Classical Encryption Techniques

Week 4

WHAT IS CRYPTOGRAPHY?

Cryptography is the science of using mathematics to encrypt and decrypt data.

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

WHAT IS CRYPTOGRAPHY?

- The art of secret writing
- The art of protecting information
- The science of encrypting or hiding *secrets*
- Needed for confidentiality

BASIC TERMINOLOGY

- **plaintext** - the original message
- **ciphertext** - the 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 ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

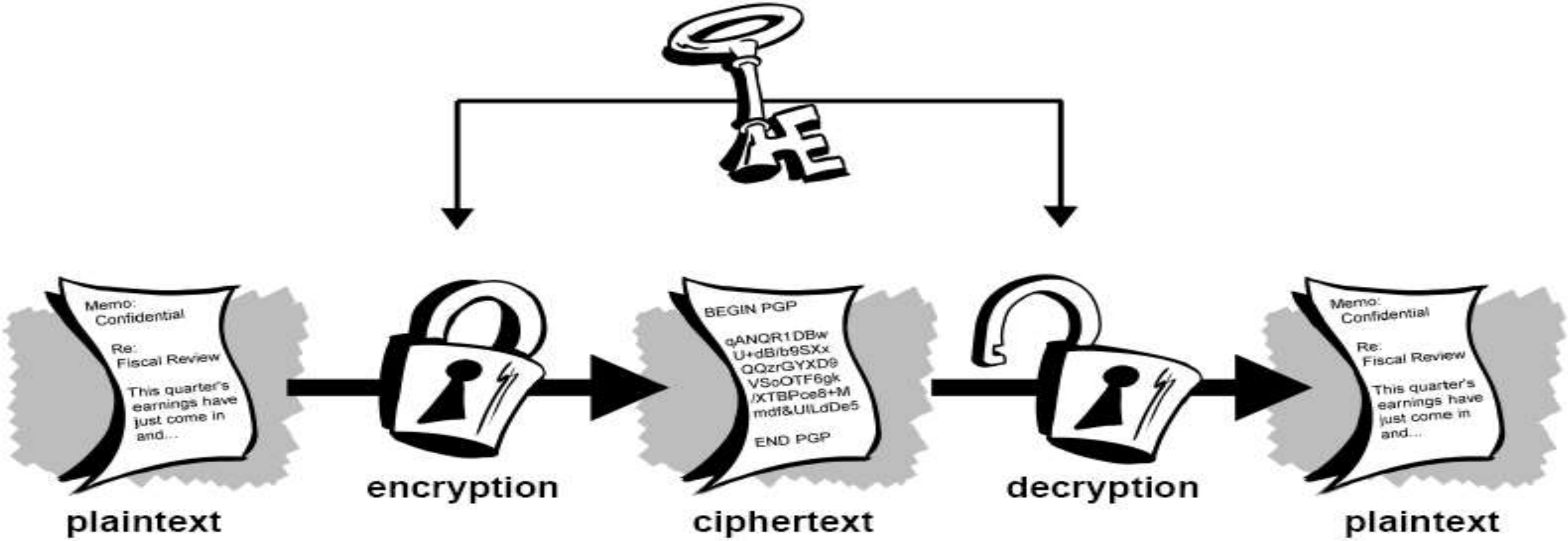
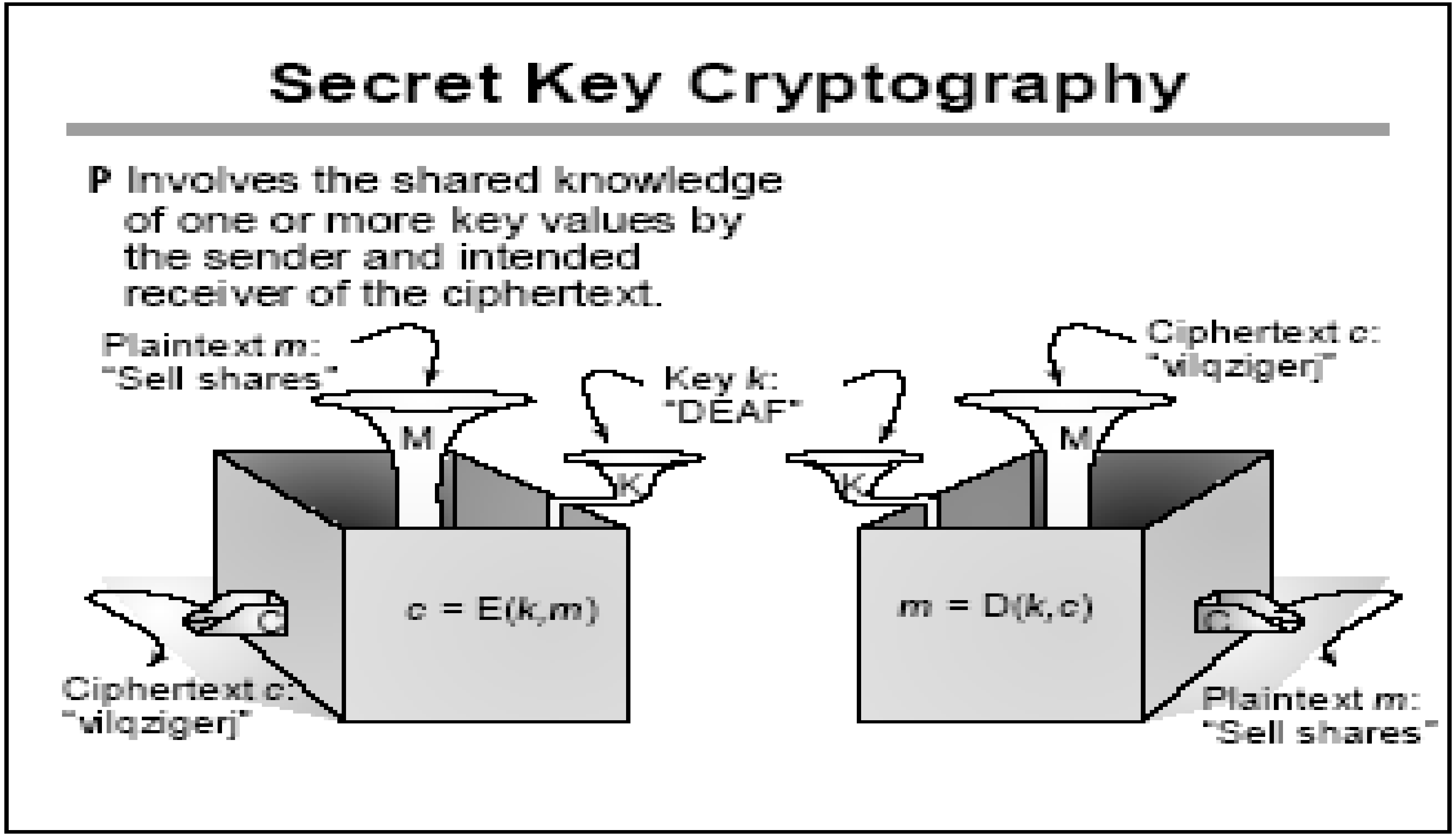
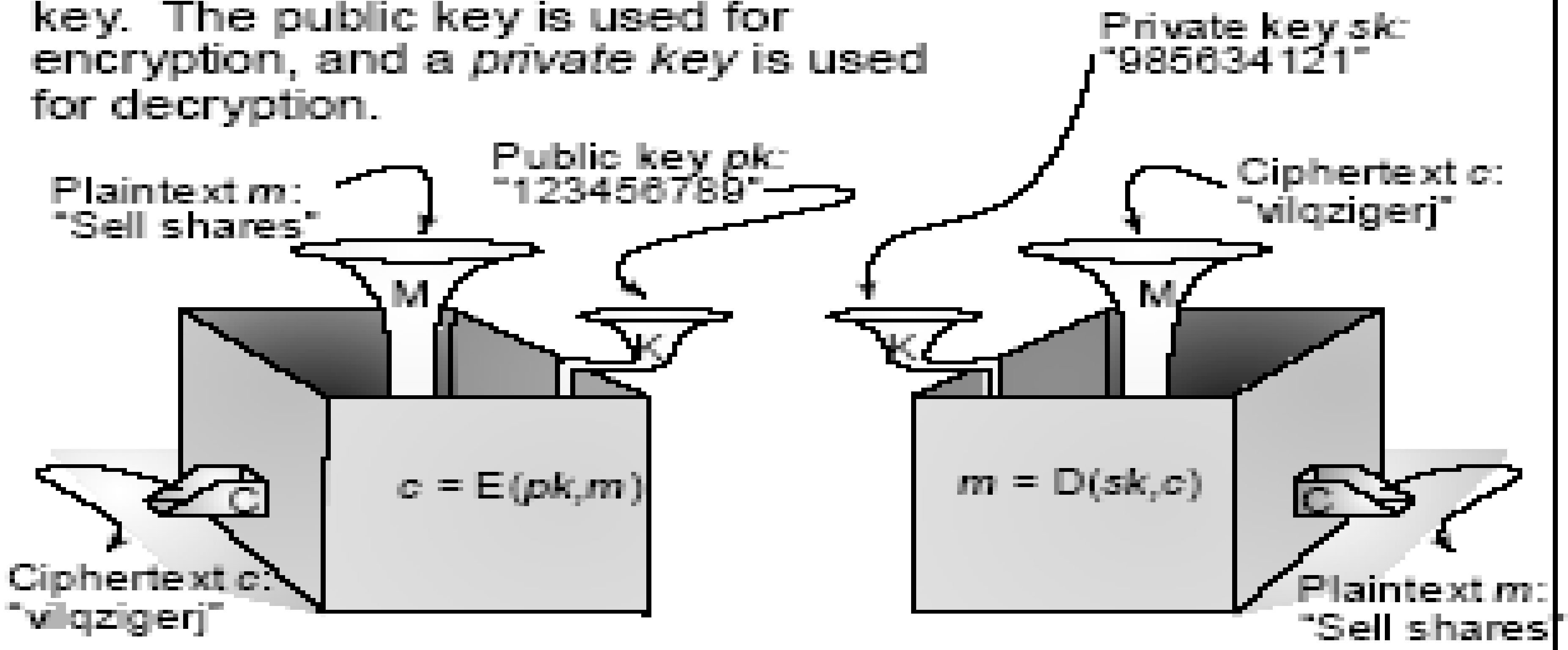


