$A \longrightarrow B$

key key

$$C = \mathrm{Enc}(P, key)$$

$$P = \mathrm{Dnc}(C, key)$$

public

secret

$A \longrightarrow B$

① Key Gen:

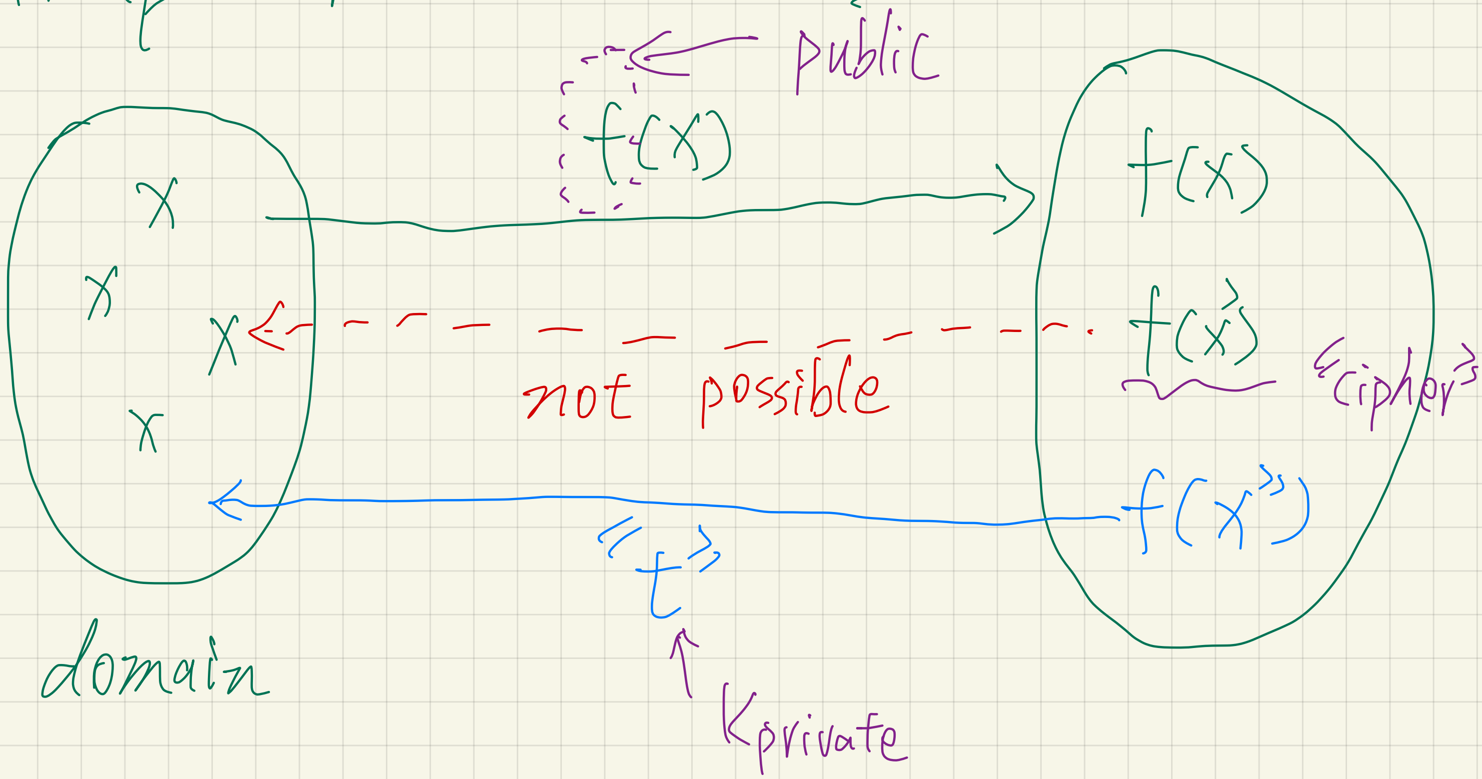
$$A \nearrow K_{pub} \Leftarrow \text{public}$$
$$A \searrow K_{private} \Leftarrow \text{private}$$

② $B \longleftarrow K_{pub}$

③ $\underset{\sim}{C} = Enc(M, K_{pub})$

④ $M = Dnc(C, K_{private})$

Trapdoor Function:



RSA

$p \times q = N$ "semi-prime"

$\underline{N}$ pub

$\underline{p \quad q}$ private

$N = 6895601$

$\underbrace{p = 1931}$

q ?

$$N \sim 2^{1024} \sim 2^{2048}$$

$$\sim 10^{150}$$

$p \qquad q \qquad\qquad p = 3 \qquad q = 11$

key Gen

$$\begin{cases} N = pq = 3 \times 11 = 33 \\ (p-1)(q-1) = 20 \\ e = 3 \\ ed \equiv 1 \mod (p-1)(q-1) \end{cases}$$

