

Caesar Cipher

- Example:** suppose the key for a *shift cipher is $K = 13$* and the plaintext is

we go to INU



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

Plain text	w	e	g	o	t	o	i	n	u
Sequence	22	4	6	14	19	14	8	13	20
Cipher sequence ($p + 13$) mod 26	9	17	19	1	6	1	21	0	7
Cipher text	j	r	t	b	g	b	v	a	h

Cipher text: jrtbgbvah

Caesar Cipher

- **Example:** suppose the key for a **shift cipher is $K = 13$** and the chipper text is:

Chipper text: jrtbgbvah

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

Chipper text	<u>i</u>	<u>r</u>	<u>t</u>	<u>b</u>	<u>g</u>	<u>b</u>	<u>v</u>	<u>a</u>	<u>h</u>
Sequence	<u>9</u>	<u>17</u>	19	1	6	1	21	0	<u>7</u>
Plain sequence	$(9-13) \bmod 26$	4	6	14	19	14	8	13	20
$(c - 13) \bmod 26$	22	$-4 \bmod 26 \rightarrow$							
Cipher text	w	e	g	o	t	o	i	n	u

plain text: we go to inu

$$-4 = -1 \times 26 + 22$$