

# CLASSICAL ENCRYPTION TECHNIQUES

- Symmetric Cipher Model
- Substitution Techniques
- Transposition Techniques
- Rotor Machines
- Steganography

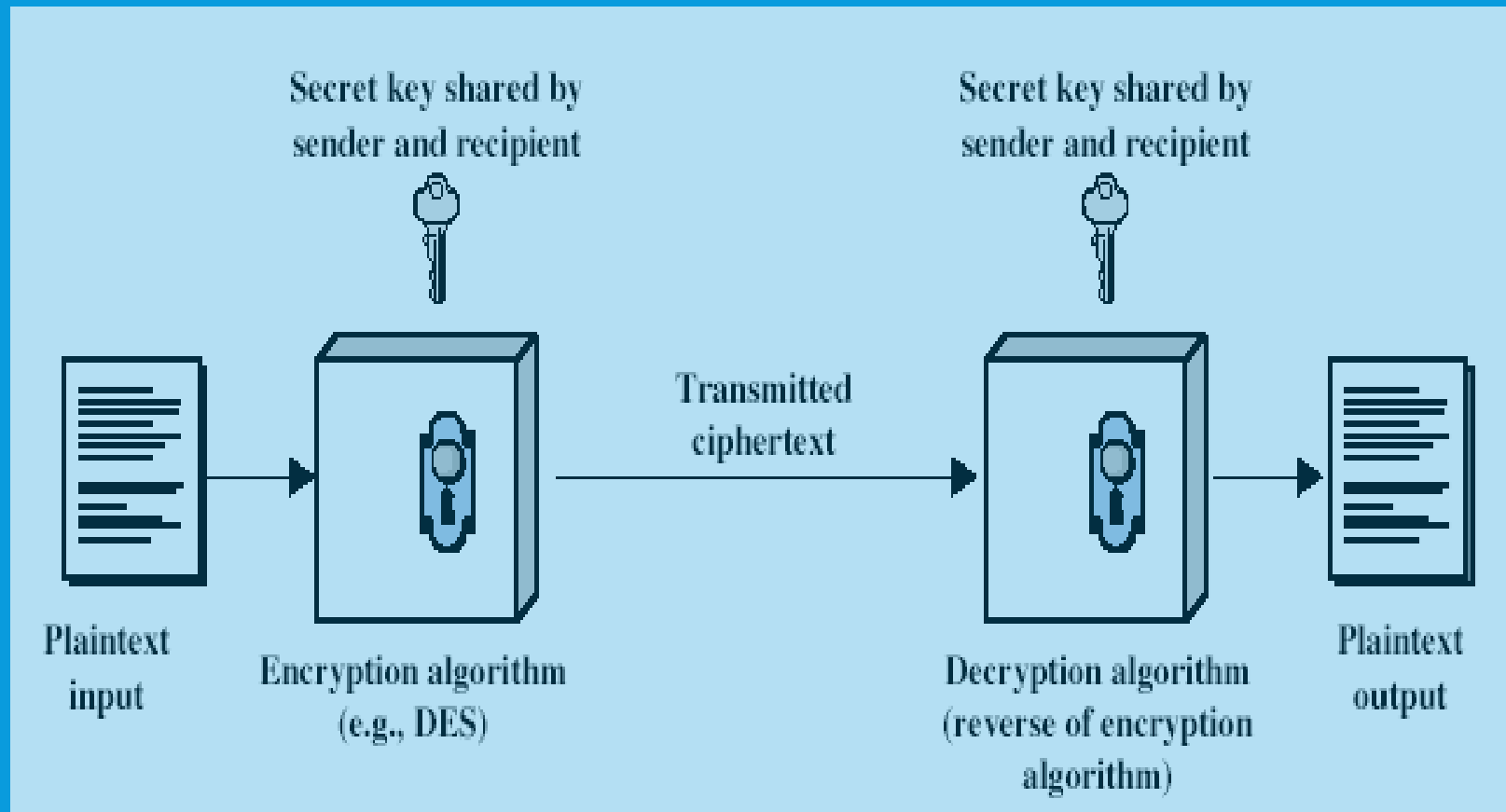
# SYMMETRIC ENCRYPTION

- Conventional / private-key / single-key
- Sender and recipient share a common key
- all classical encryption algorithms are private-key
- The only type prior to invention of public-key in 1970's
- 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 deciphering ciphertext *without* knowing key
- ❖ **Cryptology** - field of both cryptography and cryptanalysis

