Classical Cryptography

- Ancient ciphers have been in use for over 5,000 years
- Already used by ancient Egyptians, Hebrews and Greeks
- Normally they would follow the following scheme:

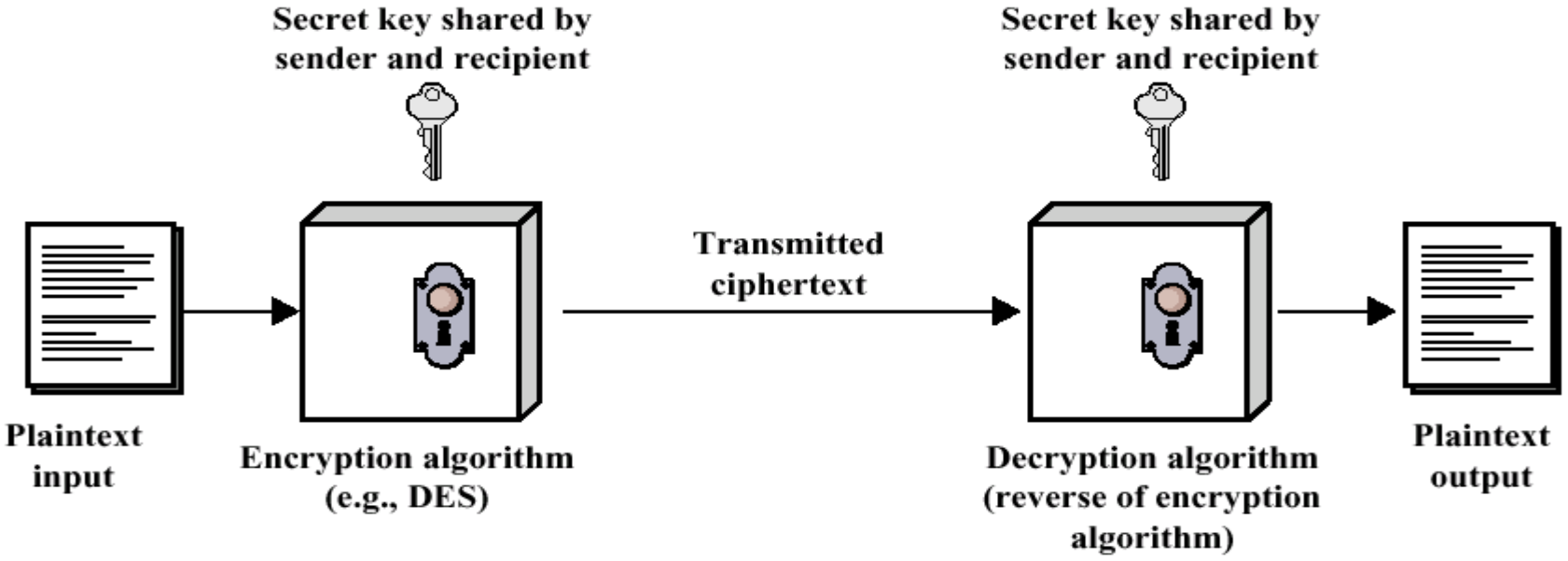

Fig. 3-1: Scheme for ancient ciphers

Caesar Cipher

- 2000 years ago Julius Caesar used a simple substitution cipher, now known as the Caesar cipher

- first attested use in military affairs (*Gallic Wars*)

- replace each letter by 3rd letter on, eg.

```
L FDPH L VDZ L FRQTXHUHG ->
I CAME I SAW I CONQUERED
```

- can describe this mapping (or **translation alphabet**) as:

```
Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC
```

Generalised Caesar Cipher

- more generally can use any shift from 1 to 25
- ie. replace each letter of message by a letter a fixed distance away
- specify **key letter** as the letter a plaintext A maps to
  - e.g. a key letter of **F** means
  - A maps to F, B to G, ... Y to D, Z to E
  - e.g. shift letters by 5 places
- hence have 26 (25 useful) ciphers

Mixed Monoalphabetic Substitution Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- or even to 26 arbitrary symbols
- hence key is 26 letters long
- this is known as a **Monoalphabetic Substitution Cipher**
- Example based on key:

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	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

Generalised Mixed Monoalphabetic Substitution Cipher

- have a total of 26! ~ 4 x 10^{26} keys!
- but … can be cracked through frequency analysis:

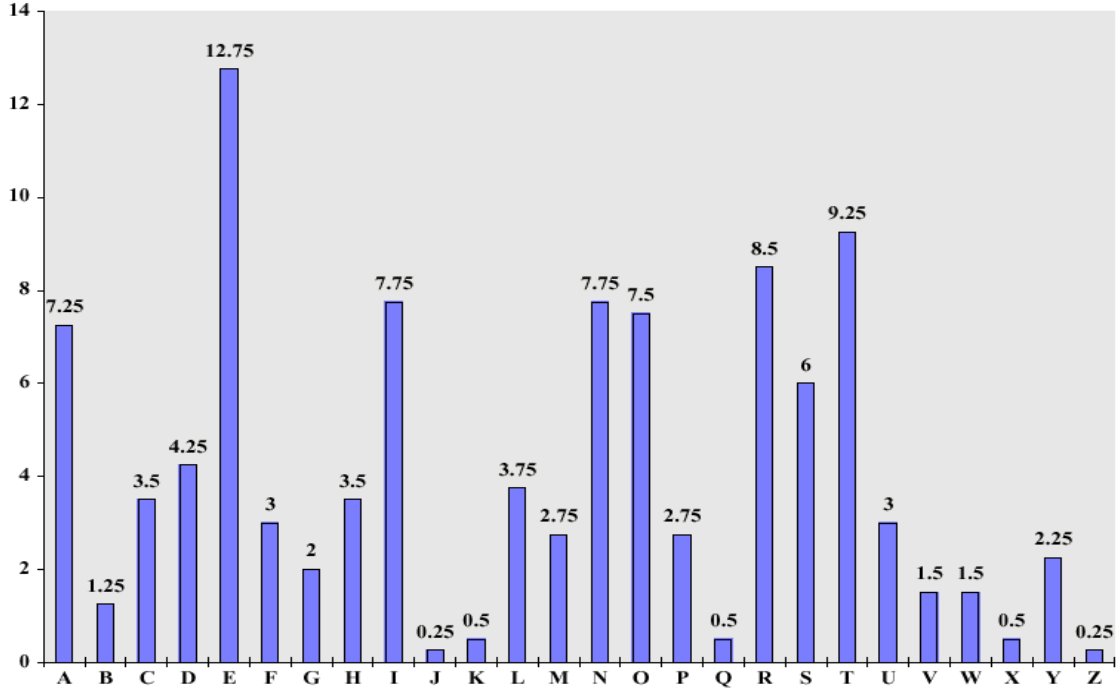

Fig. 3-2: Typical distribution of letters in a text

Playfair Cipher

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

How it works:

1. Create a 5x5 grid of letters with a keyword
2. Letters are encrypted in pairs
3. Repeats have an x inserted *balloon -> ba lx lo on*
4. Letters that fall in the same row are each replaced with the letter on the right (*ok* becomes *gm*)
5. Letters in the same column are replaced with the letter below (*fo* becomes *ou*)
6. Otherwise each letter gets replaced by the the letter in its row but in the other letters column (*qm* becomes *th*)

The cipher text has less structure than the plain text.

But again … Playfair can be cracked through frequency analysis of pairs.

Vigenère Cipher

- Blaise de Vigenère is generally credited as the inventor of the "polyalphabetic substitution cipher"
- To improve security use **many** monoalphabetic substitution alphabets
- Hence each letter can be replaced by many others
- Use a key to select which alphabet is used for each letter of the message
- i^{th} letter of key specifies i^{th} alphabet to use
- Use each alphabet in turn
- Repeat from start after end of key is reached

Vigenère Example

- Write the plaintext out and under it write the keyword repeated
- Then using each key letter in turn as a Caesar cipher key
- Encrypt the corresponding plaintext letter

Plaintext	THISPROCESSCANALSOBEEXPRESSED
Keyword	CIPHERCIPHERCIPHERCIPHERCIPHE
Ciphertext	VPXZTIQKTZWTCVPSWFDMTETIGAHLH

