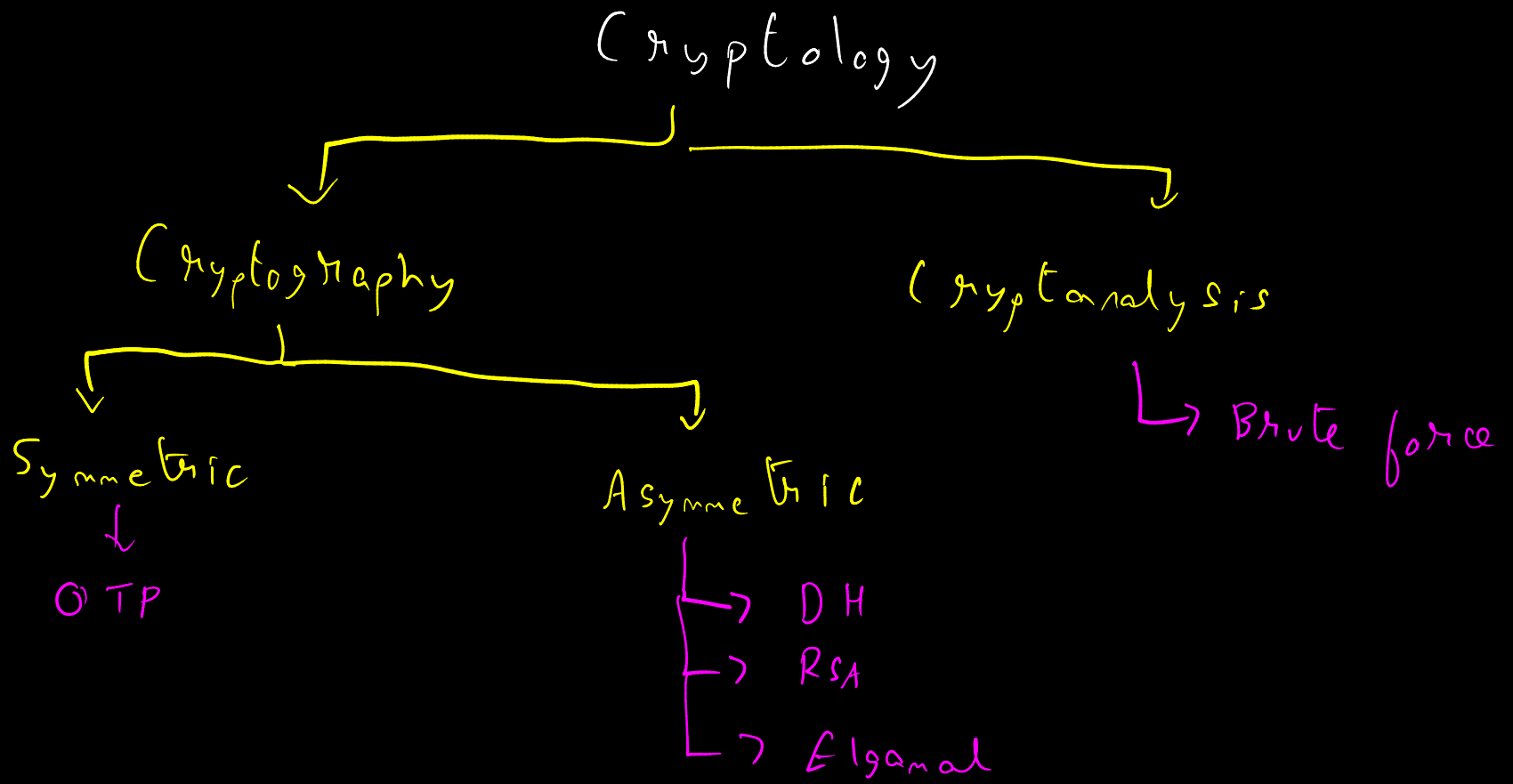
