1. WRAP-up factoring & DL.

a. factoring & RSA

FACTORING : Given: $N = p \cdot q$ p, q n-bit prime

Goal: find p.

RSA: (N, e): $N = p \cdot q$

(N, d) pick e s.t. $\gcd(e, \phi(N)) = 1$

$\Downarrow$ unique d s.t. $e \cdot d = 1 \bmod \phi(N)$.

Given: $y = x^e \bmod N$

Goal: find x

- Known: RSA $\leq$ factoring
- unknown: factoring $\overset{?}{\leq}$ RSA
- Instead

Claim1: factoring $\leq$ computing $\phi(N)$

Claim2: factoring $\leq (N, e) \mapsto d$

Pf (Claim 1)

$N = p \cdot q$

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

$= p \cdot q - p - q + 1$

B/C $q = N/p$ ↺

$\Leftrightarrow \phi(N) = N - p - N/p + 1$

$\Leftrightarrow p \cdot \phi(N) = N \cdot p - p^2 - N + p$

$\Leftrightarrow p^2 - (N - \phi(N) + 1)\, p + N = 0$

↑ unknown

$ax^2 + bx + c = 0 \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Solve for p. ∎

Ex. $N = 91$ (7×13)

Find p, q

Given: $\phi(N) = 72$, $N = 91$

↙

$p^2 - (N - \phi(N) + 1)\, p + N = 0$

$\Leftrightarrow p^2 - (\ 20\ )\, p + 91 = 0$

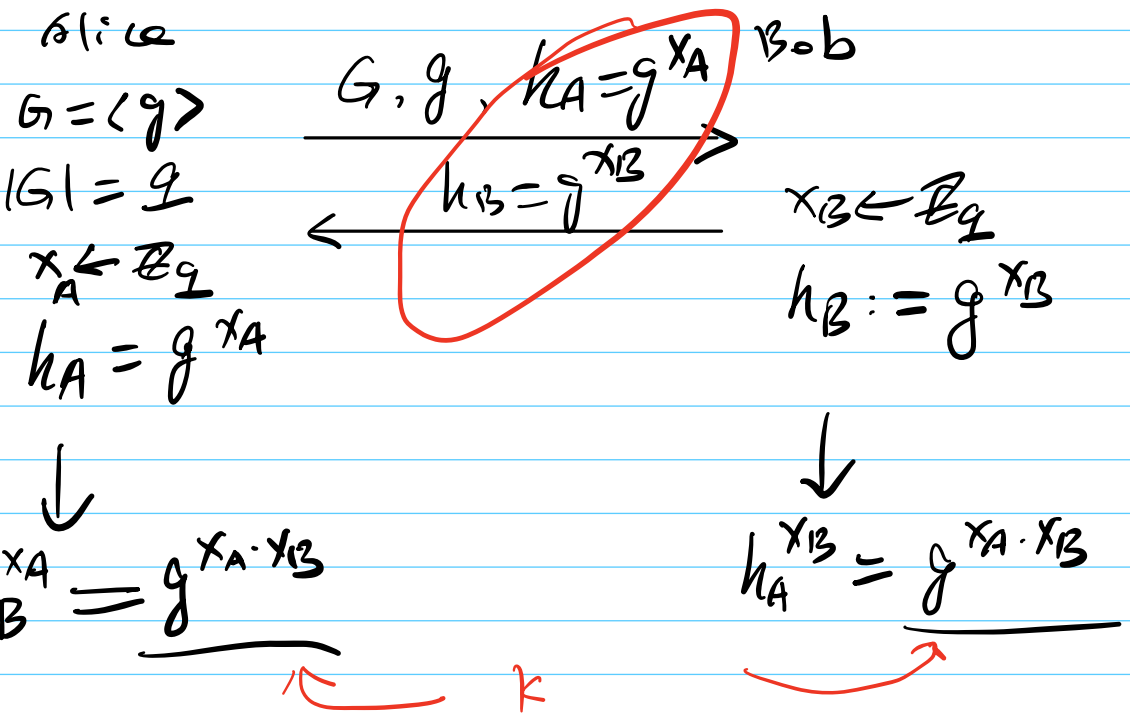
$\Leftrightarrow p^2 - 20p + 91 = 0$

$\Leftrightarrow (p-7)(p-13) = 0.$ #

b. Discrete Log.

Given: $G = \langle g \rangle$, $y = g^x$

Goal: find $x := \log_g y$



- DL assumption: $g^x \mapsto x$ hard.

  Env: $(g^{x_A}, g^{x_B}) \mapsto g^{x_A \cdot x_B}$

- CDH assumption: $(g^{x_A}, g^{x_B}) \mapsto g^{x_A \cdot x_B}$ is hard.

- DDH :

(decisional)

$(G, g, g^{x_A}, g^{x_B}, g^{x_A \cdot x_B})$ Real

$\approx$

$(G, g, g^{x_A}, g^{x_B}, g^{x_C})$ Ideal Case.