# SYMMETRIC CIPHER MODEL



# REQUIREMENTS

- Requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- Mathematically :
$$Y = E_K(X)$$
$$X = D_K(Y)$$
- Assumption: encryption algorithm is known
- Implication: a secure channel to distribute key

# SYMMETRIC CRYPTO SYSTEM

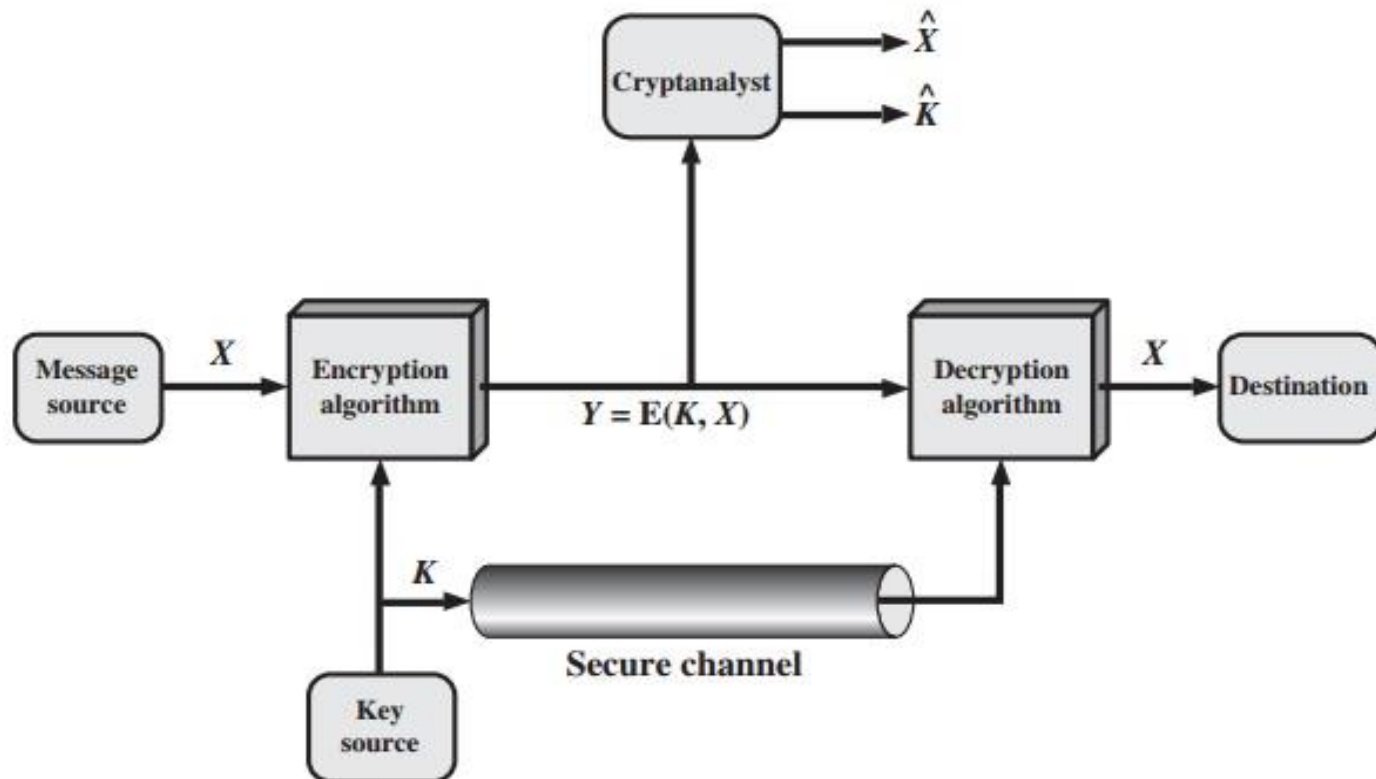


Figure 2.2 Model of Symmetric Cryptosystem

# CRYPTOGRAPHY

- Characterize cryptographic system along three dimensions:
  - 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

# CRYPTANALYSIS

- Objective is to recover key not just message
- General approaches:
  - Cryptanalytic attack
    - Rely on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs
  - Brute-force attack
    - Try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average half of all possible keys must be tried to achieve success.