$d = 7$

$K_{pub} = (N, e) = (33, 3)$

$K_{private} = (d) = 7$

$M = 8$

$C = M^e \mod N = 8^3 \mod 33$

$= 17$

$$P = C^d \bmod N = 17^7 \bmod 33$$
$$= 8$$

$$N = 2^{1024} \sim 2^{2048}$$

$$p \quad q : \quad 2^{512}$$

every 500 → prime

$$2^{512} / 500 = 2^{500}$$
$$\approx 10^{140} \sim 10^{150}$$

$$C = M^e \bmod N$$

$$\begin{cases} 4 \bmod 3 = 1 \\ 7 \bmod 3 = 1 \\ 1 \bmod 3 = 1 \end{cases}$$

$N = 2048$ bits

$\underset{\sim}{M} \Rightarrow 245$ bytes hybrid crypto:

$A \longleftrightarrow B$

① RSA exchange symmetric key

② exchange data with symmetric cipher

confidentiality:

$$\begin{cases} C = E(m, K_{pub}) \\ m = D(C, K_{private}) \end{cases}$$

Integrity:

$$C = E(m, K_{private})$$

$$m = \text{"I'm Alice; I give Bob \$10"}$$

$$m_{sign} = E(m, K_{private})$$

$$\underbrace{m}_{\text{"id"}} = D(m_{sign}, \underbrace{K_{pub}}_{\text{owner}})$$

$A \longrightarrow B$

① key Gen ② $\dfrac{K_{public}}{\text{Alice}}$

PKI:

CA: Certificate Authority

△1 key gen

? △2 ([K_{pub} of Alice] sign by CA)

△3 Bob ⟹ K_{pub} of Alice

(△4 K_{pub} of CA → ① ship OS
→ ② ship browser
→ ③ wifi

△5 K_{pub} of Alice

CA ← ID

CA ← K_{pub}

$$A \xrightarrow{\hspace{4cm}} B$$

10GB

$$m \,,\; [m]_{sign} \longrightarrow B$$

$$\underbrace{\{[m]_{sign}\}}_{}{}_{K_{pub}} = m$$

$$H : \{ m \,,\; [H(m)]_{sign} \}$$

$$\underbrace{\{[H(m)]_{sign}\}}_{}{}_{K_{pub}} = H(m)$$

$m_1 \qquad m_2$ collision

$$H(m_1) = H(m_2)$$

$m_1, \quad [H(m_1)]_{sign}$

$m_2 \quad [H(m_1)]_{sign}$

N-bit:

$x \quad y \quad (x \neq y) \quad h(x) \neq h(y)$

2^N

1 compute m hash outputs:

$$C_m^2 = \frac{m(m-1)}{2}$$

2 estimation:

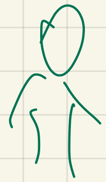
$$\frac{m(m-1)}{2} = \frac{1}{2}m^2 - \frac{1}{2}m \approx m^2$$

3 :

$$m^2 = 2^N \Rightarrow \text{collision}$$

$$m^2 = 2^N \Rightarrow m = 2^{\frac{N}{2}}$$

$$N = 256 \Rightarrow m = 2^{128}$$



(user, pwd)

