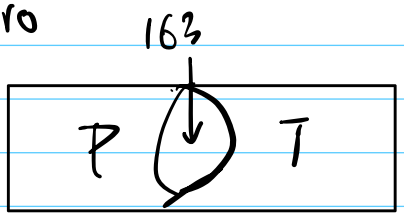
03/31 251 Lec 1

宋方 (FANG SONG)
fang.song@pdx.edu

0. Intro



CS curriculum
P: coding, hands-on
T: Theory

250/251: Discrete structures.
Typical topics

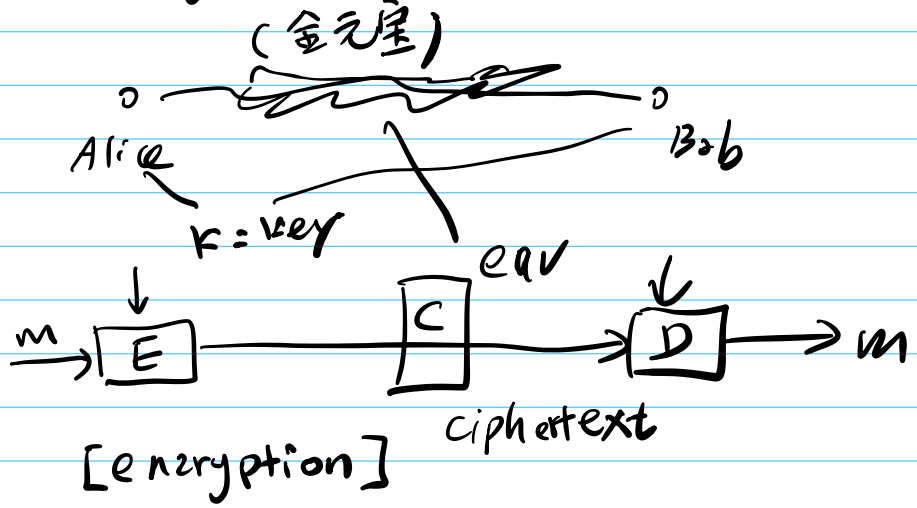
250
- ☐ set theory
- ☐ math proofs
- △ Graph theory
- ◇ probability theory

251
- ○ Logic
- ☆ Algebraic structures (aka. abstract) algebra

others
- △ Combinatorics
- ☆ number theory
- ◇ linear Algebra

why bother?
- ☐: foundations
- ○ PL theory
- ◇: ML / AI / Data science
- ☆: cryptography / PL / LLMs

1. Motivating question:



[encryption]

Private-key encryption scheme

(Symmetric-key encryption)

? How to share the secret key k?

