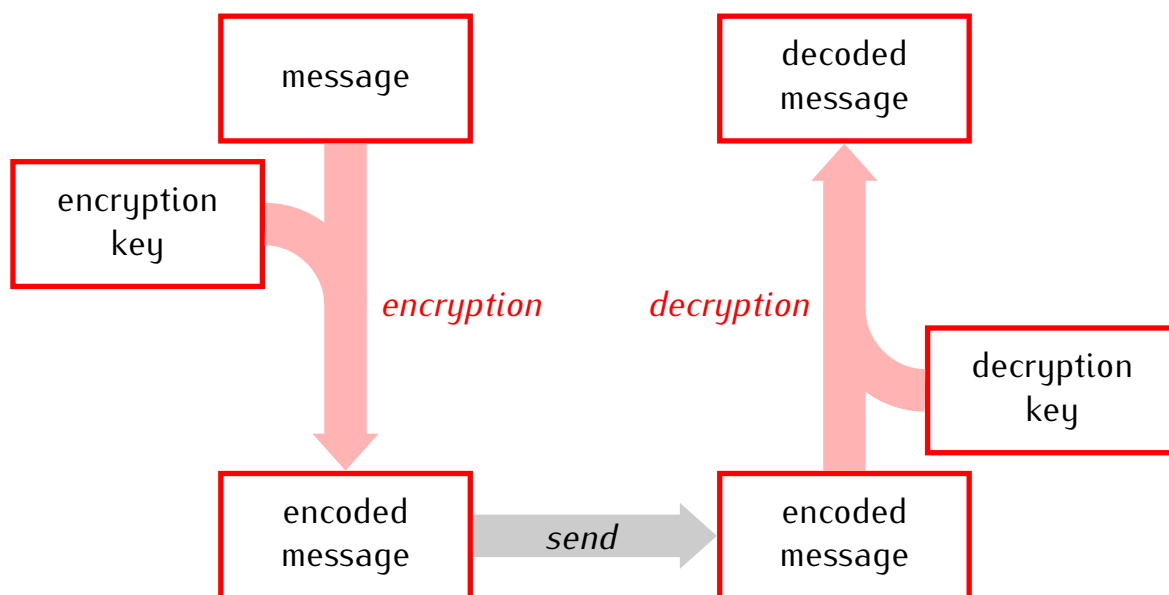


### Ciphers.

Cipher is an algorithm for encrypting and decrypting data to conceal its meaning.

#### Basic working scheme of ciphers



**Substitution cipher:** Replace each letter of the alphabet by some other letter.

**Example.**

encrypt ↓	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	↑ decrypt
	T	V	W	X	Y	S	C	N	O	U	Z	A	B	P	I	M	J	Q	R	K	D	E	F	G	H	L	
encryption/decryption key																											

message: TOP SECRET

**Hill cipher:** Use matrix multiplication

**Example.**

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 1 \\ 2 & 0 & -1 \end{bmatrix}$$

encryption key                      decryption key  
invertible matrix                      matrix inverse

message: TOP SECRET

**Encryption:**

1) Replace letters by numbers:

_	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	26

2) Since the key is a  $3 \times 3$  matrix split the number sequence numbers in vectors with 3 entries each.

3) Multiply each vector by the encryption matrix  $A$ .

4) Write the new vectors as a sequence of numbers.

**We can do better**, but the next part will not work with an arbitrary invertible matrix  $A$ . It will work though e.g. if all entries of  $A$  and  $A^{-1}$  are integers.

5) Reduce all numbers obtained in step 4 modulo 27. That is, add or subtract from each number a multiple of 27 to get a number between 0 and 26.

6) Replace numbers by letters.

### **Decryption.**

1) Replace letters by numbers, split into vectors, and multiply each vector by  $A^{-1}$

2) Write the new vectors as a sequence of numbers, reduce each number modulo 27.

3) Replace numbers by letters