Amazon

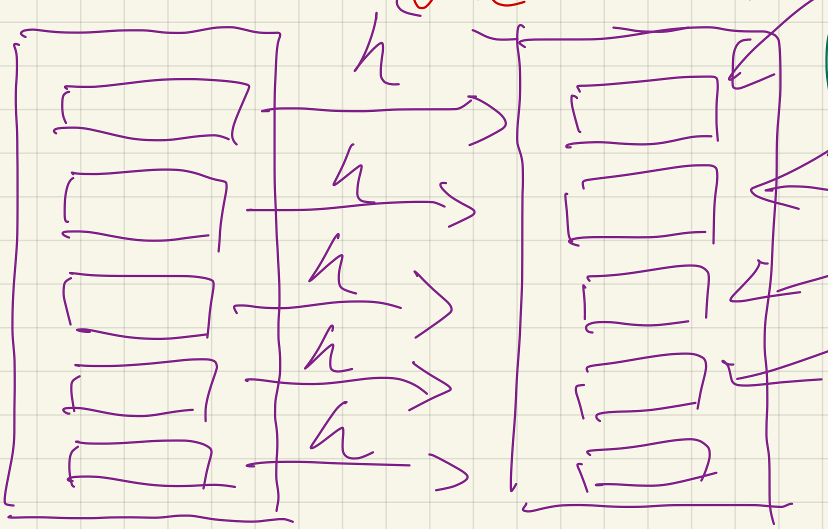
① pwd

② encrypt

reversible

dictionary

one-time

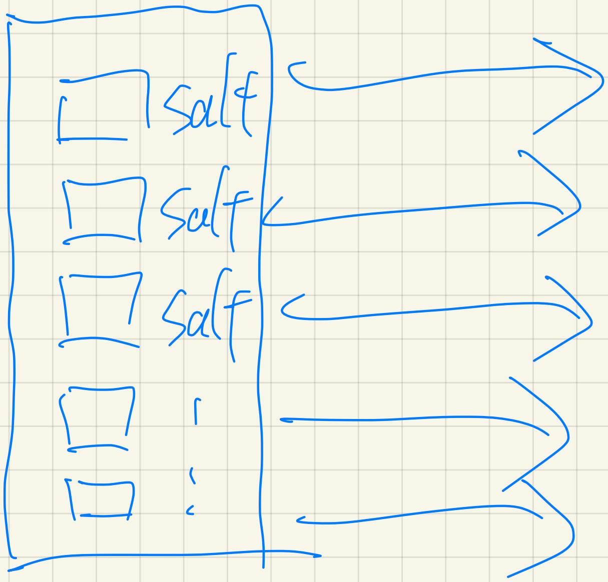


③ $h(pwd) \not\to pwd$

"rainbow table"

④ salt

(salt, h(salt || pwd))


salt
salt
salt

$A \longrightarrow B$

$t \xrightarrow{H} H(t) \xrightarrow{H} H^2(t) \to H^3(t) \cdots\cdots H^{2^4}(t)$

$t \dashleftarrow \cdots\cdots H^{2^4}(t)$

$\downarrow$ Bob

△1 1st lecture

Trudy $\boxed{H^{2^3}(t)} \longrightarrow$ Bob

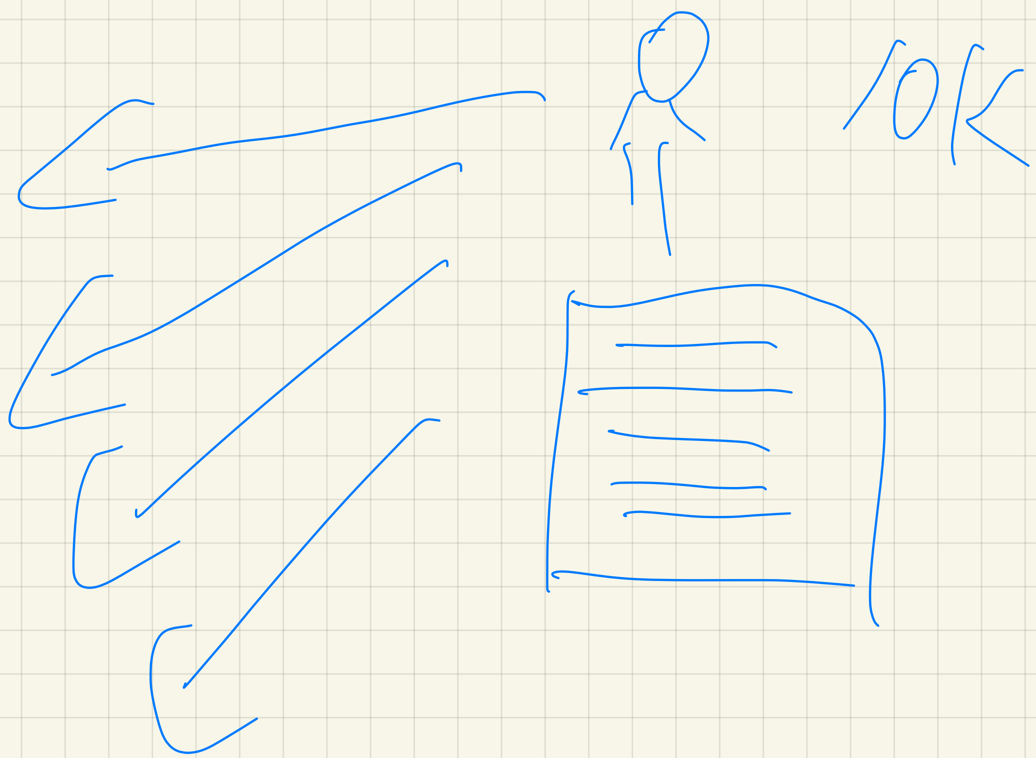
$H^{2^3}(t) \xrightarrow{H} H^{2^4}(t)$

△2 2nd lecture

$\underline{H^{2^1}(t)} \longrightarrow$ Bob

$H^{2^1}(t) \xrightarrow{H^3} H^{2^4}(t)$

spam email:



cost-free $\rightarrow$ costly

"work":

h : $\underline{32 \text{ bits}}$ $\underline{2^{32}}$

$h(x) \longleftarrow$ for leading zero

2^{10} ← computation

$10K \times 2^{10}$

$h(x)$ one-time

x	content