

③ RSA : public key cryptography

prime nums.

p

5

q

11

$$N = p * q$$

55

$$r = (p-1)(q-1)$$

40

$$K = i \cdot r + 1$$

$e = 3$

$$= e \cdot d$$

$d = 57$

Public: N, e

Private: N, d

Encode

$$a = 72$$

$$c = a^e \% N = 18$$

Decode

$$c = 18$$

$$a = c^d \% N = 72$$