$x_C \leftarrow \mathbb{Z}_q$

Gav. Key

indistinguishable

- Relations.

$$DDH \leq CDH \leq DL$$

???

2.

a. Recall : RSA for key exchange.

Alice (N, e, d) — Bob

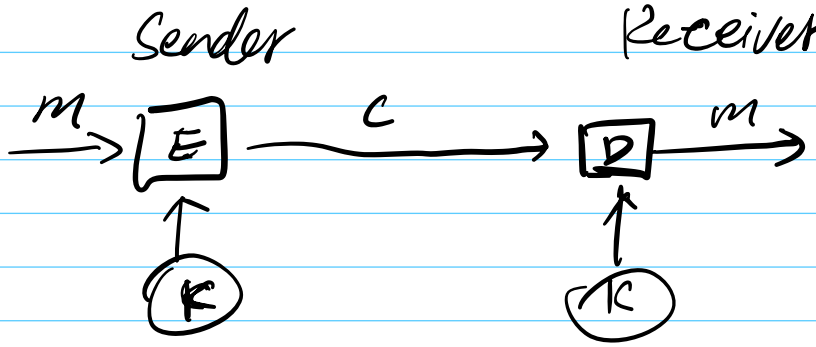
(N, e) public

$y = x^e \bmod N$

$x := y^d$ — $x \in \mathbb{Z}_N$ — x

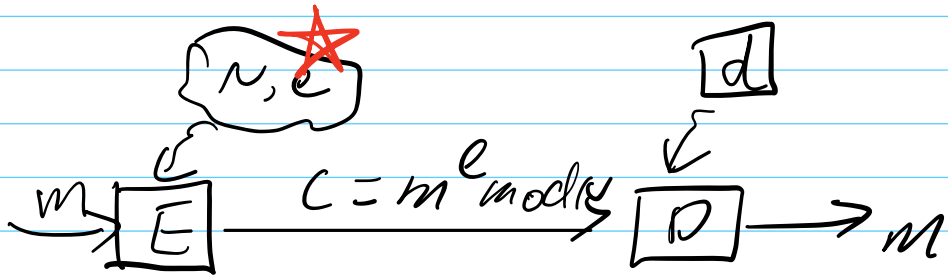
- we treated x as a key. but it could be any msg.
- key obs:

prior:



Symmetric-key Enc.
/ Private-key Enc

now:



Asymmetric-key Enc
/ Public-key Enc

- **DEF.** A pubkE is a triple Alg's:
  $\Pi = (KG, E, D)$ key Generation
  - G: $(pk, sk) \leftarrow KG(1^n)$
    (Pub key / Enc key), (secret key / Dec key)

- E: $c \leftarrow E_{pk}(m)$
- D: $m \leftarrow D_{sk}(c)$

Correctness: $D_{sk}(E_{pk}(m)) = m$.

RSA: $KG(1^n) \rightarrow (N, e, d)$

$pk = (N, e)$

$sk = (N, d)$

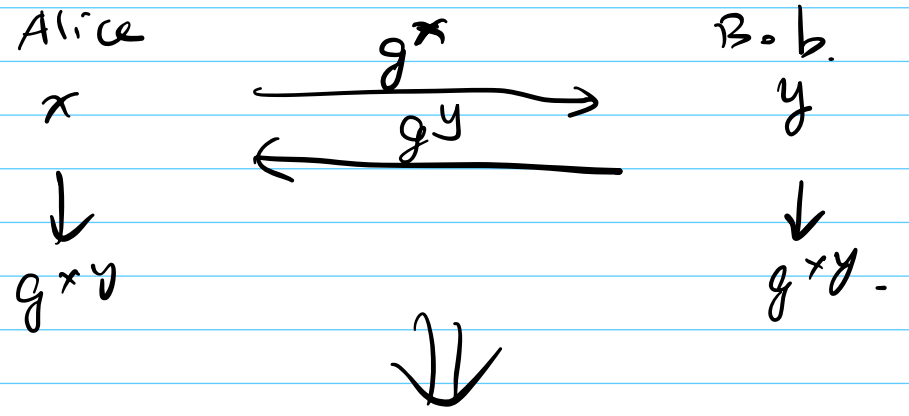
E: $m \mapsto m^e \bmod N$

D: $c \mapsto c^d \bmod N$.

★ Caution! plain-RSA / Textbook-RSA.

- to enc. random x OK!
- NOT OK for arb. msg x, more work needed!

b. D.H. k.E $\Rightarrow$ El Gamal PubKE



ElGamal $\Pi = (KG, E, D)$.

- KG: $(G, q, g) \leftarrow KG(1^n)$

  i.e. $G = \langle g \rangle$, $|G| = q$.

