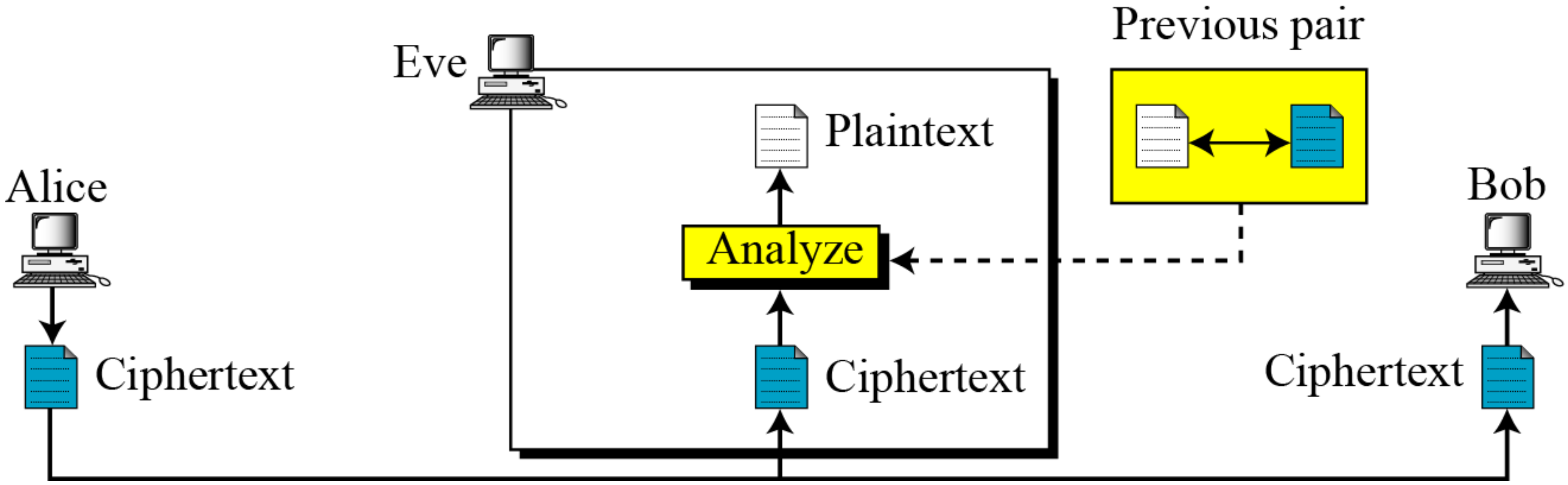
Ciphertext-Only Attack

Figure 3.4 Ciphertext-only attack



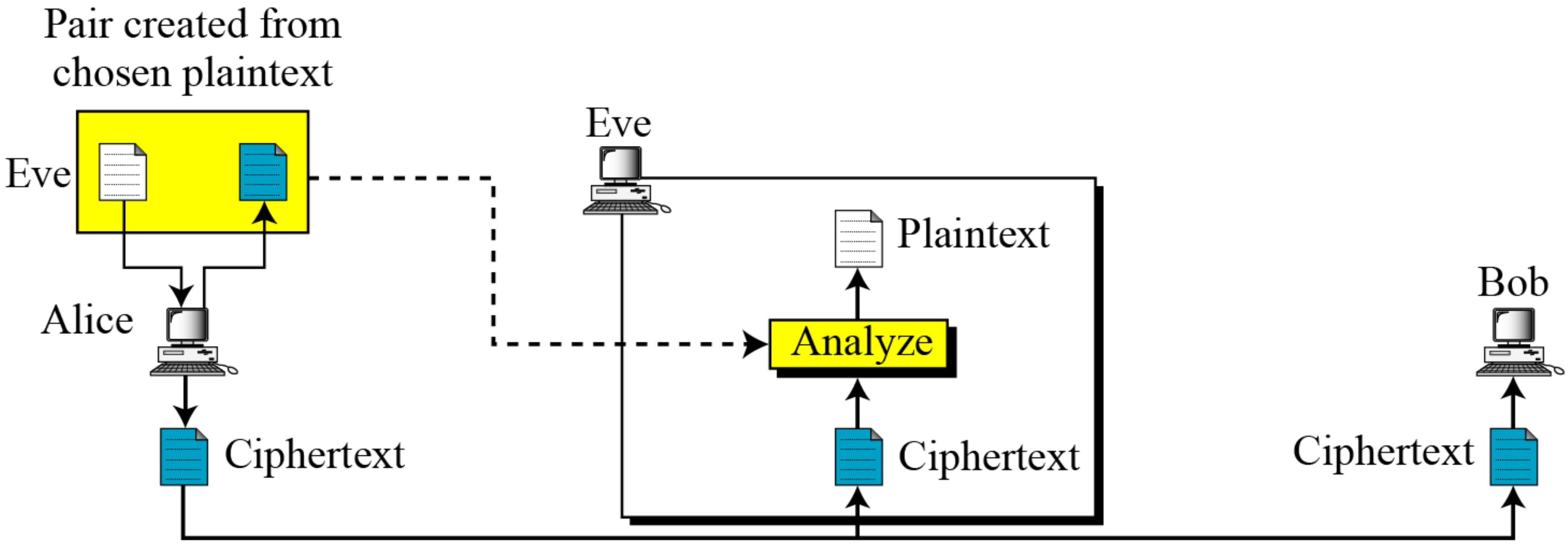
Known-Plaintext Attack

Figure 3.5 Known-plaintext attack



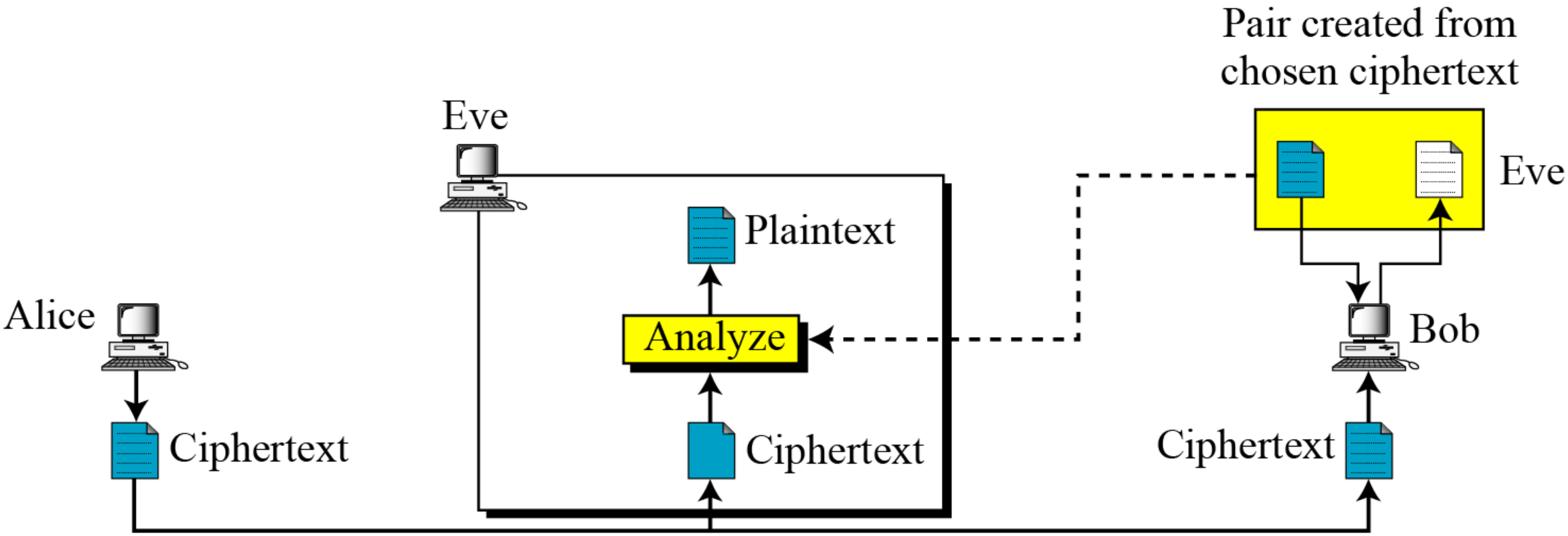
Chosen-Plaintext Attack

Figure 3.6 Chosen-plaintext attack



Chosen-Ciphertext Attack

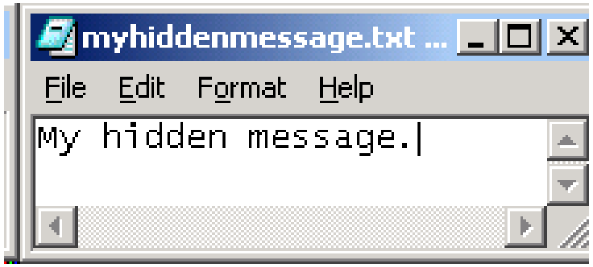
Figure 3.7 Chosen-ciphertext attack



Steganography

- Steganography
  - **from the Greek word steganos meaning “covered”**
  - **and the Greek word graphie meaning “writing”**