Figure 1-2. Conventional encryption


Secret Key Cryptography
Involves the shared knowledge of one or more key values by the sender and intended receiver of the ciphertext.
Plaintext m:
"Sell shares"
Key k:
"DEAF"
Ciphertext c:
"vilqzigerj"
M
K
c = E(k,m)
C
Ciphertext c:
"vilqzigerj"
M
K
m = D(k,c)
C
Plaintext m:
"Sell shares"

Public Key Cryptography:

- Involves the use of a decryption key that is distinct from the encryption key. The public key is used for encryption, and a *private key* is used for decryption.



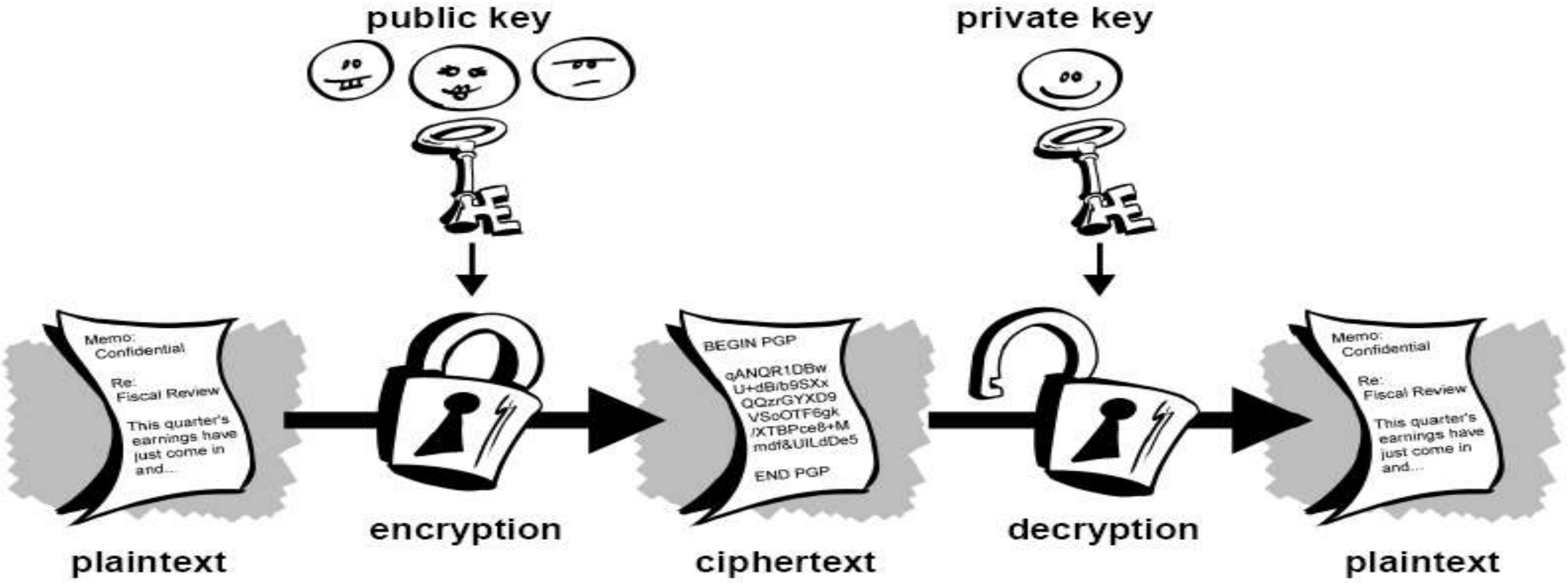
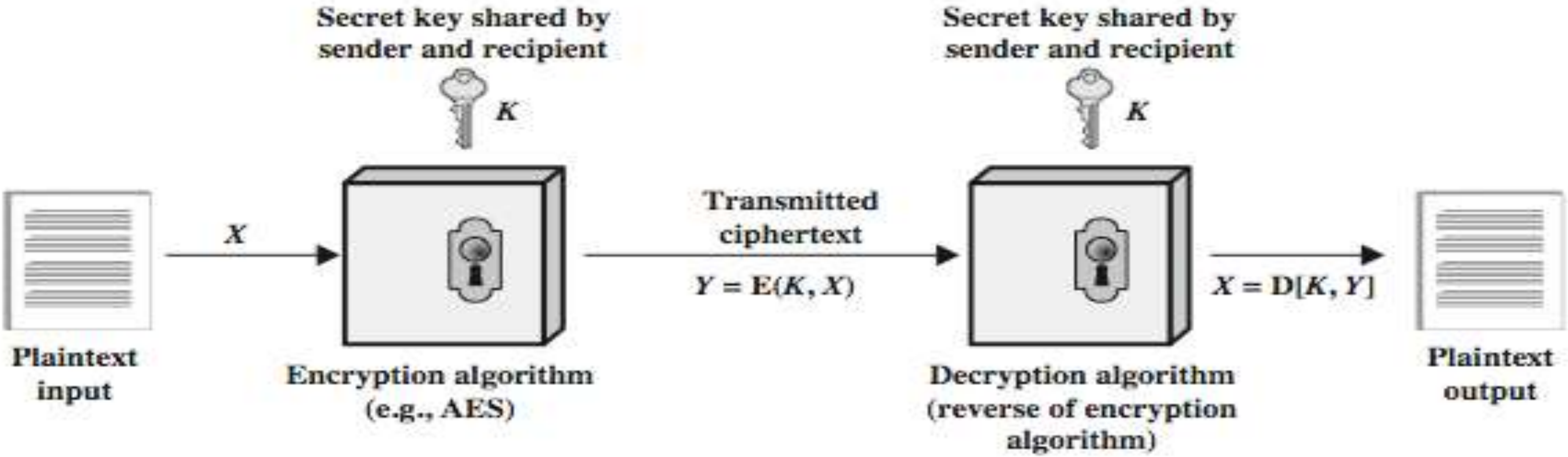


