

①

Encryption

symmetric

9/3

$$\begin{array}{ccc} \text{Alice} & K_s(m) \longrightarrow & \text{Bob} \\ m: \text{message} & & K_s(K_s(m)) = m \\ K_s: \text{key} & & \end{array}$$

asymmetric

Alice
 K_A^+ : public key
 K_A^- : private key

Bob
 K_B^+ : public
 K_B^- : private

$$K_B^+(m) \longrightarrow K_B^-(K_B^+(m)) = m$$

②

% mod operator

$$22 \% 15 = 7$$

$$n \% r = 0 \dots r-1$$

$$12345 \% 10 = 5$$

$$1023 \% 16 = 15$$

Trap Door Functions

Easy to do, hard to undo
multiplication factoring

$$839 * 653 = 547867 \approx 940 \text{ steps}$$

$$5478670 \approx 2340$$

Keys: 2048 b.ts $\sim$ 78 decimal digits
4096

③ RSA : public key cryptography

prime nums.

p

5

q

11

$$N = p * q$$

55

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

40

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

$$= e \cdot d$$

Public: N, e

Private: N, d