



Cesar Cipher - the oldest cryptosystem

*A shift* cipher – attributed to Julius Caesar (100-44 BC)

MEET ME AFTER THE TOGA PARTY

PHHW PH DIWHU WKH WRJD SDUWB

Shift the alphabet 23 places to the right and substitute 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

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 - the oldest cryptosystem

A *shift* cipher – attributed to Julius Caesar (100-44 BC)

MEET ME AFTER THE TOGA PARTY

PHHW PH DIWHU WKH WRJD SDUWB

Shift the alphabet 23 places to the right and substitute 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
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

# Representing data as numbers

Cryptographic algorithms are mathematical operations

- ➡ messages and keys must be represented as numbers  
for instance : ASCII encoding