↓

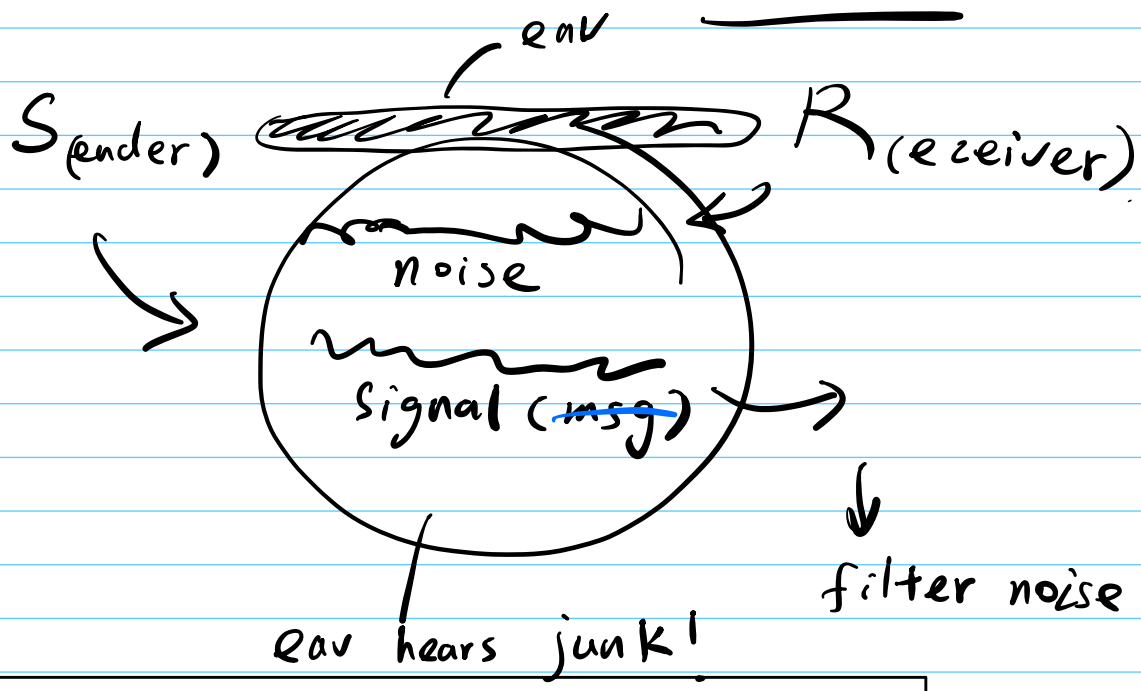
Public-key Revolution

1970s: think out of the box

Ralph Merkle,
Whitfield Diffie
Martin Hellman
Adi Shamir, Ron Rivest,
Leo Adelman, Goldwasser,
Micali, Yao, ...

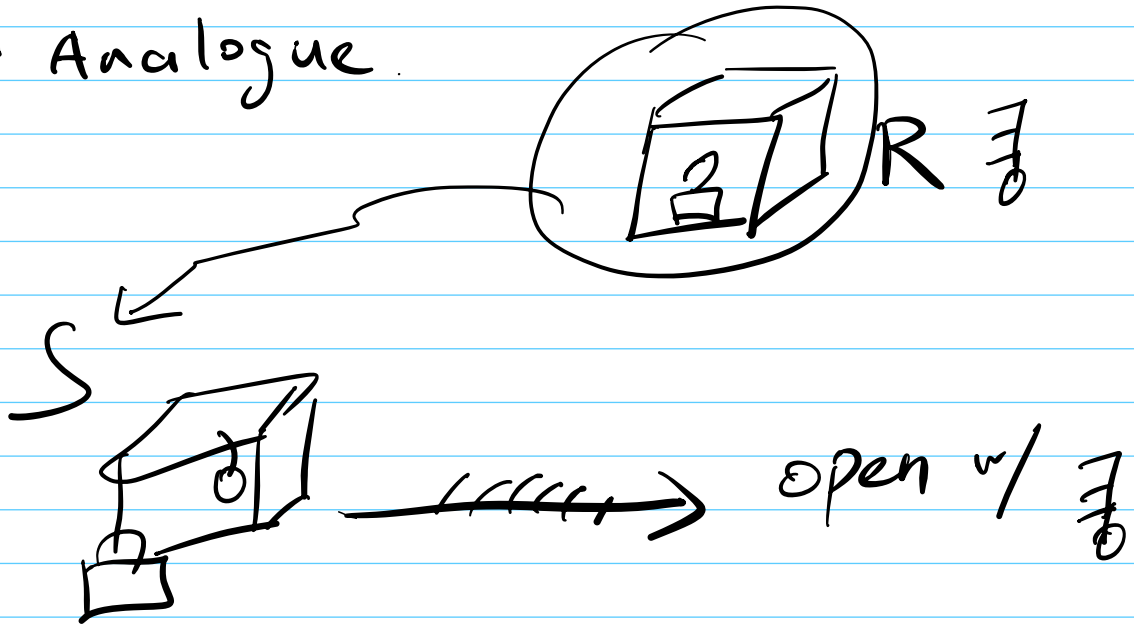
- Inspiration:

WWII: Communcation over phone



S/R don't need to meet in advance to share any secret at all!