# 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

## ➤ **Chosen text**

- Select plaintext or ciphertext to en/decrypt

# ENCRYPTION SCHEME

## ➤ Unconditionally secure

- No matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

## ➤ Computationally secure

- Given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

# BRUTE FORCE SEARCH

- Always possible to simply try every key
- Most basic attack, proportional to key size
- Assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ $\mu$ s	Time required at $10^6$ decryptions/ $\mu$ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56 (DES)	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128 (AES)	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168 (Triple-DES)	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation) (Mono-alphabetic)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

# CLASSICAL ENCRYPTION TECHNIQUES

- Symmetric Cipher Model
- **Substitution Techniques**
- Transposition Techniques
- Rotor Machines
- Steganography

# CLASSICAL SUBSTITUTION CIPHERS

- Where letters of plaintext are replaced by other letters or by numbers or symbols
- If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
  - Caesar Cipher
  - Monoalphabetic Cipher
  - Playfair Cipher
  - Hill Cipher
  - Vignere Cipher
  - Auto key Cipher
  - Vernam Cipher

# 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

- 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

# 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

- Decrypt the following :
  - wuhdwb lpsrvvleoh

# 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:

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

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



# 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"

# 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:    abcdefghijklmnopqrstuvwxyz

Cipher:  DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:    ifwewishtoreplaceletters