Figure 1-3. Public key encryption

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

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

CRYPTOGRAPHY

can be characterized 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

CRYPTANALYSIS

- **objective to recover key not just message**
- **general approaches:**
  - cryptanalytic attack
  - brute-force attack
- **if either succeed all key use compromised**

TYPES OF CRYPTANALYTIC ATTACKS

1. ciphertext only
   - only know algorithm / ciphertext, statistical, can identify plaintext
2. known plaintext
   - know/suspect plaintext & ciphertext to attack cipher
3. chosen plaintext
   - select plaintext and obtain ciphertext to attack cipher
4. chosen ciphertext
   - select ciphertext and obtain plaintext to attack cipher
5. chosen text
   - select either plaintext or ciphertext to en/decrypt to attack cipher

An encryption scheme: computationally secure if

- The cost of breaking the cipher exceeds the value of encrypted information
- The time required to break the cipher exceeds the useful lifetime of information

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/µs**	**Time required at 10^6 decryptions/µs**
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^{6} years

SUBSTITUTION CIPHERS

A substitution cipher replaces one symbol with another.

Substitution ciphers can be categorized as

- Monoalphabetic ciphers
- Polyalphabetic ciphers.

CIPHERS

Monoalphabetic ciphers: each letter in the plaintext is encoded by only one letter from the cipher alphabet, and each letter in the cipher alphabet represents only one letter in the plaintext.

Polyalphabetic ciphers: each letter in the plaintext can be encoded by any letter in the cipher alphabet, and each letter in the cipher alphabet may represent different letters from the plaintext each time it appears.

Monoalphabetic Ciphers

In monoalphabetic substitution,

the relationship between a symbol in the plaintext

to a symbol in the ciphertext is always one-to-one.

Monoalphabetic Ciphers

Example

The following shows a plaintext and its corresponding ciphertext. The cipher is probably monoalphabetic because both l's (els) are encrypted as O's.

Plaintext: hello **Ciphertext:** KHOOR

Example

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each l (el) is encrypted by a different character.

Plaintext: hello **Ciphertext:** ABNZF

Monoalphabetic Ciphers

Additive Cipher

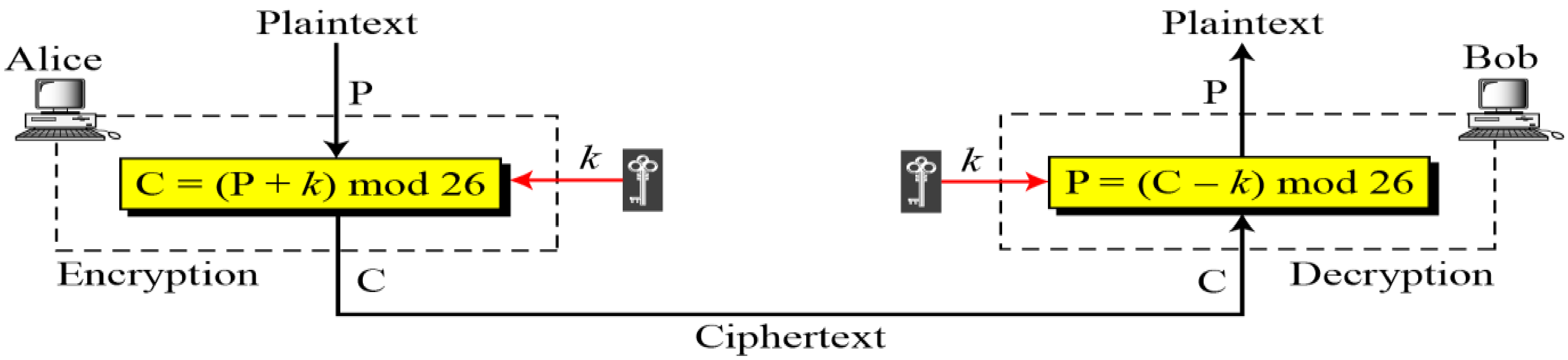
The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a **shift cipher** and sometimes a **Caesar cipher**, but the term additive cipher better reveals its mathematical nature.