- Analogue



6. A wishful math object

- Function: $F(\cdot, \cdot)$
  - key
  - input (msg)
  - 2 keys every one can generate
    - pk: public key
    - sk: secret key aka. trapdoor
  - $F(pk, \cdot)$ [lockable box]
  - $F(sk, \cdot) = F^{-1}(pk, \cdot)$
    - $F(sk, \cdot)$: [open box]
    - $F^{-1}(pk, m)$: c
- Two desired properties:
  - $F(pk, \cdot)$ $F(sk, \cdot)$ can be computed efficiently
  - $F(pk, m) = c \xrightarrow{\text{w.o. sk}} m$

    $F(pk, \cdot)$ hard to invert w.o. sk.

Modern Terminology

Trapdoor one-way permutation

TOWP

04/02 251 Lez 2

1. Number theory 101

a. modular arithmetics

- $a, N \in \mathbb{Z}$, $N \geq 2$ — N: modulus

$a = qN + r$

q: quotient, r: remainder

- $a, b, N \in \mathbb{Z}$

$a = b \bmod N$

iff. a, b have same remainder divided by N.

- $\mathbb{Z}_N := \{0, 1, 2, \ldots, N-1\}$
  - mod N addition $+_{\bmod N}$ $(+_N)$
  - mod N multiplication $\cdot_{\bmod N}$ $(\cdot_N)$

$N = 15$, $\mathbb{Z}_N := \{0, \ldots, 14\}$

$7 +_N 14 = 6 \bmod N$

$3 \cdot_N 9 = 12 \bmod N$

- $\forall a \in \mathbb{Z}_N$, has unique additive inverse

  $\exists b \in \mathbb{Z}_N$ s.t. $a+b = 0 \bmod N$.

- $\forall a \in \mathbb{Z}_N$,

  $\exists b \in \mathbb{Z}_N$ s.t. $a \cdot b = 1 \bmod N$

Ex: $N=6$ $a=2$ $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$.

$2 \cdot 1 = 2$ ✗

$\cdot 2 = 4$

$\cdot 3 = 0$ $\stackrel{?}{=} 1 \bmod 6$

$\cdot 4 = 2$

$\cdot 5 = 4$

- greatest common divisor (gcd)
  - $\gcd(a, b)$: largest int. that divides a & b.

    $\gcd(6, 10) = 2$
  - Euclid(ean) alg: computing $\gcd(a, b)$

- Thm: $a \in \mathbb{Z}_N$ has a mult. inverse ($b \in \mathbb{Z}_N$, $a \cdot b = 1 \bmod N$)

  iff. $\gcd(a, N) = 1$ → (coprime)

$\mathbb{Z}_N^* := \{ a \in \mathbb{Z}_N : \gcd(a, N) = 1 \}$

Ex: $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$. $a=2$ # mult. inverse.

$\gcd(a, 6) = 1$

$\mathbb{Z}_6^* := \{1, 5\}$

- $\phi(N) := |\mathbb{Z}_N^*|$: Euler's function

FACT: $\phi(p \cdot q) = (p-1)(q-1)$.

(p, q prime)

$\Rightarrow \phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3)$

$= 2$

- Modular exponentiation
  - $a \in \mathbb{Z}_N$, $b > 0$
  - $a^b \bmod N := \underbrace{a \cdot a \cdot \dots \cdot a}_{b \text{ times}} \bmod N$

a, b

Size $\|a\|, \|b\| \approx \log_2 a$, $\log_2 b$

(len of binary rep)

$5 = 101$

$64 = 1000000$

$128 = \dots$

- Repeated squaring alg.: $\text{poly}(\|a\|, \|b\|, \|N\|)$

- Thm (Euler Thm)

If $N \geq 2$, $\forall a \in \mathbb{Z}_N$, then $a^{\phi(N)} = 1 \bmod N$

Ex. Let $N = 33 = 3 \times 11$

$\phi(N) = \phi(33) = (3-1)\cdot(11-1) = 20$

- $\mathbb{Z}_{33}^* := \{1, 2, 4, 5, \ldots\}$
  $\gcd(a, 33) = 1$ $\quad \phi(33) \stackrel{?}{=} |\mathbb{Z}_{33}^*|$
- $2^{22} \bmod 33 = 2^{20+2} = 2^{20} \cdot 2^2$
  $= 1 \cdot 4 \pmod{33}$
  (by Euler Thm)
- Let $e = 7$ $\quad \gcd(e, \phi(N)) = \gcd(7, 20) = 1$
  ✓ $\exists$? d s.t. $e \cdot d = 1 \bmod 20$ $[\bmod \phi(N)]$
  $d = 3$