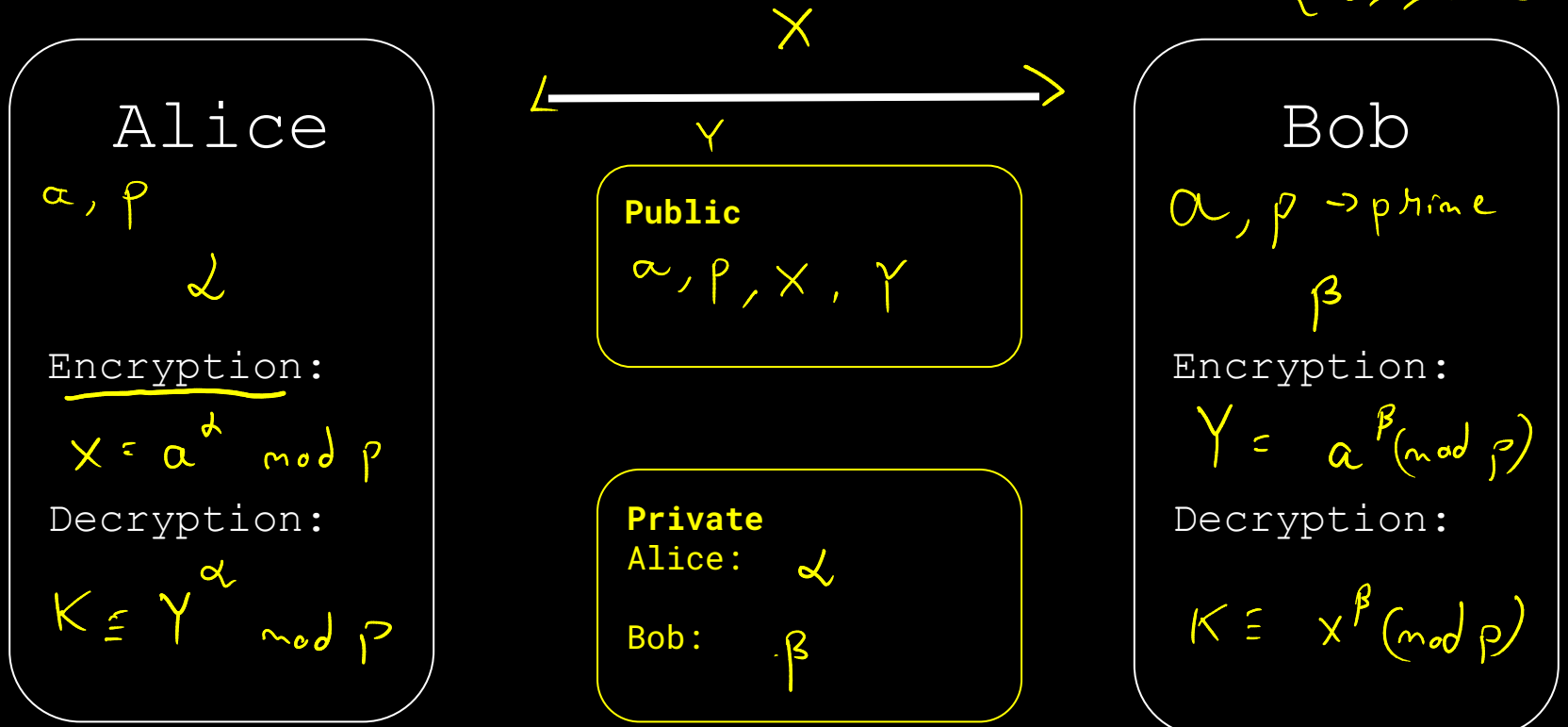

