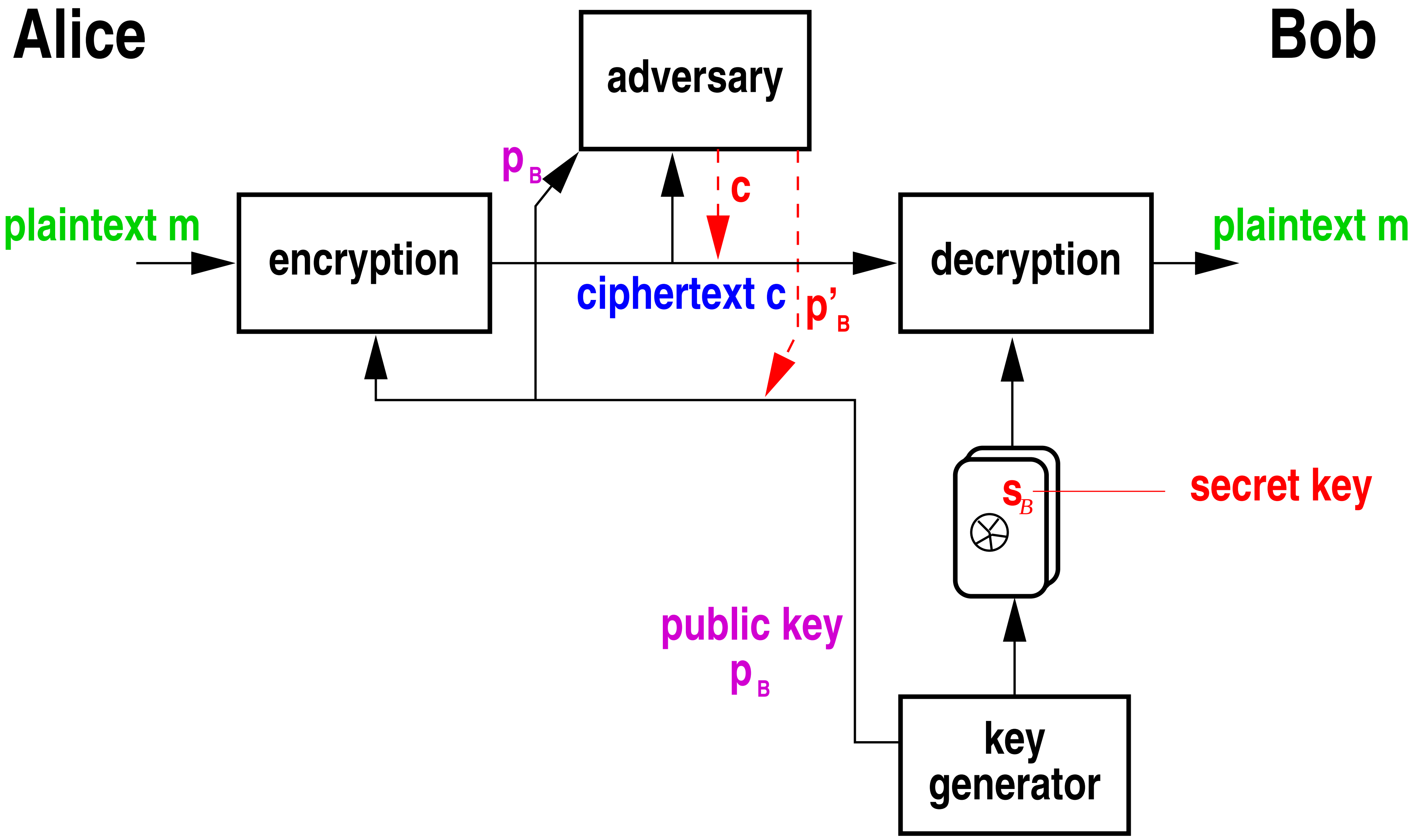