Ciphertext:  WIRFRWAJUHYFTSDVFSFUUFYA

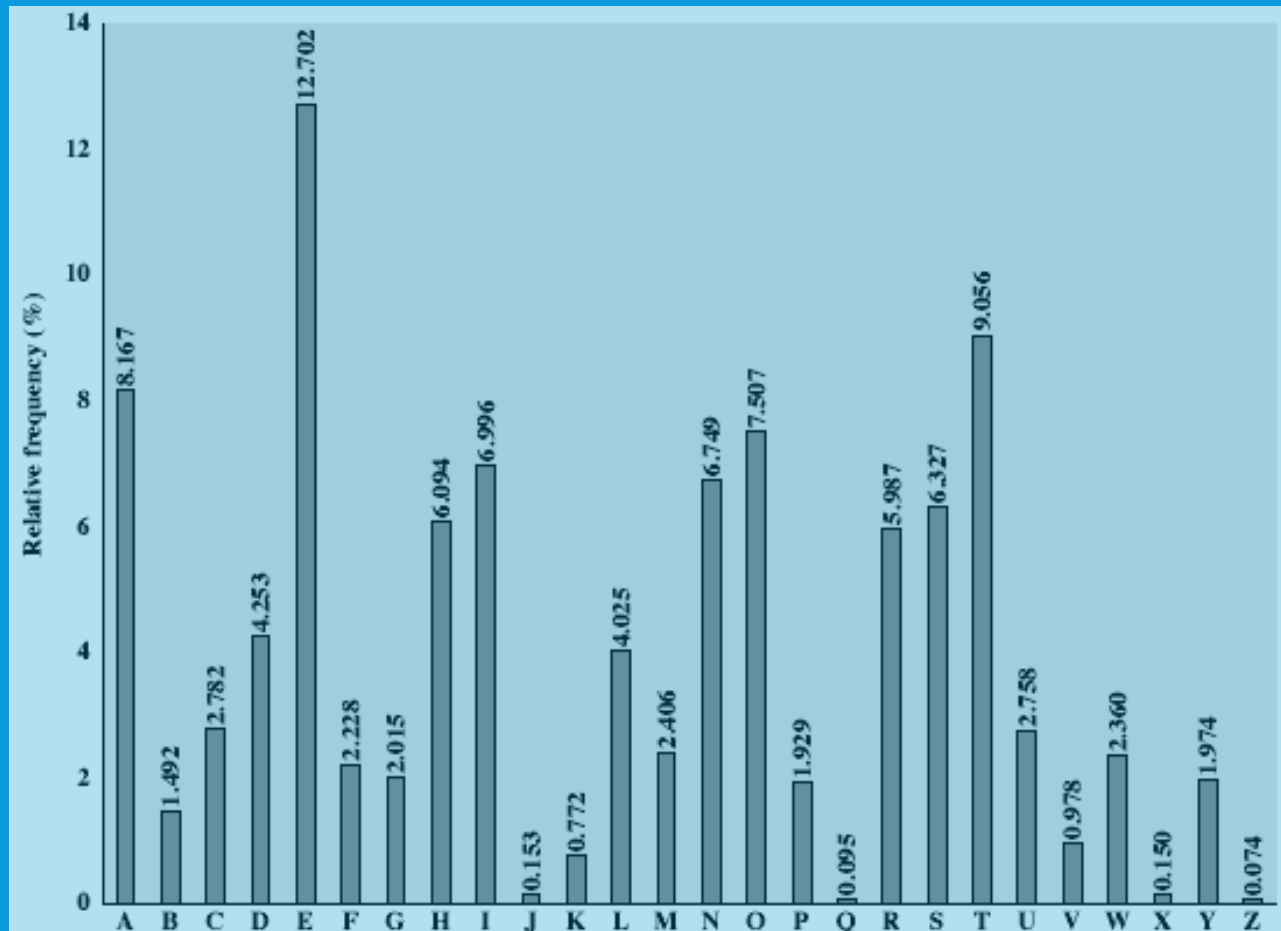
# MONOALPHABETIC CIPHER SECURITY

- 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**
- Eg "th lrd s m shphrd shll nt wnt"
- Letters are not equally commonly used
- In english E is by far the most common letter
  - Followed by T,R,N,I,O,A,S
- 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



# USE IN CRYPTANALYSIS

- Key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- Discovered by arabian scientists in 9<sup>th</sup> century
- Calculate letter frequencies for ciphertext
- Compare counts/plots against known values
- If caesar cipher look for common peaks/troughs
  - Peaks at: A-E-I triple, NO pair, RST triple
  - Troughs at: JK, X-Z
- For monoalphabetic must identify each letter
  - Tables of common double/triple letters help

# EXAMPLE CRYPTANALYSIS

VUEPHZHZMDZSHZOWSFPAPPDTSVPQUZWYMXUZHUSX  
EPYEPDPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- count relative letter frequencies
- guess P & Z are e and t

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				

- guess ZW is th and hence ZWP is the

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ  
t a e e te a that e e a a  
VUEPHZHZMDZSHZOWSFPAPPDTSVPQUZWYMXUZHUSX  
e t ta t ha e ee a e th t a  
EPYEPDPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ  
e e e tat e the t

# EXAMPLE CRYPTANALYSIS

## ➤ Given ciphertext:

Uzqsovuohxmopvgpozpevsgzwszopfpesxudbmetsxaiz  
Vuephzhmdzshzowsfpappdtsvpquzwxymxuzuhsx  
Epyepopdzszufpombzwpfupzhmdjudtmohmq

## ➤ Count relative letter frequencies

## ➤ 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

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				



# 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

# Example of Playfair Cipher

- Key: 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

- Plaintext: BALLOON

○ BA LX LO ON

- Ciphertext: IB SU PM NA

# ENCRYPTING

## ➤ INSTRUMENTS

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

# ENCRYPTING

- INSTRUMENTS
- IN ST RU ME NT SZ
- GA TL MZ CL RQ TX

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

# DECRYPTING

## ➤ KOKFRYPBFS

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

# DECRYPTING

➤ KOKFRYPBFS

➤ KO KF RY PB FS

➤ FR IE ND SH IP

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

# 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



# SECURITY OF PLAYFAIR CIPHER

- Security much improved over monoalphabetic
- Since have  $26 \times 26 = 676$  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

# Hill Cipher

- Developed by the mathematician Lester Hill in 1929.
- The encryption algorithm takes  $m$  successive plain text and substitute for them  $m$  cipher text letters.
- Each character is assigned a numerical value ( $a=0, \dots, z=25$ ).