Cryptology
Cryptography
Cryptanalysis
Brute force
Symmetric
OTP
Asymmetric
DH
RSA
Elgamal

Diffie-Hellman Key Exchange

$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$



Conditions on selection: a is a generator for $\mathbb{Z}_p$

Proof of Correctness

Alice

$$K \equiv Y^{\alpha} \pmod{p}$$

$$\equiv \left(a^{\beta}\right)^{\alpha} \pmod{p}$$

$$\equiv a^{\alpha\beta} \pmod{p}$$

Bob

$$K \equiv X^{\beta} \pmod{p}$$

$$\equiv \left(a^{\alpha}\right)^{\beta} \pmod{p}$$

$$\equiv a^{\alpha\beta} \pmod{p}$$

Proof of Security

Cannot find K

Public:
a, p, X, Y

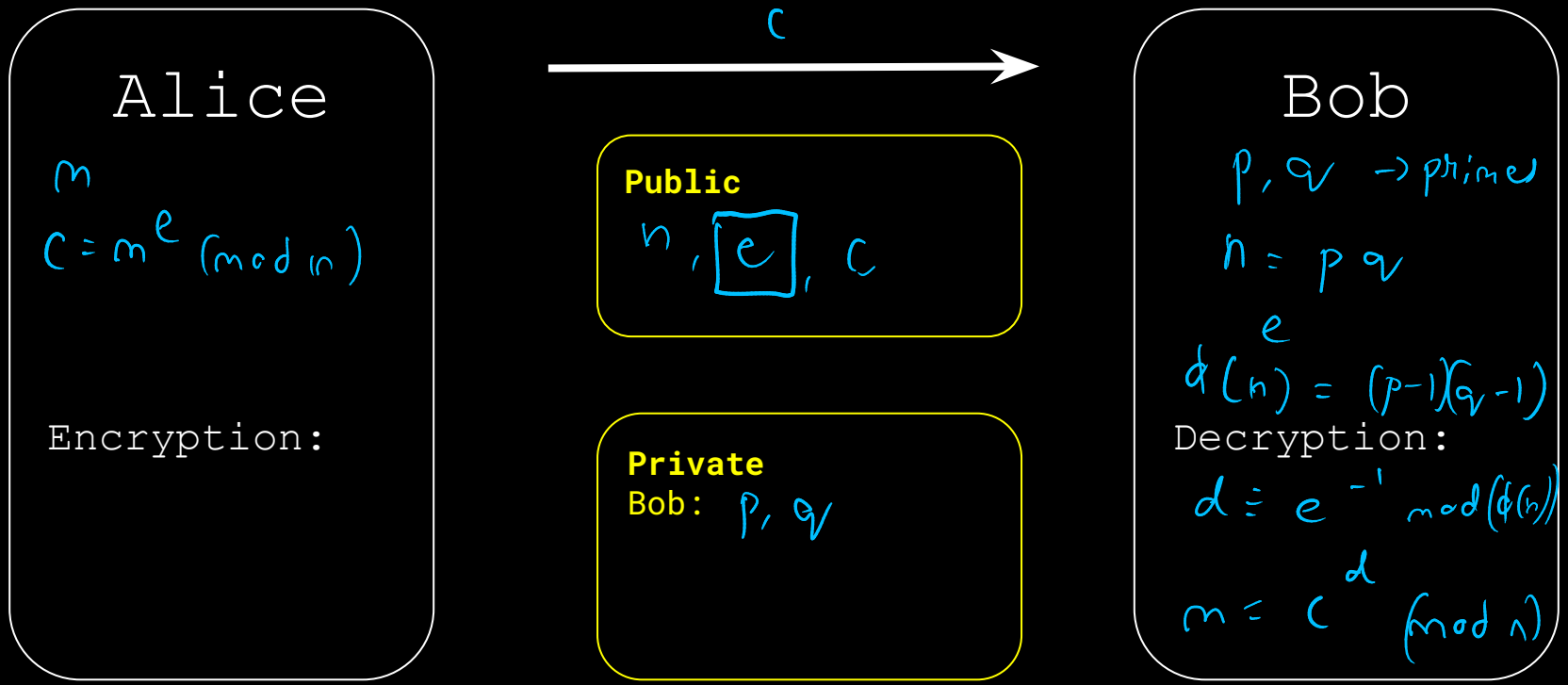
$X \equiv a^{\alpha} \pmod{p}$

$Y \equiv a^{\beta} \pmod{p}$

α -> Cannot find DLP

β -> " " "