Figure . Plaintext and ciphertext in Z_{26}

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Monoalphabetic Ciphers

Figure . Additive cipher



When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26}.

Monoalphabetic Ciphers

Example

Use the additive cipher with **key = 15** to encrypt the message "hello".

Solution

We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h $\rightarrow$ 07	Encryption: $(07 + 15) \bmod 26$	Ciphertext: 22 $\rightarrow$ W
Plaintext: e $\rightarrow$ 04	Encryption: $(04 + 15) \bmod 26$	Ciphertext: 19 $\rightarrow$ T
Plaintext: l $\rightarrow$ 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 $\rightarrow$ A
Plaintext: l $\rightarrow$ 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 $\rightarrow$ A
Plaintext: o $\rightarrow$ 14	Encryption: $(14 + 15) \bmod 26$	Ciphertext: 03 $\rightarrow$ D

Monoalphabetic Ciphers

Example

Use the additive cipher with key = 15 to decrypt the message "WTAAD".

Solution

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

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

Monoalphabetic Ciphers

Shift Cipher and Caesar Cipher

Historically, additive ciphers are called shift ciphers.

Julius Caesar used an additive cipher to communicate with his officers.

For this reason, additive ciphers are sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications.

Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

Monoalphabetic Ciphers

Cryptanalysis

Example

Eve has intercepted the ciphertext "UVACLYFZLJBYL".
Show how she can use a brute-force attack to break the cipher.

Solution

Eve tries keys from 1 to 7. With a key of 7,
the plaintext is "not very secure", which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