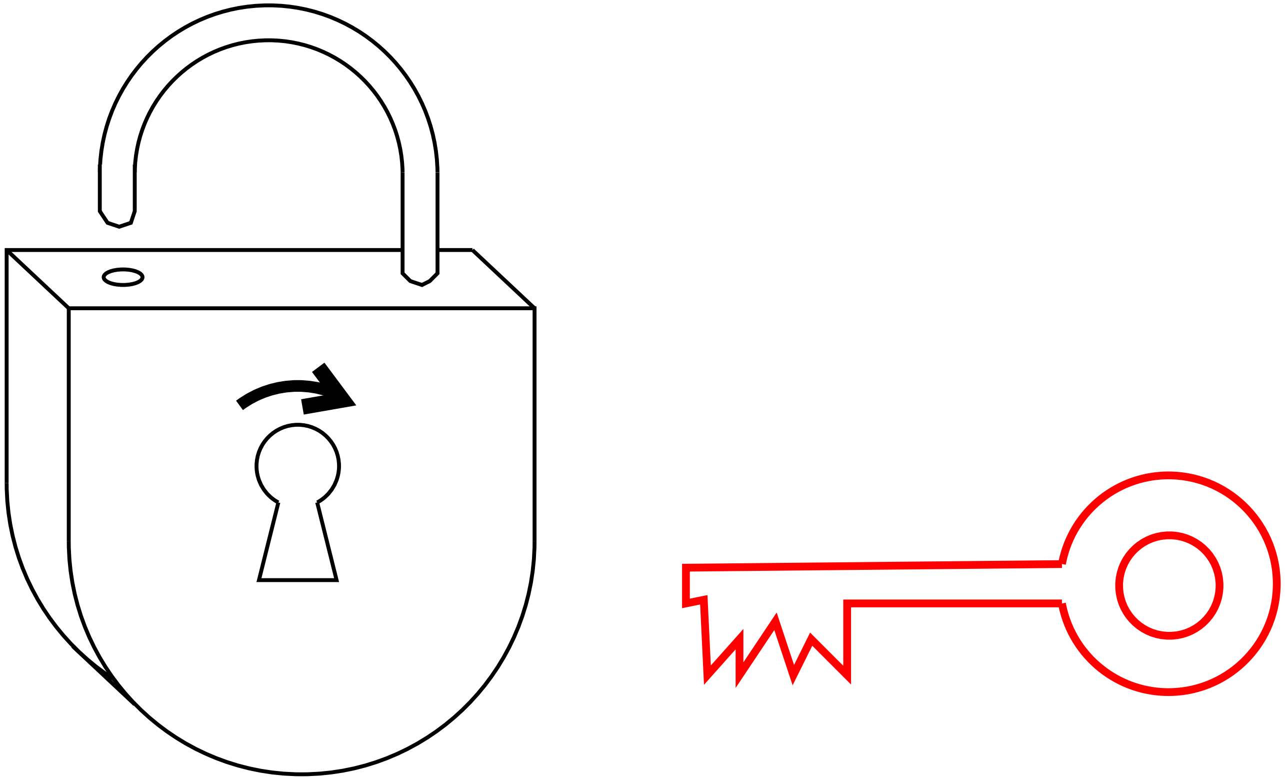