  - $x \leftarrow \mathbb{Z}_q$, $h = g^x$

  $pk := (G, q, g, h)$

  $sk := (G, q, g, x)$

- E: msg $m \in G$.

  - $y \leftarrow \mathbb{Z}_q$, $h^y (= g^{xy})$

  - $(c_1 := g^y, c_2 := h^y \circ m) \rightarrow c$: ciphertext.

    ($\circ$ ↑ Group op)

- D: on sk $(= x)$, $c = (c_1, c_2)$.

  $c_1 = g^y$, $c_2 = h^y \circ m$

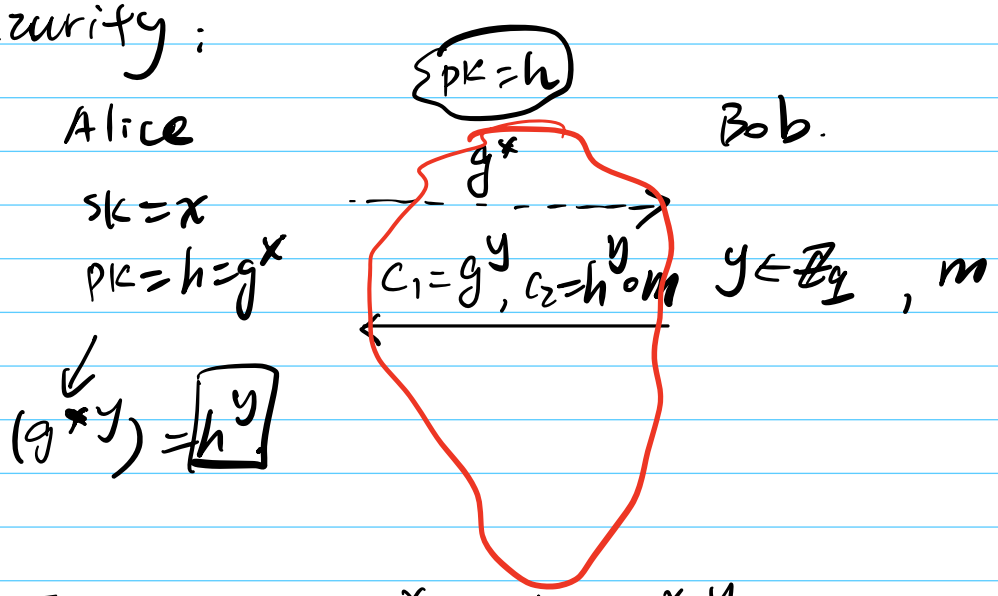
  - $(c_1^x) = g^{xy} = h^y$

  - $(h^y)^{-1} \circ c_2 = \underbrace{(h^y)^{-1} \circ h^y}_{\text{(Assoc.)}} \circ m$

    $= m$

$\blacksquare$

- Security:



Eav sees: $(g^x, g^y, g^{x \cdot y} \circ m)$

$\approx_{DDH}$ $(g^x, g^y, g^z \circ m)$

$z \leftarrow \mathbb{Z}_q$

$g^z \circ m$

↑

indep. random group elem. in G.

$\Leftrightarrow$ OTP : in G w/ fresh key.

(one-time-pad)

Thm: under DDH, ElGamal PubKE is secure. (informal)

2. Group isomorphism.

a. Basics.

. DEF (iso) G, H be groups.

w/ Group op's. $\circ_G$, $\circ_H$

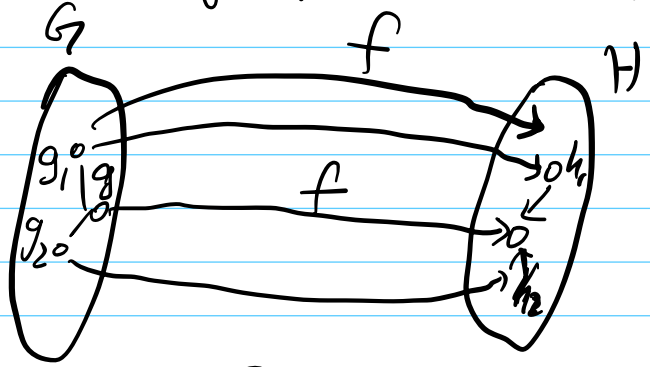
A function $f: G \to H$
is an <u>isomorphism</u> from G to H

① f is bijeztion (one-one correpondenze)

② $\forall\ g_1, g_2 \in G$.

$$f(g_1 \circ_G g_2) = f(g_1) \circ_H f_2(g_2)$$

$g \in G$ $\quad h_1 \in H$ $\quad h_2 \in H$



If only ② : call it <u>hormomorphism</u>.

If $f: G \to H$ iso, $G \cong H$

b. CRT (Chinese Remainder Theorem)

Let $N = p \cdot q$ $\quad (p, q) = 1$ $\quad p, q > 1$.

then $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ ∎