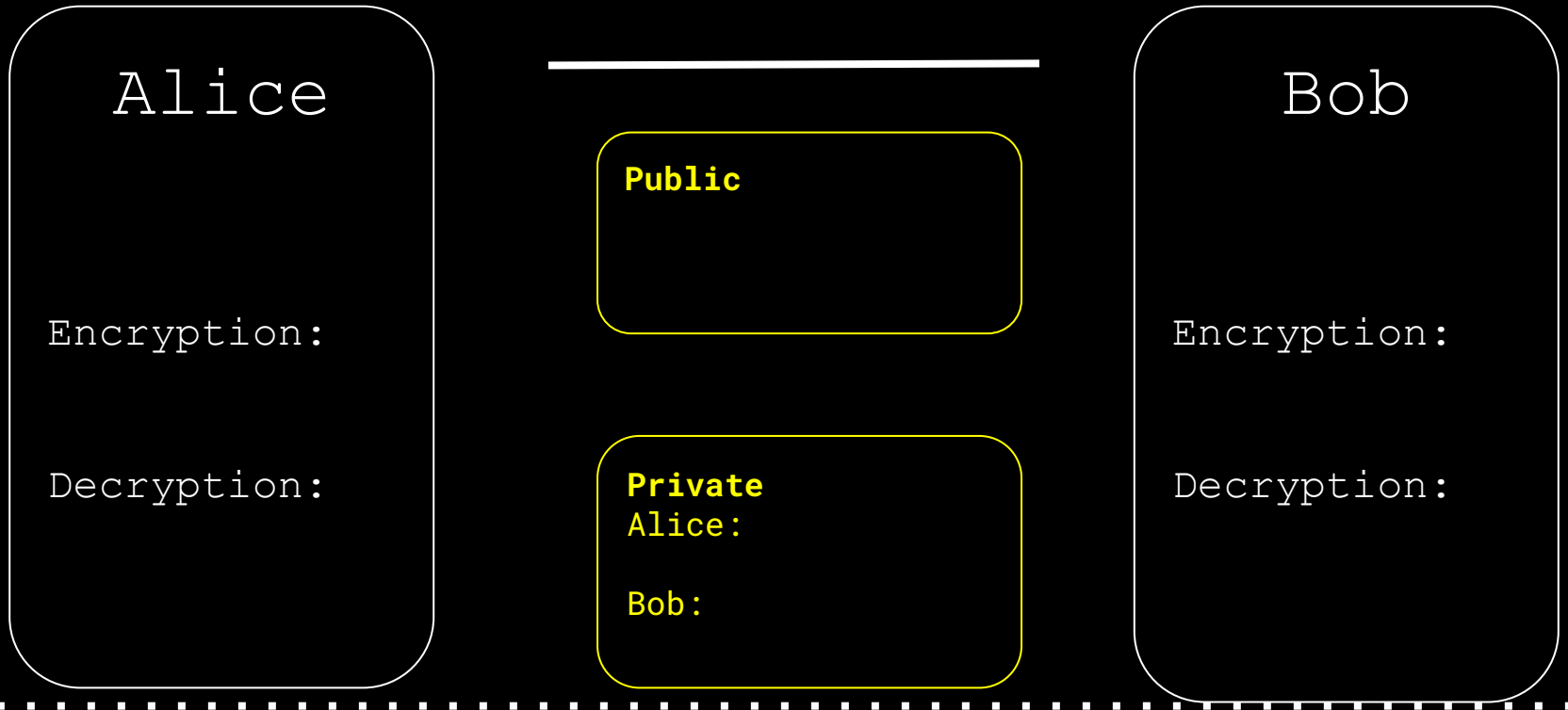
Sieve of Eratosthenes

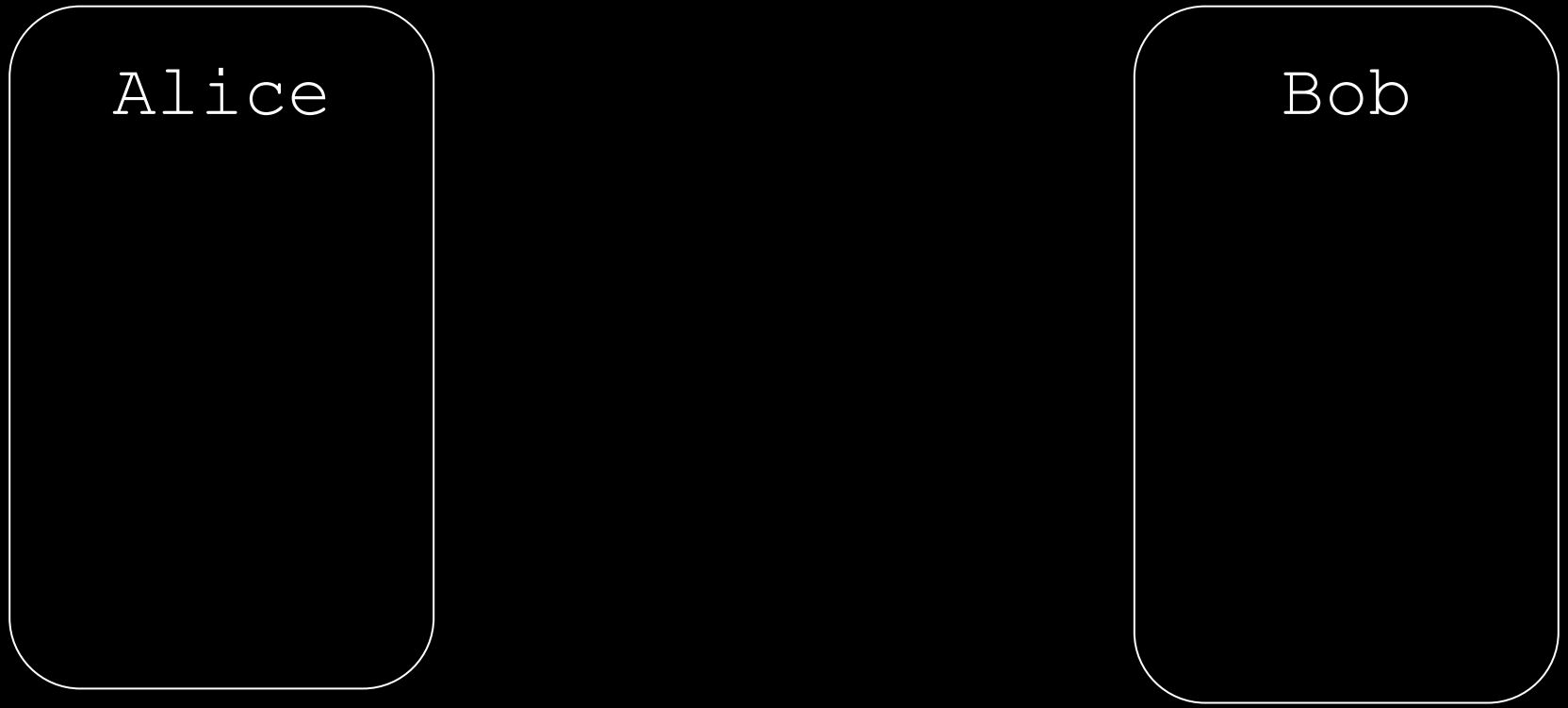
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Diffie-Hellman Key Exchange



Conditions on selection:

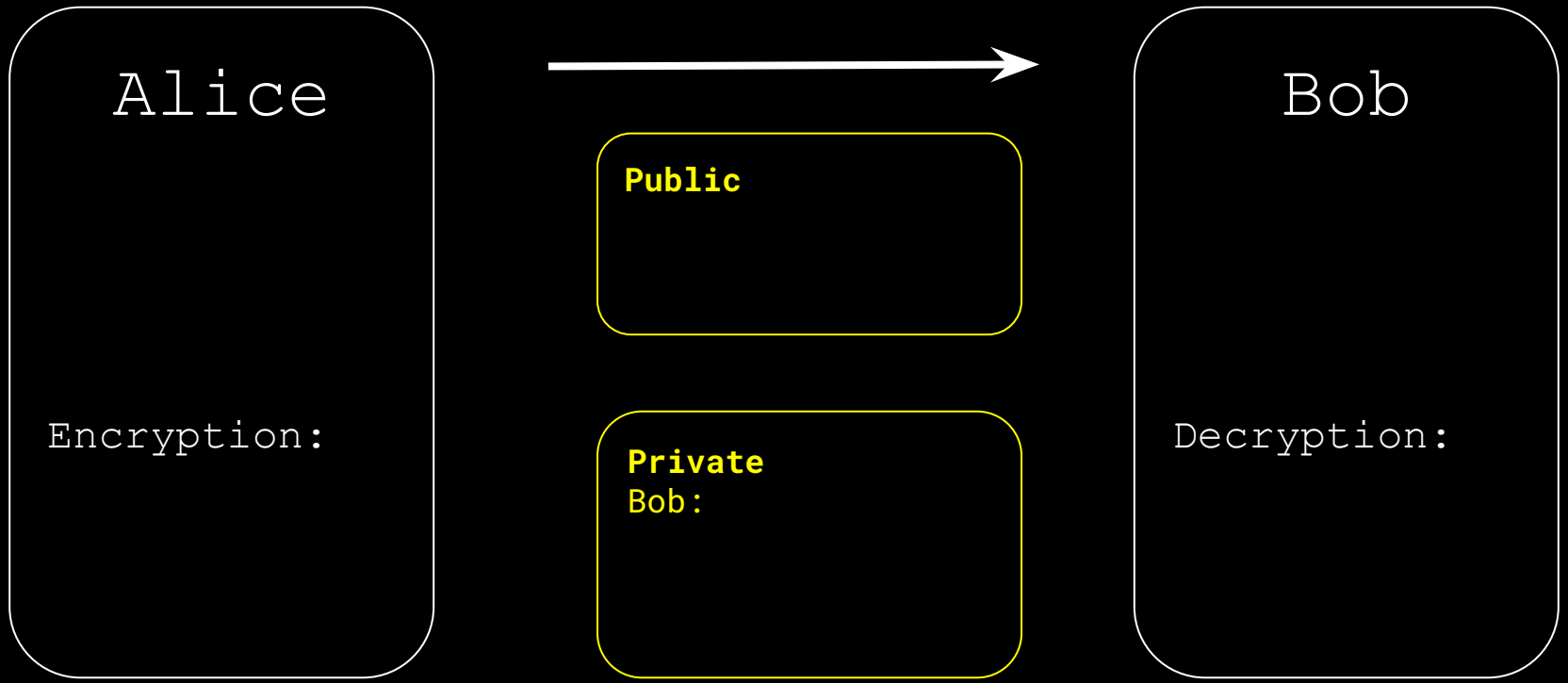
Proof of Correctness



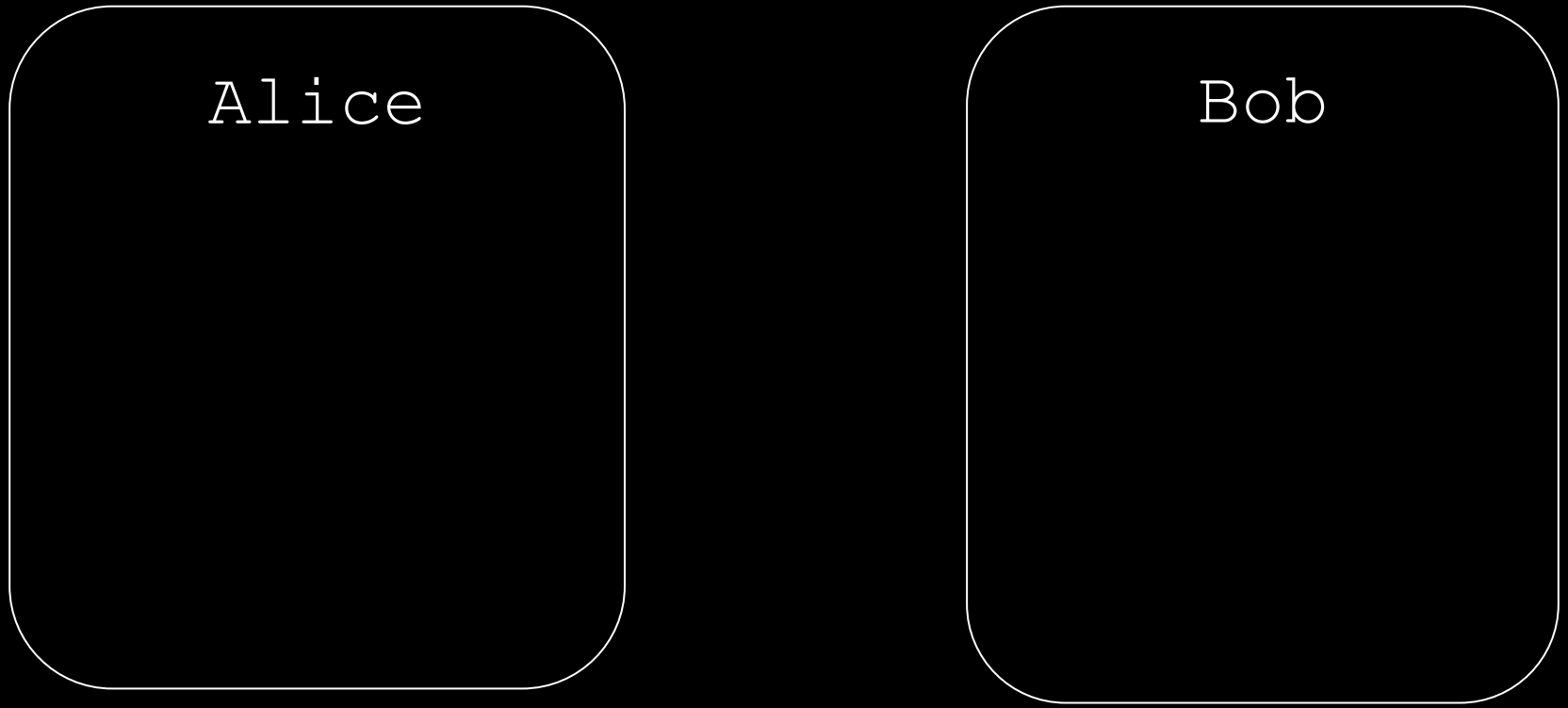
Proof of Security

Public:
a, p, X, Y

