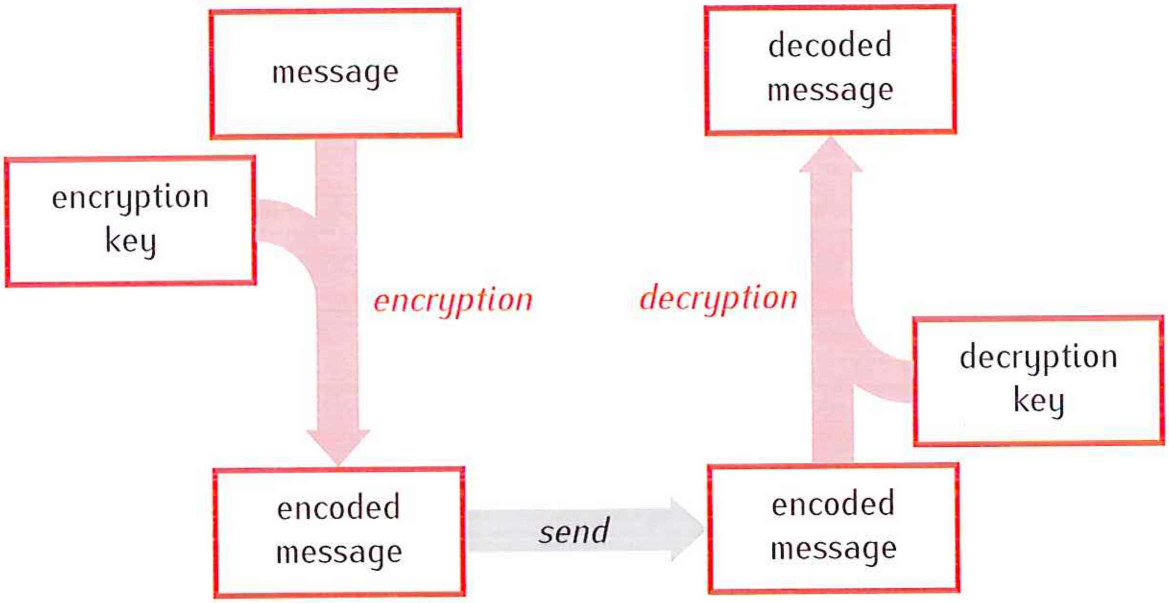
Ciphers.

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
	K	V	W	X	Y	S	C	N	O	U	Z	A	B	P	I	M	J	Q	R	T	D	E	F	G	H	L	

encryption/decryption key

message: TOP SECRET

encryption: TOP SECRET

↓

TIM RYWQYT

Problem: Very easy to break by looking at letter frequencies and patters.

Hill cipher: Use matrix multiplication

Example.

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

encryption key
invertible matrix

decryption key
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 × 3 matrix split the number sequence numbers in vectors with 3 entries each.

added to get a vector

$$\begin{array}{cccccccccccc} T & O & P & \_ & S & E & C & R & E & T & X & X \\ 20 & 15 & 16 & 0 & 19 & 5 & 3 & 18 & 5 & 20 & 24 & 24 \end{array}$$

$$\underbrace{20\ \ 15\ \ 16}\ \ \underbrace{0\ \ 19\ \ 5}\ \ \underbrace{3\ \ 18\ \ 5}\ \ \underbrace{20\ \ 24\ \ 24}$$

$$\begin{bmatrix} 20 \\ 15 \\ 16 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 19 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 3 \\ 18 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 20 \\ 24 \\ 24 \end{bmatrix}$$

3) Multiply each vector by the encryption matrix A.

$$A \cdot \begin{bmatrix} 20 \\ 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 31 \\ 35 \\ 46 \end{bmatrix}$$

$$A \cdot \begin{bmatrix} 0 \\ 19 \\ 5 \end{bmatrix} = \begin{bmatrix} 24 \\ 19 \\ 43 \end{bmatrix}, \quad A \cdot \begin{bmatrix} 3 \\ 18 \\ 5 \end{bmatrix} = \begin{bmatrix} 23 \\ 21 \\ 41 \end{bmatrix}, \quad A \cdot \begin{bmatrix} 20 \\ 24 \\ 24 \end{bmatrix} = \begin{bmatrix} 48 \\ 44 \\ 72 \end{bmatrix}$$

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

$$\begin{array}{cccccccccccc} T & O & P & \_ & S & E & C & R & E & T & X & X \\ 31, & 35, & 46, & 24, & 19, & 43, & 23, & 21, & 41, & 48, & 44, & 72 \end{array}$$

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.

31 35 46 24 19 43 23 21 41 48 44 72

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.

$31-27=4$

$35-27=8$

$46-27=19$

$24=24$

$19=19$

$43-27=16$

$23=23$

$21=21$

$41-27=14$

$48-27=21$

$44-27=17$

$72-2\cdot 27=18$

6) Replace numbers by letters.

4	8	19	24	19	16	23	21	14	21	17	18
D	H	S	X	S	P	W	U	N	U	Q	R
T	O	P	_	S	E	C	R	E	T	X	X

Decryption.

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

$$A^{-1}\cdot\begin{bmatrix}4\\8\\19\end{bmatrix}=\begin{bmatrix}1&1&-1\\-1&0&1\\2&0&-1\end{bmatrix}\cdot\begin{bmatrix}4\\8\\19\end{bmatrix}=\begin{bmatrix}-7\\15\\-11\end{bmatrix}$$

$$A^{-1}\begin{bmatrix}24\\19\\16\end{bmatrix}=\begin{bmatrix}27\\-8\\32\end{bmatrix},\quad A^{-1}\begin{bmatrix}23\\21\\14\end{bmatrix}=\begin{bmatrix}30\\-9\\32\end{bmatrix}$$

$$A^{-1}\begin{bmatrix}21\\17\\18\end{bmatrix}=\begin{bmatrix}20\\-3\\24\end{bmatrix}$$

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

−7 15 −11 27 −8 32 30 −9 32 20 −3 24

↓ mod 27

20 15 16 0 19 5 3 18 5 20 24 24

↓

3) Replace numbers by letters

T O P _ S E C R E T X X