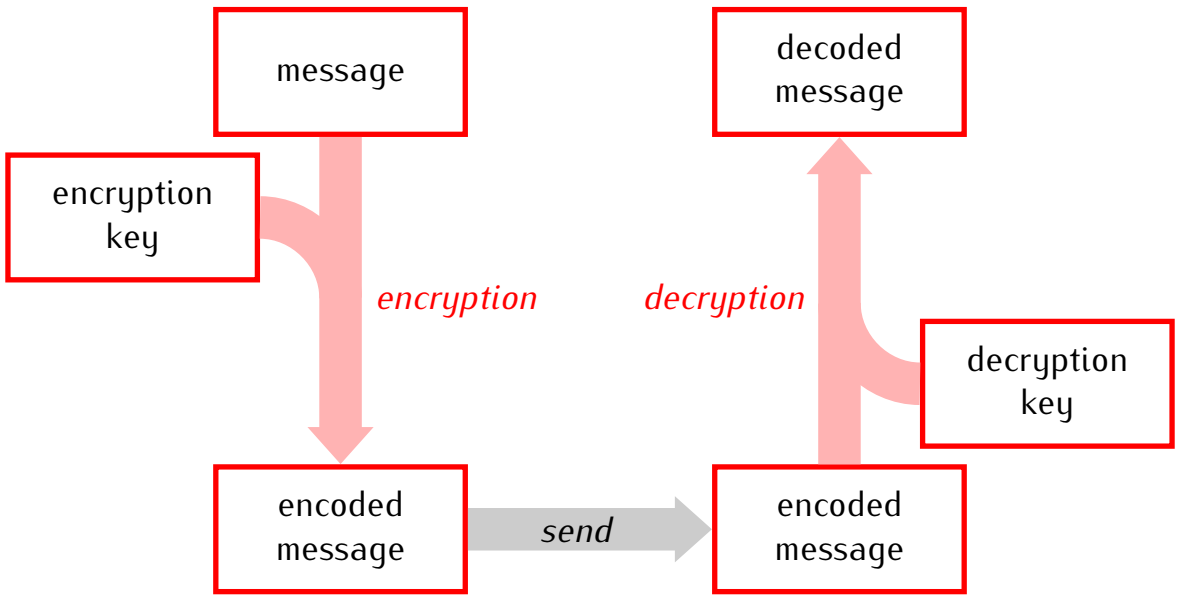
Ciphers.

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
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

↑ decrypt

encryption/decryption key

message: TOP SECRET

encryption: TOP SECRET
↓
KIB RYWQYK

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

Hill cipher: Use matrix multiplication

Example.

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

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

added to get a vector

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

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

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

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

3) Multiply each vector by the encryption matrix A.

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

$$A \cdot \begin{bmatrix} 9 \\ 19 \\ 5 \end{bmatrix} = \begin{bmatrix} 24 \\ 19 \\ 43 \end{bmatrix}, \quad A \cdot \begin{bmatrix} 3 \\ 18 \\ 5 \end{bmatrix} = \begin{bmatrix} 23 \\ 21 \\ 41 \end{bmatrix} \quad A \cdot \begin{bmatrix} 20 \\ 24 \\ 24 \end{bmatrix} = \begin{bmatrix} 48 \\ 44 \\ 72 \end{bmatrix}$$

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

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

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

Decryption.

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

1) Split the sequence of numbers into vectors and multiply each vector by A^{-1}

$$\begin{bmatrix}31\\35\\46\end{bmatrix} \quad \begin{bmatrix}24\\19\\43\end{bmatrix} \quad \begin{bmatrix}23\\21\\41\end{bmatrix} \quad \begin{bmatrix}48\\44\\72\end{bmatrix}$$

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

$$A^{-1}\cdot\begin{bmatrix}24\\19\\43\end{bmatrix} = \begin{bmatrix}0\\19\\5\end{bmatrix}$$

$$A^{-1}\cdot\begin{bmatrix}23\\21\\41\end{bmatrix} = \begin{bmatrix}3\\18\\5\end{bmatrix}$$

$$A^{-1}\cdot\begin{bmatrix}48\\44\\72\end{bmatrix} = \begin{bmatrix}20\\24\\24\end{bmatrix}$$

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

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

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

3) Replace numbers by letters:

_	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