JLOBP BZOBQ ZLABP

Secret Codes in Computing

We know that:

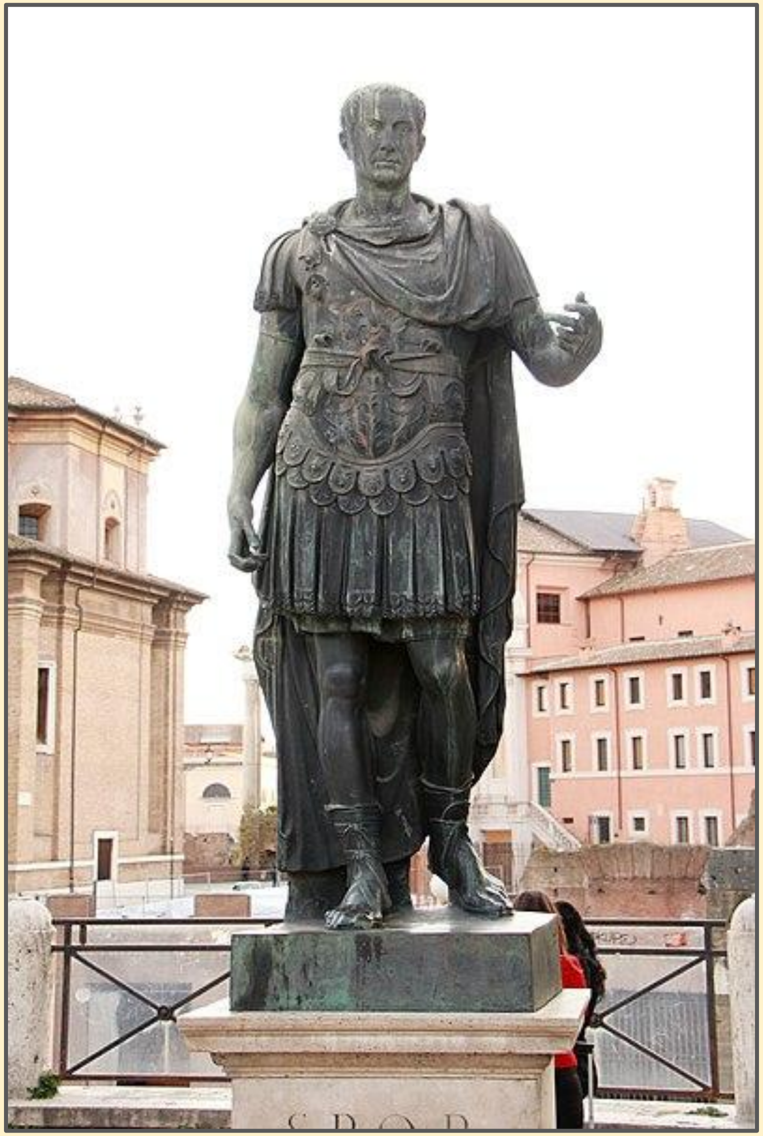
- secret codes are used in computing
- there are all sorts of thing we don’t want other people to know
- data stored on computers is encrypted so that people can’t read it
- substitution ciphers are easy to break

SBKF SFAF SFZF

Secret Codes in Computing

This is a very ancient type of substitution cipher

It is named after -->



Secret Codes in Computing

The **caesar cipher** shifts letters along the alphabet.

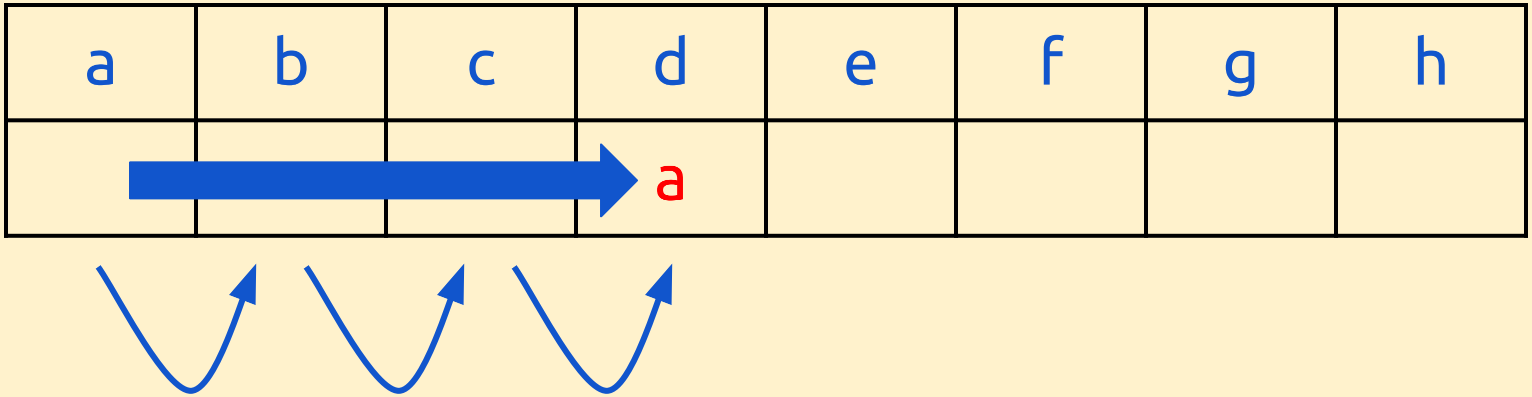
The number of places each letter is **shifted** is agreed beforehand.

a	b	c	d	e	f	g	h

Secret Codes in Computing

The caesar cipher shifts letters along the alphabet.

With a **shift of 3** places, **d** is written as **a**



a	b	c	d	e	f	g	h
			a				

Secret Codes in Computing

The caesar cipher shifts letters along the alphabet.