2. Factoring & RSA

a. FACTORING:

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

Goal: Find p (& q) $\quad n = \log N = |N|$

- Best alg known: $\exp(n^{\frac{1}{3}} \cdot \log n^{2/3})$
  (classical)

b. RSA problem (Rivest – Shamir – Adelman)

- Consider $\mathbb{Z}_N^*$, $\phi(N) = (p-1)\cdot(q-1)$
  - $N = p \cdot q$
  - pick $e > 1$, s.t. $\gcd(e, \phi(N)) = 1$.

$\Rightarrow \exists d$ s.t. $e \cdot d = 1 \mod \phi(N)$

- Compute d

$\boxed{(N, e, d)}$

- Define functions

$F_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$

$x \mapsto x^e \bmod N$

$F_d : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$

$y \mapsto y^d \bmod N$

Claim: $(F_e)^{-1} = F_d$

$\forall x \in \mathbb{Z}_N^* : \quad F_d(F_e(x)) = x$

Pf: $F_d(x^e) = (x^e)^d = x^{e \cdot d}$

$e \cdot d = 1 \mod \phi(N)$

i.e. $e \cdot d = k \cdot \phi(N) + 1$ for some k

$= x^{k \cdot \phi(N) + 1}$

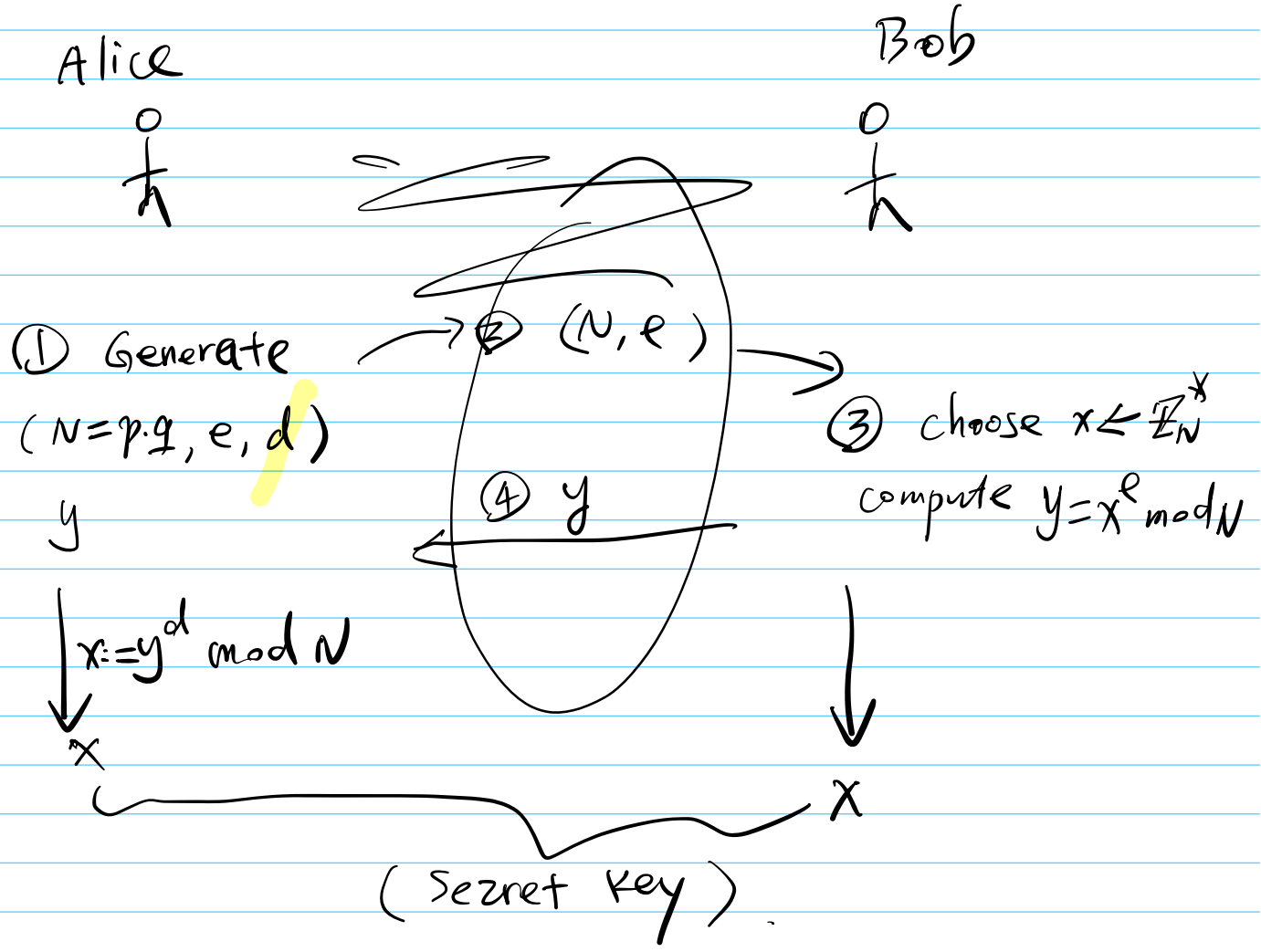
$= x^{k \cdot \phi(N)} \cdot x$

$= x \bmod N$

? Find x from $y = x^e \bmod N$ (w.o. knowing d)

Conj: Inverting F_e ($x^e \bmod N \mapsto x$) is hard (w.o. d)

c. RSA app: exchange a secret key in public.



- Correctness: ✓ both agree on x
- Security: computing $(x^e \mapsto x)$ ✓ is hard (w.o. knowing d).

04/07 251 Lec 3

0. Recap: Factoring & RSA problems.

a. defs recall

b. RSA exercise

$N = 33 = 3 \times 11$ $\quad \phi(N) = (3-1)(11-1) = 20$.

$\Rightarrow |\mathbb{Z}_{33}^*| = 20$

$e := 7$ $\quad \gcd(e, \phi(N)) = 1$

$d = e^{-1} = \underline{3}$ s.t. $e \cdot d = 1 \mod \phi(N)$ (20)

$F_e: \; x \longmapsto x^7 \mod 33$

$F_d: \; y \longmapsto y^3 \mod 33$

RSA problem: Given $y = x^e \mod 33$. find x.