RSA Encryption



Conditions on selection: $\gcd(e, \phi(n)) = 1$

Proof of Correctness

$e, d \rightarrow$ Modular inv mod $\phi(n)$

Alice

m

$C = m^e \pmod n$

$ed \equiv 1 \pmod \phi$

$ed - 1 = k\phi$

$\boxed{ed = k\phi + 1}$

Bob

$C = m^e \pmod n$

$m = C^d \pmod n$

$= (m^e)^d \pmod n$

$= m^{k\phi+1} \pmod n$

$= (m^\phi)^k \cdot m \pmod n$

$= (1)^k m \pmod n$

Proof of Security

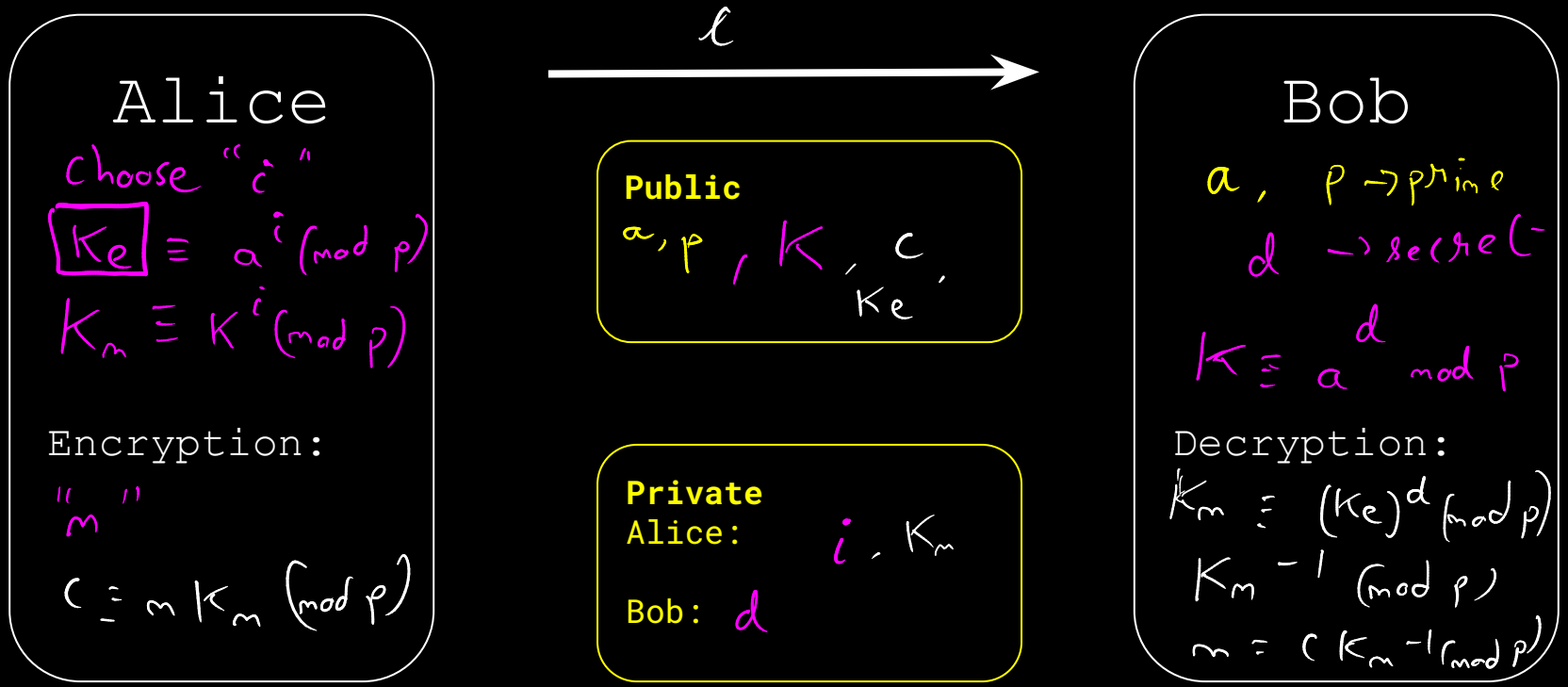
Public:
e, n, c

$n = p \times q$

Cannot p, q find

↳ Not find $\phi(n)$ → Not find d → $c^d \pmod n$ Not find m

Elgamal Cryptosystem



Conditions on selection: a should be generator of $\mathbb{Z}_p$

Proof of Correctness

Alice

$K_e \equiv a^i \pmod p$

$K_m = K^i \pmod p$

$\equiv a^{id} \pmod p$

m

$c \equiv m K_m \pmod p$

Bob

"d"

$K \equiv a^d \pmod p$

$K_m \equiv K_e^d \pmod p$

$\equiv a^{id} \pmod p$

$m \equiv c K_m^{-1} \pmod p$

$\equiv m K_m K_m^{-1} \pmod p$

$\equiv m \pmod p$

Proof of Security

$K \equiv a^d \pmod{p}$

↳ DLP

$K_e \equiv a^i \pmod{p}$

↳ DLP

Public:
a, p, K, K_e, c

$K_m \rightarrow K^i \pmod{p}$

$K_m \rightarrow K_e^d \pmod{p}$

Cannot find K_m

No K_m → cannot break