RSA Encryption



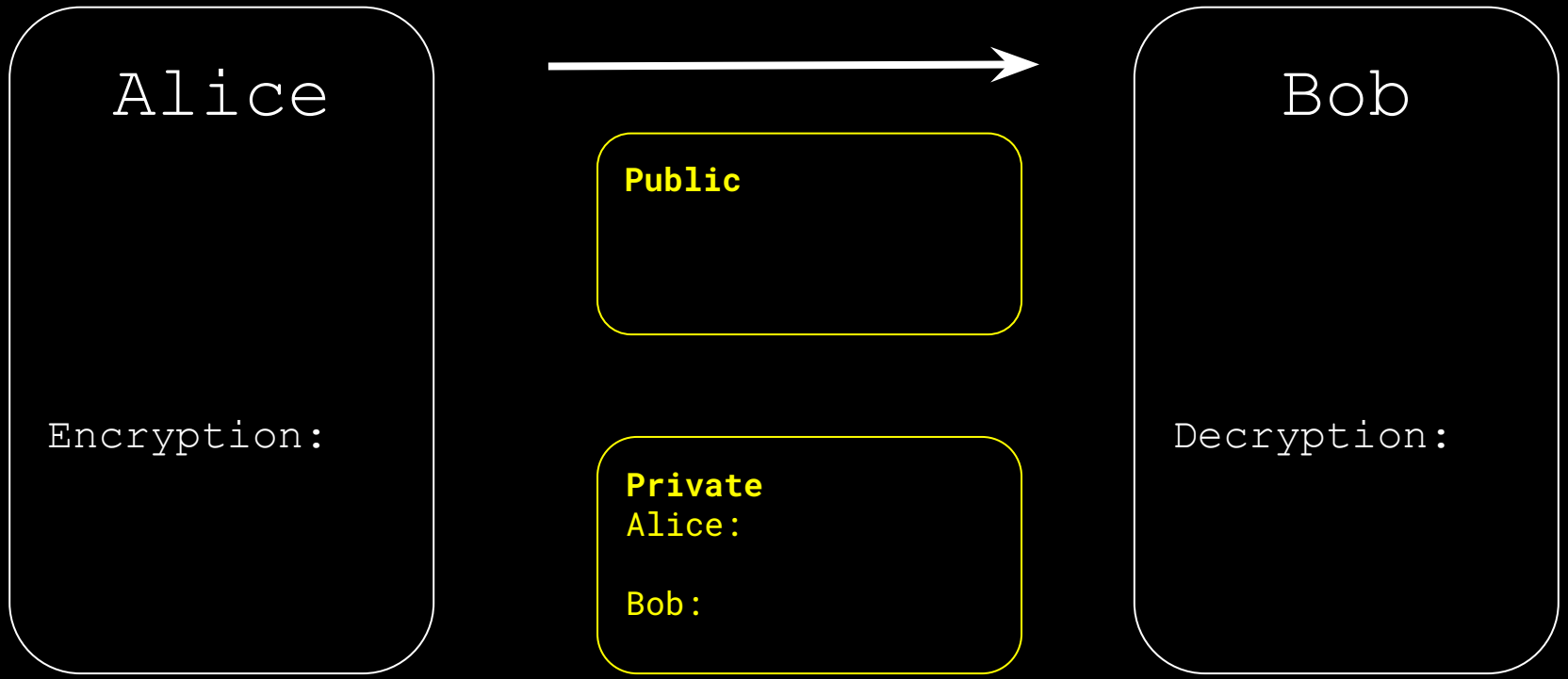
Proof of Correctness



Proof of Security

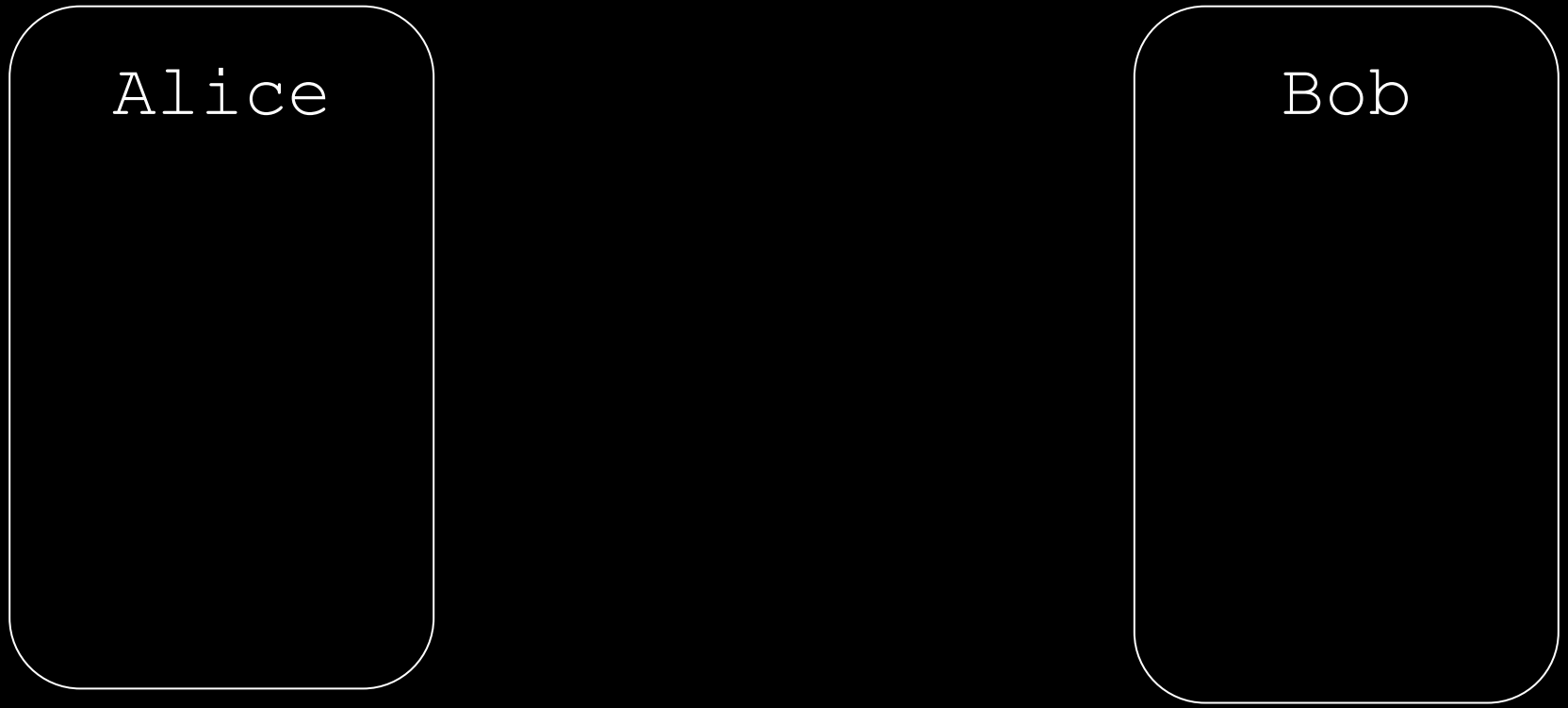
Public:
e, n, c

Elgamal Cryptosystem



Conditions on selection:

Proof of Correctness



Proof of Security

Public:

a, p, K, K_e, c