CHAPTER 2

CLASSICAL ENCRYPTION/DECRYPTION TECHNIQUES

Symmetric Encryption

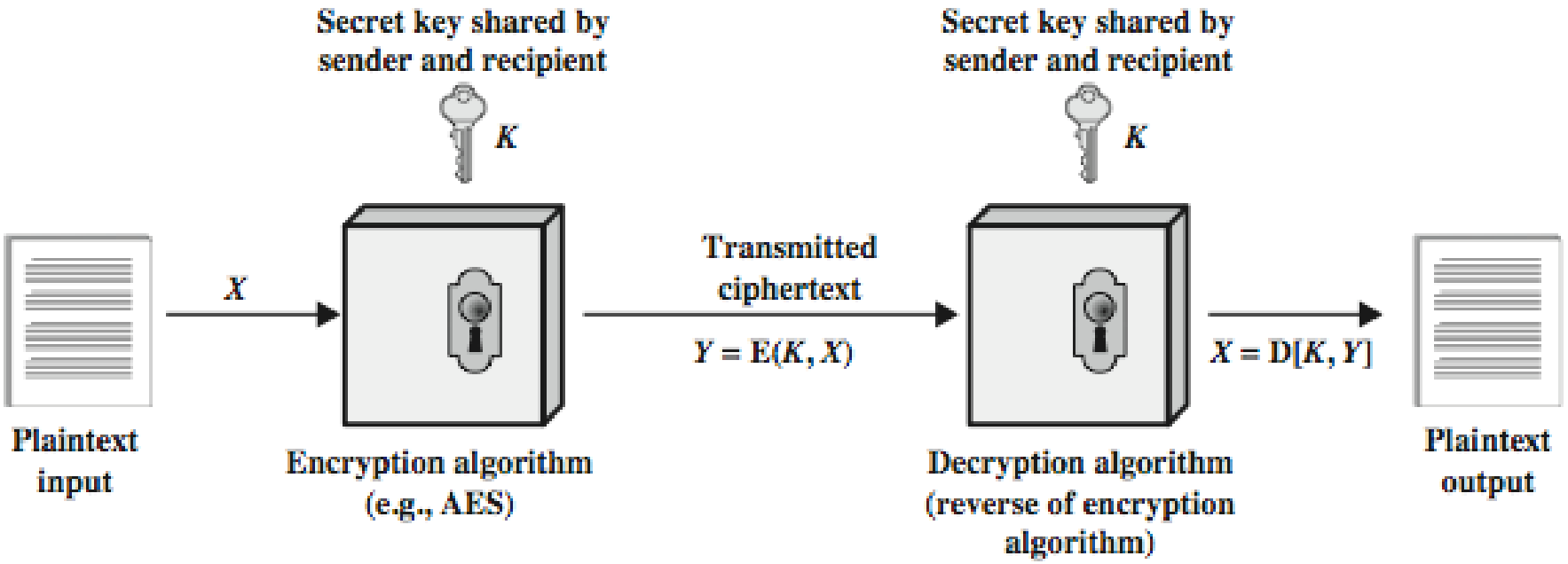
- Oldest type of encryption until 1970's

- **Symmetric**
  - Both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.

- **Other names**
  - Classical / Conventional / Single-key encryption

- **Plaintext** - original message
- **Encryption algorithm**
  - performs substitutions, transformations on plaintext.
  - **input**: plaintext, key. **output**: cipher text
- **Secret Key**
  - different keys → different outputs, using substitutions and transformations
- **Cipher text** - depend on plaintext and key
- **Decryption algorithm**
  - Inverse of encryption algorithm.
  - **input**: cipher text, key. **output**: plaintext

Simplified Model



Characterization

- **Type of operations for transforming plaintext to cipher text:**
  - **Substitution:** each element of plaintext is mapped to another element.
  - **Transposition:** plaintext elements rearranged.
  - **Product systems:** involve multiple stages of substitutions and transpositions

- **Number of keys used**
  - **Symmetric encryption:** both sender and receiver use the same key.
  - **Asymmetric, or public-key encryption:** sender and receiver use different keys.

Classical Substitution Ciphers

- Letters in plaintext is replaced by
  - other letters
  - numbers
  - symbols

Substitution Techniques

- Caesar cipher
- Monoalphabetic ciphers
- Playfair cipher
- Polyalphabetic ciphers
- One-time pad

Caesar Cipher

- Ciphertext letter = plaintext letter + 3
- Letters wrap around, Z is next after A

```
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
```

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

Caesar Cipher

- C = E(3, p) = (p + 3) mod 26

C = E(k, p) = (p + k) mod 26

p = D(k, C) = (C - k) mod 26

- Example

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

Brute Force Attack

Break ciphertext “PHHW PH DIWHU WKH KRJD SDUWB"

- Encryption and decryption algorithms are known
- Only 25 keys to try
- Plaintext language is known

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

Playfair Cipher

- 5×5 matrix of letters
- Constructed using a keyword

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 encrypted two letters at a time
- Repeating letters separated by filler “x”

e.g. balloon → ba lx lo on

- Letters in same row are each replaced by letter to right.

e.g. ar → RM

- Letters in same col are each replaced by letter beneath.

e.g. mu → CM

- Otherwise, letter replaced by one in its row and col of the other letter.

e.g. hs → BP

Vigenère Table

Key	Plaintext																									
	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
a	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
b	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	A
c	C	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
d	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Example

- Keyword: deceptive
- Plaintext: we are discovered save yourself

Keyword	**deceptive**
Key	**deceptivedeceptivedeceptive**
Plaintext	**wearediscoveredsaveyourself**
Ciphertext	**ZICVTWQNGRZGVTWAVZHCQYGLMGJ**

One-Time Pad – Example

- Vigenère scheme with 27 characters
- 27th character is space
- One-time key/message, = message length

```
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
```

Transposition Matrix

- Write message in rectangle, row by row
- Read message off, column by column
- Permute order of columns
- Order of columns is the key

```
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
```

Multiple Transpositions

```
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
```

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