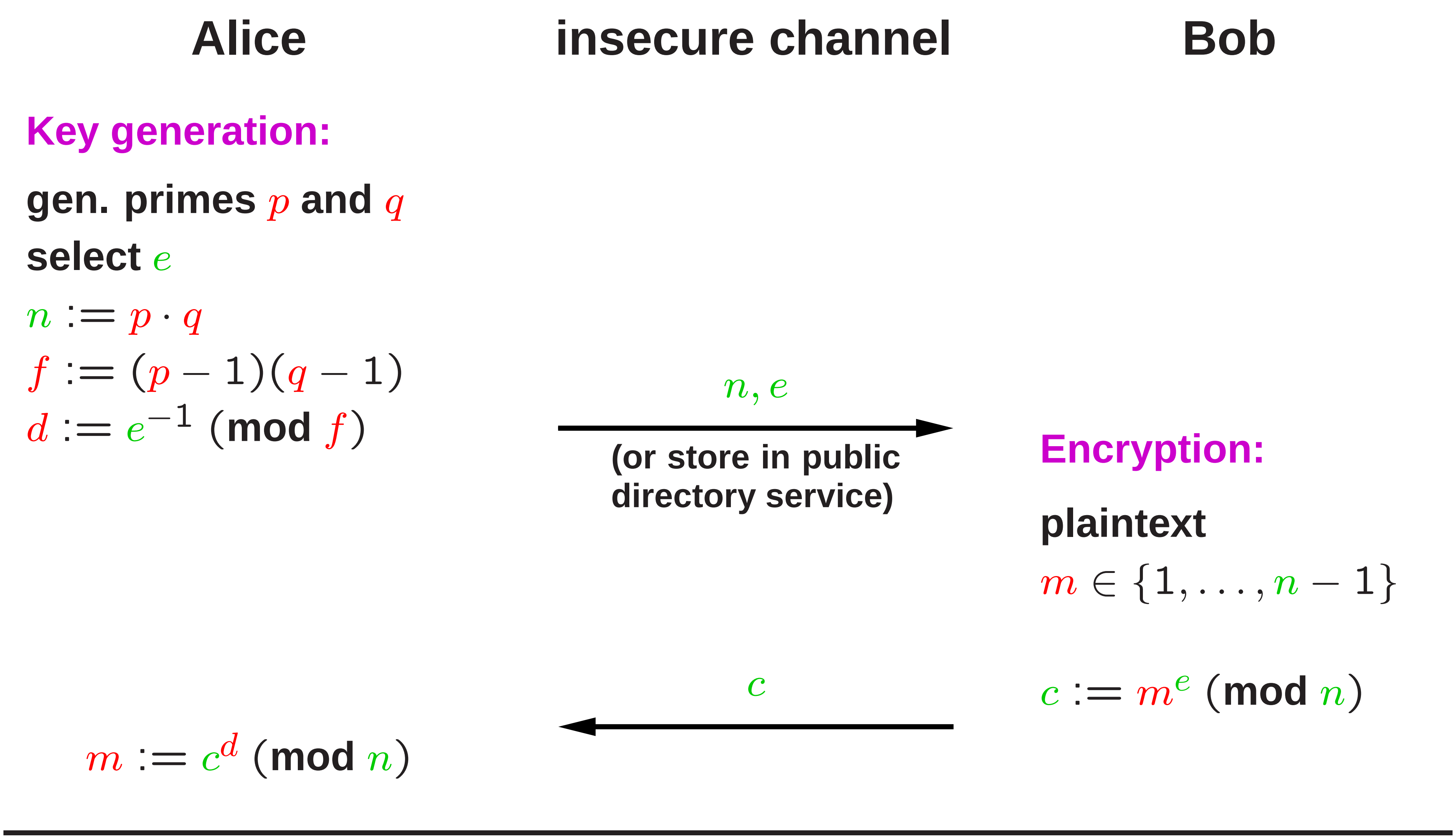
Public-key cryptosystem



