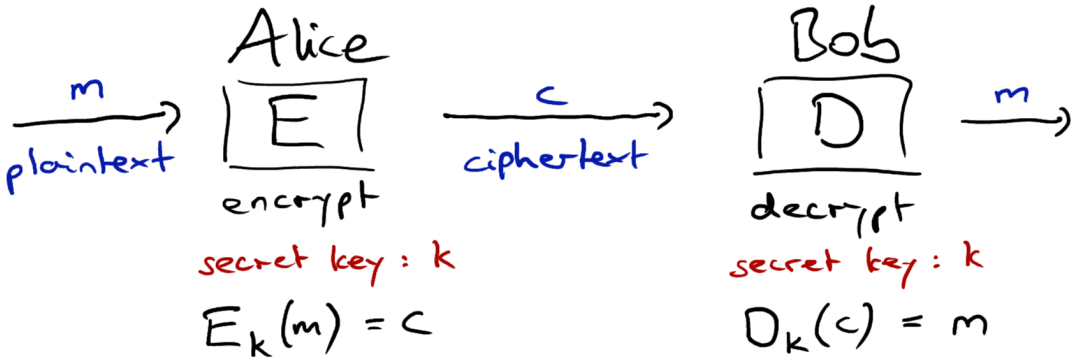
Historical ciphers

symmetric encryption

A, B share same secret key k from some key space



secret key : k

$E_k(m) = c$

secret key : k

$D_k(c) = m$

goals secure messaging against

- eavesdropping (confidentiality)
- tampering (integrity, authenticity)

historical examples

alphabet A-Z identified with 0...25

EG D ↔ 3

shift cipher encrypt each character x

$$E_k(x) = x + k \pmod{26}$$

Caesar $k = 3$

$k = 13$?!

EG m = HELLO, $k = 1$, $E_k(m)$ = IFMMP

key space size 26 = $\{0, 1, \ldots, 25\}$ (0: not a good key)

affine cipher slight upgrade with

$$E_k(x) = ax + b \pmod{26}$$

$k = (a, b)$

Exercise $D_k(x)$? size of key space ?

Vigenere cipher

m = HOLIDAY

\+ BADBADB...

k = BAD (1 0 3)

c = IOOJDDZ