- In this example have the keyword "CIPHER". Hence have the following translation alphabets:

```
C -> CDEFGHIJKLMNOPQRSTUVWXYZAB
I -> IJKLMNOPQRSTUVWXYZABCDEFGH
...          ...
     ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

to map the above plaintext letters.

Rotor Ciphers

- A N-stage polyalphabetic substitution algorithm modulo 26
- 26^N steps before a repetition (N = 5 cylinders == 11881376 steps)

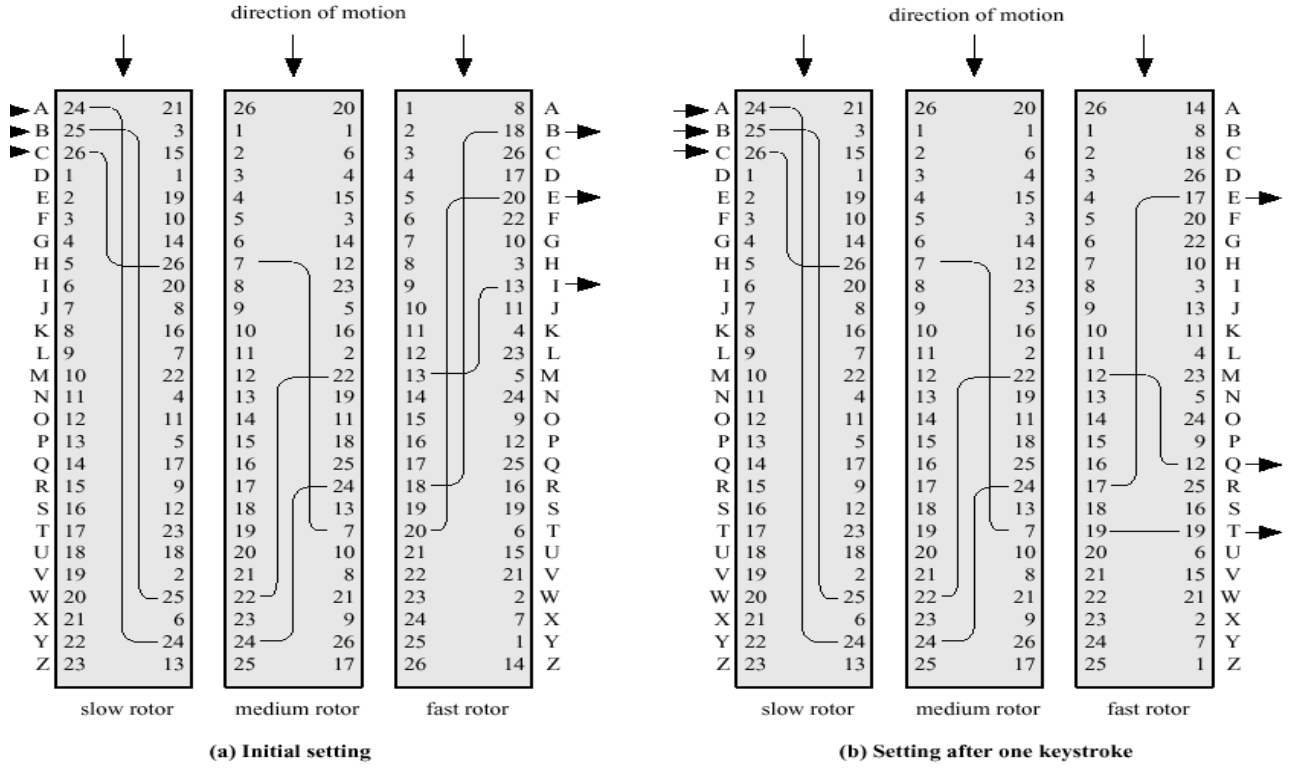

Fig. 3-3: Example for a rotor cipher

Transposition (or Permutation) Ciphers

- Substitution provides only part of the answer
- Transposition will scramble a message
- IWOULDRATHERBESOMEWHEREELSENOW could be rewritten as

  IWOUL
  DRATH
  ERBES
  OMEWH
  EREEL
  SENOW

  And reordered IDEOESWRRMREOABEENUTEWEOLHSHLW
- There are many ways to do a transposition
- But … transposition can be cracked as well

Product Ciphers

Problem: ciphers based on just substitutions or transpositions are not secure,

But: a substitution followed by a transposition makes a new much harder cipher

Product ciphers

- are substitution-transposition combinations chained together
- are generally far too hard to be processed manually
- are the basis for many modern block cipher algorithms