Public-key cryptosystem: Mechanical analog



RSA public-key cryptosystem



Alice

insecure channel

Bob

Key generation:

gen. primes p and q

select e

$n := p \cdot q$

$f := (p-1)(q-1)$

$d := e^{-1} \pmod{f}$

n, e

(or store in public directory service)

Encryption:

plaintext

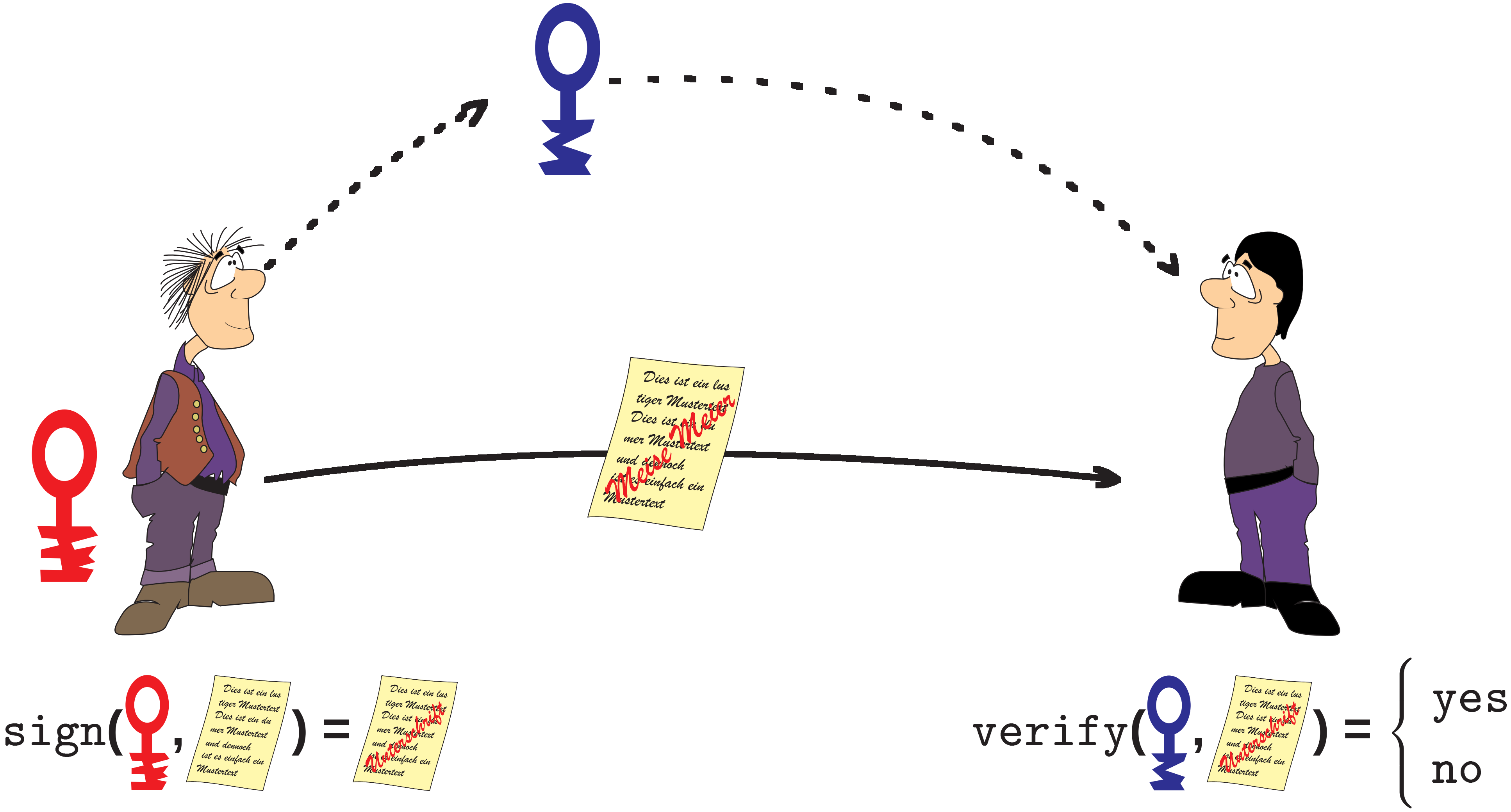
$m \in \{1, \ldots, n-1\}$

$c := m^e \pmod{n}$

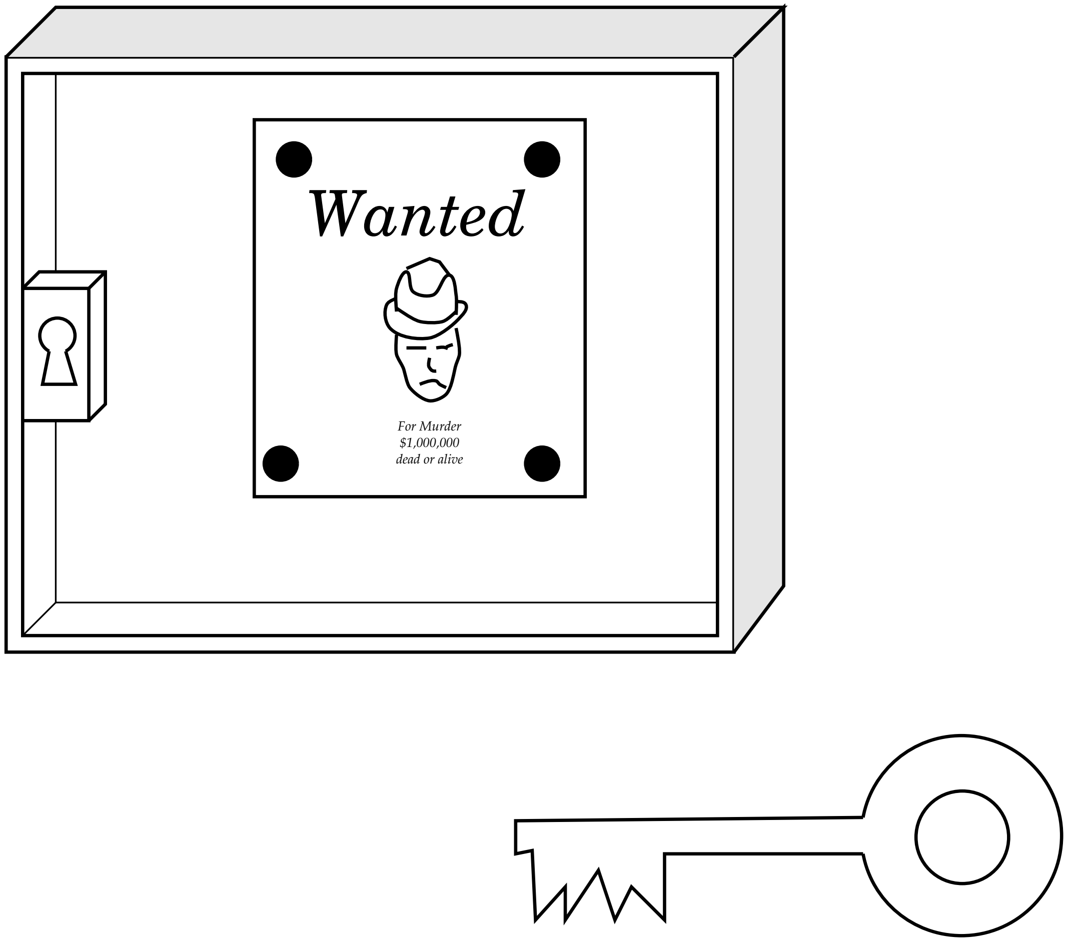
c

$m := c^d \pmod{n}$

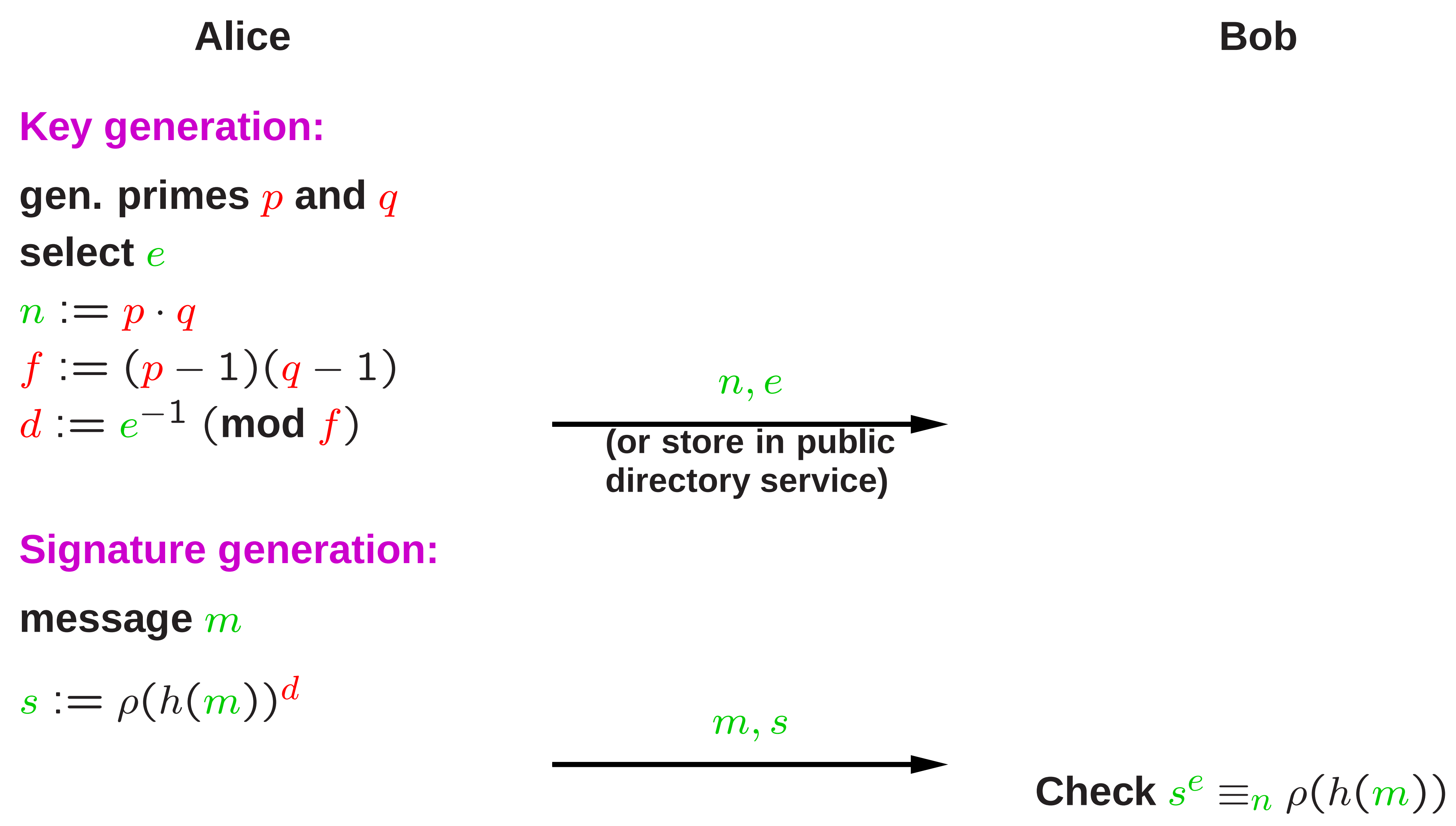
Digital signatures



Digital signature scheme: mechanical analog



Digital signatures using RSA



Alice

Bob

Key generation:

gen. primes p and q

select e

$n := p \cdot q$

$f := (p-1)(q-1)$

$d := e^{-1}$ (mod f)

$\xrightarrow{n, e}$

(or store in public directory service)

Signature generation:

message m

$s := \rho(h(m))^{d}$

$\xrightarrow{m, s}$

Check $s^{e} \equiv_{n} \rho(h(m))$