Chapter 16

Cryptology

Modular Arithmetic Cryptology[Julius Caesar to 1980]

Firstly, we set up a correspondence between the letters of the alphabet and the numbers $0, 1, 2, \cdots, 25$. Thus

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Let x be a plaintext letter and y be the corresponding ciphertext letter.
Julius Caesar's method is to take y to satisfy

$$y \equiv x + 3 \,(\text{mod } 26)\,.$$

To decipher, one uses that

$$x \equiv y - 3 \,(\text{mod } 26)\,.$$

We divide the message into groups of 5 letters.

Example 16.1 (Enciphering)**.**

	J	U	L	I	U	S		C	A	E	S	A	R		plaintext
→	J	U	L	I	U		S	C	A	E	S		A	R	
→	9	20	11	8	20		18	2	0	4	18		0	17	
→	12	23	14	11	23		21	5	3	7	21		3	20	
→	M	X	O	L	X		V	F	D	H	V		D	U	ciphertext