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

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
```

PERMUTATION

A permutation of a finite set of elements

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 S :

abc, acb, bac, bca, cab, cba

MONOALPHABETIC CIPHER SECURITY

now have a total of 26! = 4 x 10^{26} keys

with so many keys, might think is secure

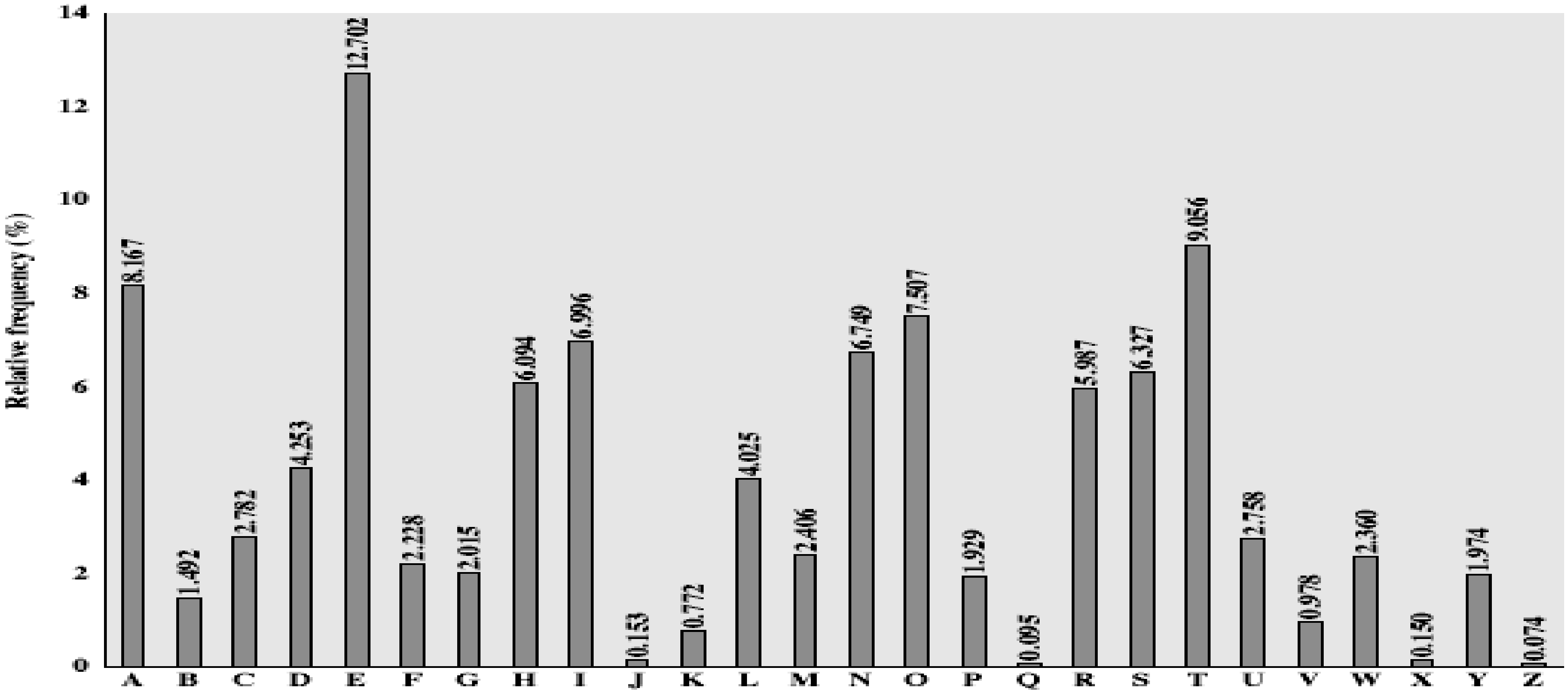
but would be !!!WRONG!!!

problem is language characteristics

LANGUAGE REDUNDANCY AND CRYPTANALYSIS

- human languages are redundant
- eg “computer science department defence road"
- letters are not equally commonly used
- in English e is by far the most common letter
- then T,R,N,I,O,A,S
- other letters are fairly rare Z,J,K,Q,X
- have tables of single, double & triple letter frequencies

ENGLISH LETTER FREQUENCIES



Monoalphabetic Ciphers

Table.1 Frequency of characters in English

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Table .2 Frequency of diagrams and trigrams

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

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

Fill rest of matrix with other letters(minus duplicates)

eg. using the keyword MONARCHY

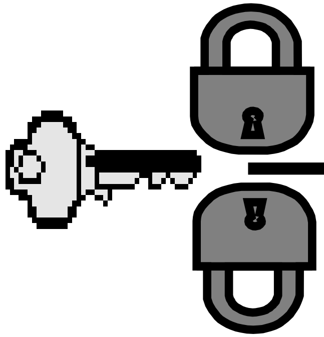
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

ENCRYPTING AND DECRYPTING

plaintext encrypted two letters at a time:

- if a pair is a repeated letter, insert a filler like 'X',
  eg. "balloon" encrypts as "ba lx lo on"
- if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. “ar" encrypts as "RM"
- if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom),
  eg. “mu" encrypts to "CM"
- otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “hs" encrypts to "BP", and “ea" to "IM" or "JM"

SECURITY OF THE 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. US & British military in WW1)

PLAYFAIR EXAMPLE

Using "playfair example" as the keyword, (assuming I and J are interchangeable) the table becomes:

Encrypting the message "Hide the gold in the tree stump":

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

HI DE TH EG OL DI NT HE TR EX ES TU MP

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

HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

BM

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

DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

HI DE TH EG OL DI NT HE TR EX ES TU MP

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

TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

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

EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

HI DE TH EG OL DI NT HE TR EX ES TU MP

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

OL

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

NA

HI DE TH EG OL DI NT HE TR EX ES TU MP

The pair DI forms a rectangle, replace it with BE

The pair NT forms a rectangle, replace it with KU.

The pair HE forms a rectangle, replace it with DM

The pair TR forms a rectangle, replace it with UI

HI DE TH EG OL DI NT HE TR EX ES TU MP

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

EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

The pair ES forms a rectangle, replace it with MO

The pair TU is in a row, replace it with UV

The pair MP forms a rectangle, replace it with IF

FURTHER READING

BOOK: Cryptography and Network Security by William Stallings : chapter 2