

Cryptology



Cryptography

Cryptanalysis

↳ Brute force



Symmetric

↳ OTP

Asymmetric

↳ DH
↳ RSA
↳ Elgamal

Diffie-Hellman Key Exchange

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

Alice

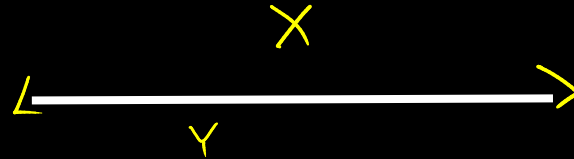
α, p

α

Encryption:

$$X = \alpha^\alpha \pmod p$$

Decryption:

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


Public

$$\alpha, p, X, Y$$

Private

Alice: α

Bob: β

Bob

$\alpha, p \rightarrow \text{prime}$

β

Encryption:

$$Y = \alpha^\beta \pmod p$$

Decryption:

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

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

Proof of Correctness

Alice

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

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

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

Bob

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

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

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

Proof of Security

Cannot find K

Public:
 a, p, X, Y

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

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

$\alpha \rightarrow$ Cannot find DLP

$\beta \rightarrow$ " " "

RSA Encryption

Alice

$$m$$
$$C = m^e \pmod{n}$$

Encryption:

C

Public

n, \boxed{e}, C

Private

Bob: p, q

Bob

$p, q \rightarrow \text{primes}$

$$n = p \cdot q$$

$$\phi(n) = (p-1)(q-1)$$

Decryption:

$$d \equiv e^{-1} \pmod{\phi(n)}$$

$$m = C^d \pmod{n}$$

Conditions on selection:

$$\gcd(e, \phi(n)) = 1$$

Proof of Correctness

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

Alice

$$C = m^e \pmod{n}$$

$$ed \equiv 1 \pmod{\phi}$$

$$ed - 1 = k\phi$$

$$ed = k\phi + 1$$

Bob

$$\begin{aligned} C &= m^e \pmod{n} \\ m &= C^d \pmod{n} \\ &= (m^e)^d \pmod{n} \\ &= m^{k\phi+1} \pmod{n} \\ &= (m^\phi)^k \cdot m \pmod{n} \\ &= (1)^k m \pmod{n} \end{aligned}$$

Proof of Security

$$n = p \cdot q$$

Cannot p, q

find

(

Not find \rightarrow Not find \rightarrow

$\phi(n)$

d

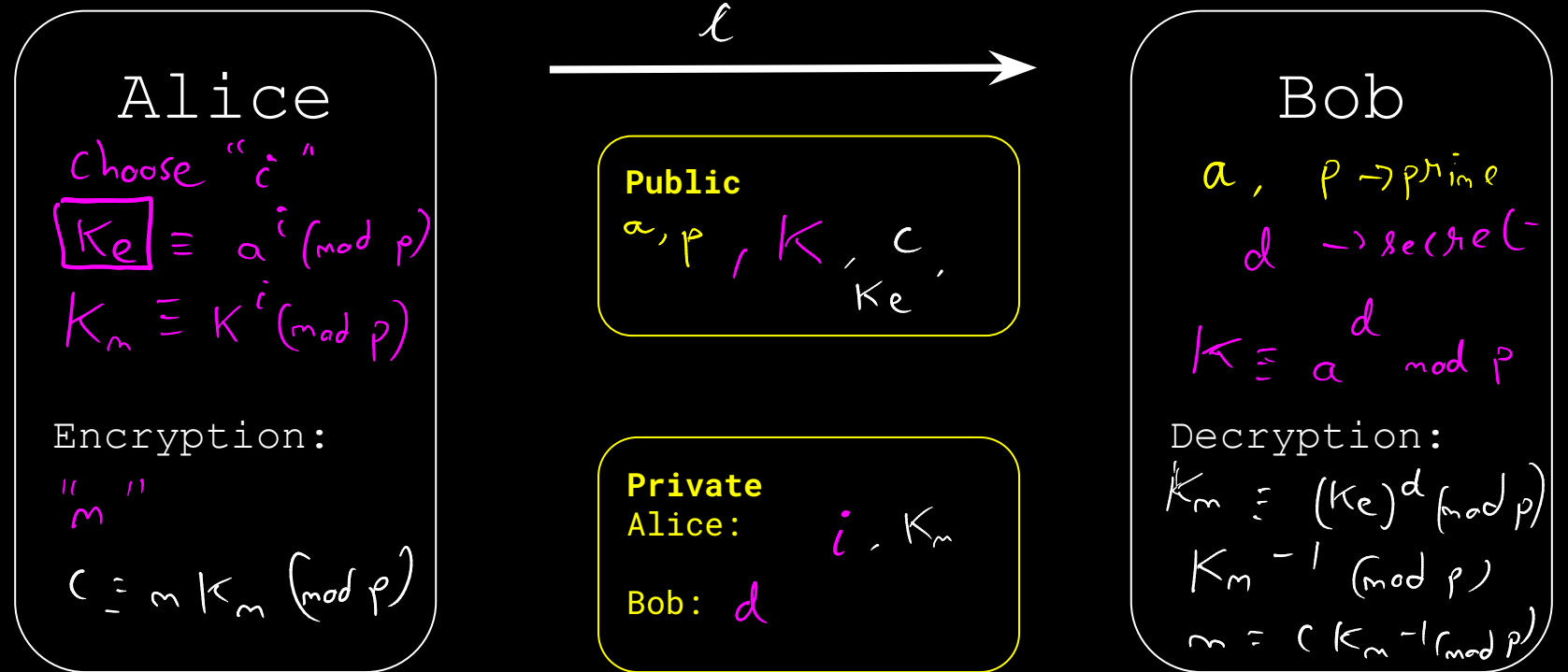
$$c^d \pmod n$$

Not find
 m

Public:

e, n, c

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"

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

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

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

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

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

$$\equiv m \pmod{p}$$

Proof of Security

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

\rightarrow DLP

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

\rightarrow DLP

cannot find K_m

Public:
 a, p, K, K_e, c

$$K_m \begin{cases} \rightarrow K^i \pmod{p} \\ \rightarrow K_e^d \pmod{p} \end{cases}$$

No $K_m \rightarrow$ cannot break