- **Steganography** is the process of hiding of a secret message within an ordinary message and extracting it at its destination
- Anyone else viewing the message will fail to know it contains hidden/encrypted data
- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few info bits

Steganography – Modern Day

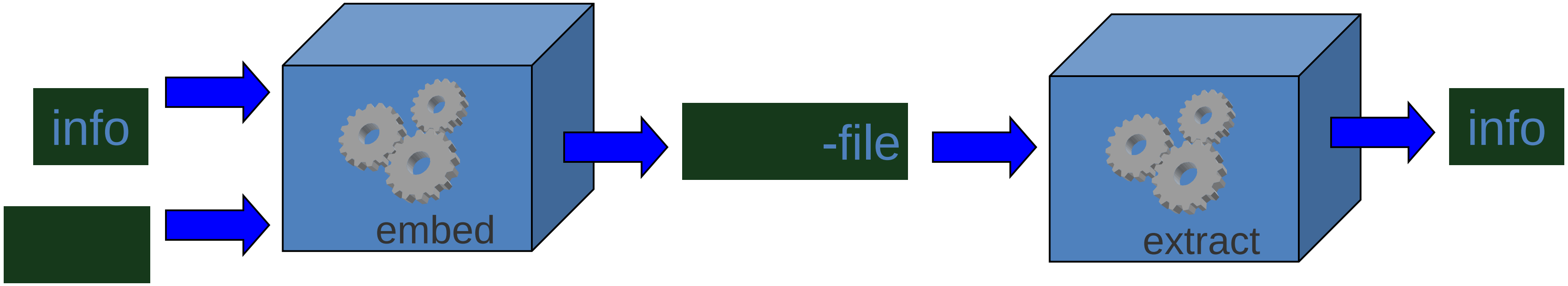


My hidden message.

Carrier File

Carrier File with Hidden Message

Steganography



The **cover** provides a host for transporting the hidden info.

Steganography Carrier Files

bmp

jpeg

gif

wav

mp3

Amongst others…

Steganalysis - Definition

- Definition
  - Identifying the existence of a message
  - **Not** extracting the message
  - Note: Technically, Steganography deals with the concealment of a message, not the encryption of it

- Steganalysis essentially deals with the *detection* of hidden content

Watermarking

- **Watermark-**-an invisible signature embedded inside digital Media, such as images to show authenticity or proof of ownership
- Discourage unauthorized copying and distribution of images over the internet
- Ensure a digital picture has not been altered
- Software can be used to search for a specific watermark

Copyright Protection: To prove the ownership

of digital media