With a **shift of 3** places, **d** is written as **a**

e is written as **b**, **c** as **f** etc...

a	b	c	d	e	f	g	h
			a	b	c	d	

Secret Codes in Computing

a	b	c	d	e	f	g	h	i	j	k	l	m
			a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	t	u	v	w

So, **z** becomes **w**. Then what do we do?

Secret Codes in Computing

a	**b**	**c**	d	e	f	g	h	i	j	k	l	m
x	**y**	**z**	a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	y	u	v	w

We continue at the start of the alphabet.

So, **a** becomes **x** etc…

How many possible shifts are there?

Secret Codes in Computing

The **shift** is the number of places along the alphabet that each letter is moved (or “shifted”)

If you know the shift it’s easy to work out the meaning of the code.

Secret Codes in Computing

A shift of 3 moves each letter 3 places

a	b	c	d	e	f	g	h
			a	b	c	d	e

Secret Codes in Computing

A shift of 3 moves each letter 3 places

a	b	c	d	e	f	g	h
			a	b	c	d	e

A shift of 5 moves each letter 5 places

a	b	c	d	e	f	g	h
					a	b	c

Secret Codes in Computing

A shift of 3 moves each letter 3 places

a	b	c	d	e	f	g	h
x	y	z	a	b	c	d	e

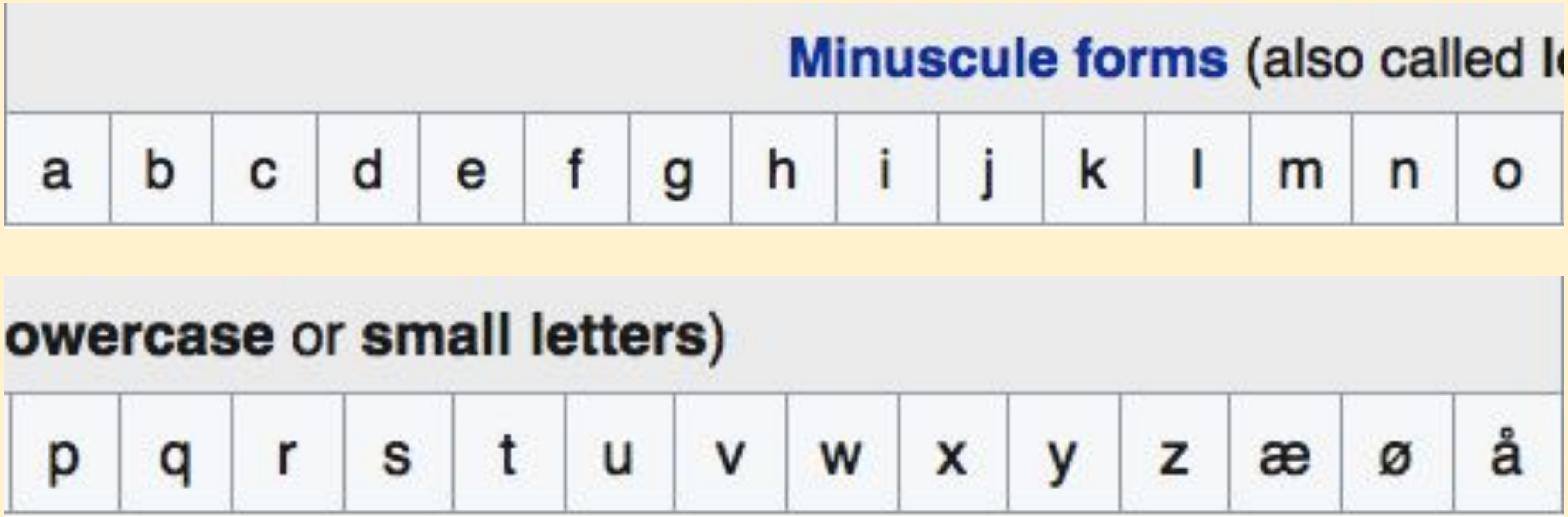
A shift of 5 moves each letter 5 places

a	b	c	d	e	f	g	h
v	w	x	y	z	a	b	c

What’s the maximum shift possible?

Secret Codes in Computing

Not every language has 26 letters...



Minuscule forms (also called lowercase or small letters)																												
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	æ	ø	å

Secret Codes in Computing

a	b	c	d	e	f	g	h	i	j	k	l	m
x	y	z	a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	y	u	v	w

To **encrypt**, find the **plaintext** letter on the top and write down the letter below it as the **ciphertext**

u becomes **r** in code with a **shift of 3**

Secret Codes in Computing

a	b	c	d	e	f	g	h	i	j	k	l	m
x	y	z	a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	y	u	v	w

romans

oljxkp

Secret Codes in Computing

a	b	c	d	e	f	g	h	i	j	k	l	m
x	y	z	a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	y	u	v	w

To decode, find the letter on the bottom and look up

o decoded with a shift of 3 is **r**

Secret Codes in Computing

a	b	c	d	e	f	g	h	i	j	k	l	m
x	y	z	a	b	c	d	e	f	g	h	i	j

n	o	p	q	r	s	t	u	v	w	x	y	z
k	l	m	n	o	p	q	r	s	y	u	v	w

Can you decode:

a. pbjxmelob

b. xii olxap ibxa ql oljb

JLOBP BZOBQ
ZLABP

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

Shift is 3

SBKF SFAF SFZF

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

Shift is 3

Secret Codes in Computing

Caesar ciphers **shift** each letter of the alphabet along a set number of places.

This creates an easy to use code - but one which is also easy to crack simply by trying each possibility.

It was used by the Romans, but many of the people they were trying to hide messages from couldn’t read or write anyway!