Representing data as numbers

Cryptographic algorithms are mathematical operations

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

Back to Caesar Cipher

Algorithm : shift the alphabet of a certain number of positions

Key : the number of positions to shift

Key space : 25 possible rotations (~ 5 bits security)

Encoding :

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

Encrypting and decrypting one character is obtained as follows:

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

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