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

$$C = KP \text{ mod } 26$$

$$P = K^{-1}C \text{ mod } 26 = KK^{-1}P = P$$

# ENCRYPT

- Text : ACT
- Key: GYBNQKURP

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

- ENCRYPT : POH

# DECRYPT

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

# DECRYPT

Decrypt → POH

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Plain text → ACT

# INVERSE OF A MATRIX

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

The inverse of a matrix is found using the following formula:

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}$$

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\begin{aligned} \begin{bmatrix} 4 & 7 \\ 2 & 6 \end{bmatrix}^{-1} &= \frac{1}{4 \times 6 - 7 \times 2} \begin{bmatrix} 6 & -7 \\ -2 & 4 \end{bmatrix} \\ &= \frac{1}{10} \begin{bmatrix} 6 & -7 \\ -2 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 0.6 & -0.7 \\ -0.2 & 0.4 \end{bmatrix} \end{aligned}$$

# FINDING K

- Suppose that the plaintext "friday" is encrypted using a 2 x 2 Hill cipher to yield the ciphertext PQCFCU

$$\mathbf{K} \begin{pmatrix} 5 \\ 17 \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 \\ 16 \end{pmatrix};$$

$$\mathbf{K} \begin{pmatrix} 8 \\ 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

$$\mathbf{K} \begin{pmatrix} 0 \\ 24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$$

$$\begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} = \mathbf{K} \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

$$\mathbf{K} = \begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} = \begin{pmatrix} 137 & 60 \\ 149 & 107 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$$

# POLYALPHABETIC CIPHERS

- Improve security using multiple cipher alphabets
- Make 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
- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.



# VIGENÈRE 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
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 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

# VIGENÈRE CIPHER

key:           deceptivedeceptivedeceptive

plaintext:wearediscoveredsaveyourself

Ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

	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

# VIGENÈRE CIPHER ENCRYPT

key: lemon

plaintext:attackatdawn

	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



# VIGENÈRE CIPHER DECRYPT

Cipher: VVVRBACP

Key: COVER

Plain text:

	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

# 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
- Repeat from start after  $d$  letters in message
- Decryption simply works in reverse

# 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 it looks monoalphabetic or not
- If not, then need to determine number of translation alphabets, since then can attack each

# KASISKI METHOD

- Method developed by babbage / kasiski
- Repetitions in ciphertext give clues to period
- So find same plaintext an exact period apart
- Which results in the same ciphertext
- Of course, could also be random fluke
- Eg repeated “VTW” in previous example
- Suggests size of 3 or 9
- Then attack each monoalphabetic cipher individually using same techniques as before



# VIGENÈRE CIPHER

key:                   deceptivedeceptivedeceptive

plaintext:wearediscoveredsaveyourself

Ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

	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

# AUTOKEY CIPHER

- Ideally want a key as long as the message
- Vigenère proposed the **autokey** cipher
- With keyword is prefixed to message as key
- Knowing keyword can recover the first few letters
- Use these in turn on the rest of the message
- But still have frequency characteristics to attack
- Eg. Given key *deceptive*

Key:           deceptivewearediscoveredsav

Plaintext: wearediscoveredsaveyourself

Ciphertext: zicvtwqngkzeiigasxstslvvwla

# VERNAM CIPHER

*Plain text – H E L L O → 7 4 11 11 14*

*Key – M O N E Y → 12 14 13 4 24*

*Plain text + key → 19 18 24 15 38*

*→ 19 18 24 15 12 (=38 - 26)*

**Cipher Text → T S Y P M**

*Cipher Text – T S Y P M → 19 18 24 15 12*

*Key – M O N E Y → 12 14 13 4 24*

*Cipher text - key → 7 4 11 11 -12*

*→ 7 4 11 11 14*

**Message → H E L L O**

# 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
- Problems in generation & safe distribution of key

# ONE-TIME PAD

```
ciphertext: ANKYODKYUREPFJBYOJDSPLEIYIUNOFDOIUERFPLUYTS  
key:        pxlmvmsydofuyrvzwc tnlebnecvvgdupahfzzlmnyih  
plaintext:  mr mustard with the candlestick in the hall
```

```
ciphertext: ANKYODKYUREPFJBYOJDSPLEIYIUNOFDOIUERFPLUYTS  
key:        mfugpmydgaxgoufhkl11lmhsqdqogtewbqfgyovuhwt  
plaintext:  miss scarlet with the knife in the library
```