- $x = 3$ $\quad F_e(3) = 3^7 = 9 \mod 33$

Repeated Squaring

① $7 = 2^2 + 2^1 + 2^0$

② $3^1 = 3 \mod 33$

$3^2 = 9$

$(3^2)^2 = 3^4 = 9^2 = 81 - 2 \cdot 33 = 15$

③ $3^7 = 3^{2^2+2^1+2^0} = 3^{2^2} \cdot 3^{2^1} \cdot 3^{2^0}$

$= 15 \cdot 9 \cdot 3$

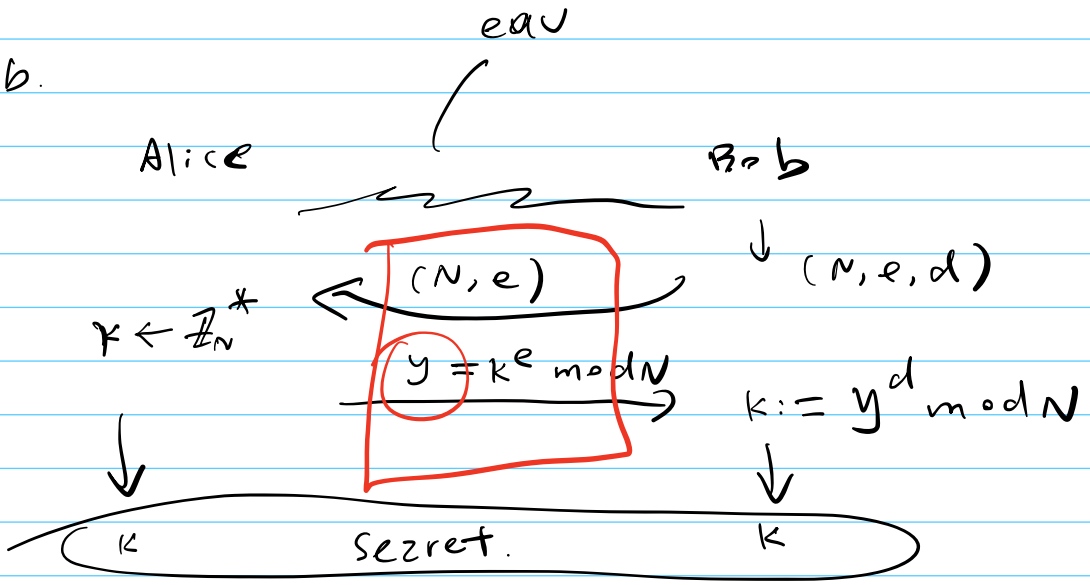
$= 9 \mod 33$

$F_e(3) = 3^7 = \boxed{9}$

F_d: $y = 9$ find x s.t. $x^e = y = 9$

$$9 \longmapsto 9^3 = 9^{2+1}$$
$$= 9^2 \cdot 9$$
$$= 3^4 \cdot 3^2 \quad \text{mod } 33$$
$$= 15 \cdot 9 = 3$$

b.



RSA-TDOWP: (G, F_{pk}, F_{sk})

- $G(1^n)$:
  - $N = p \cdot q$
  - e (RSA problem).
  - d
  - → $pk = (N, e)$ public-key
  - → $sk = (N, d)$ secret-key
- $F_{pk} := F_e = x^e \bmod N$ (→ permutation $\mathbb{Z}_N^*$)
- $F_{sk} := F_d = y^d \bmod N$.

→ TD ✓ → ow: (one-way) RSA assumption.

1. Diffie-Hellman problem
(Discret log)

a. $(\mathbb{Z}_N^*, \cdot \bmod N)$ $N = p$ prime.

$\mathbb{Z}_p^* = \{1, \dots, p-1\}$

Ex: $p = 7$. $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

- $3^0 = 1$ $3^1 = 3$ $3^2 = 2$ mod 7
  $3^3 = 6$ $3^4 = 4$ $3^5 = 5$ $3^6 = 1$
- $2^0 = 1$ $2^1 = 2$ $2^2 = 4$
  $2^3 = 1$ $2^4 = 2$ $2^5 = 4$ $2^6 = 1$

OBS: $\mathbb{Z}_7^*$ can be generated by 3 using one element.

3: a generator of $\mathbb{Z}_7^*$

2: NOT a generator.

$\mathbb{Z}_7^* = \langle 3 \rangle$

($G = \langle g \rangle$)
↘ generator.

$(\mathbb{Z}_7^*, 3)$

b. setup: $G = \langle g \rangle$ $|G| = q$

$\mathbb{Z}_q = \{0, 1, \cdots q-1\}$

$F^{Gexp}: \mathbb{Z}_q \to G.$

$x \longmapsto g^x$

Suppose: $y = g^x \in G.$

denote $x := \log_g y$

Say: x is discrete log of y w.r.t. g

Ex: $\mathbb{Z}_7^* = \langle 3 \rangle$ $3^0 = 1$

$g = 3$ $3^1 = 3$

$3^2 = 2$ mod 7

$3^3 = 6$ ←

$3^4 = 4$ ←

$3^5 = 5$

$3^6 = 1$

$\log_3 4 = 4$ i.e. $3^? = 4$

$\log_3 6 = 3$ $3^? = 6$ (in $\mathbb{Z}_7^*$).

b. DL problem

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

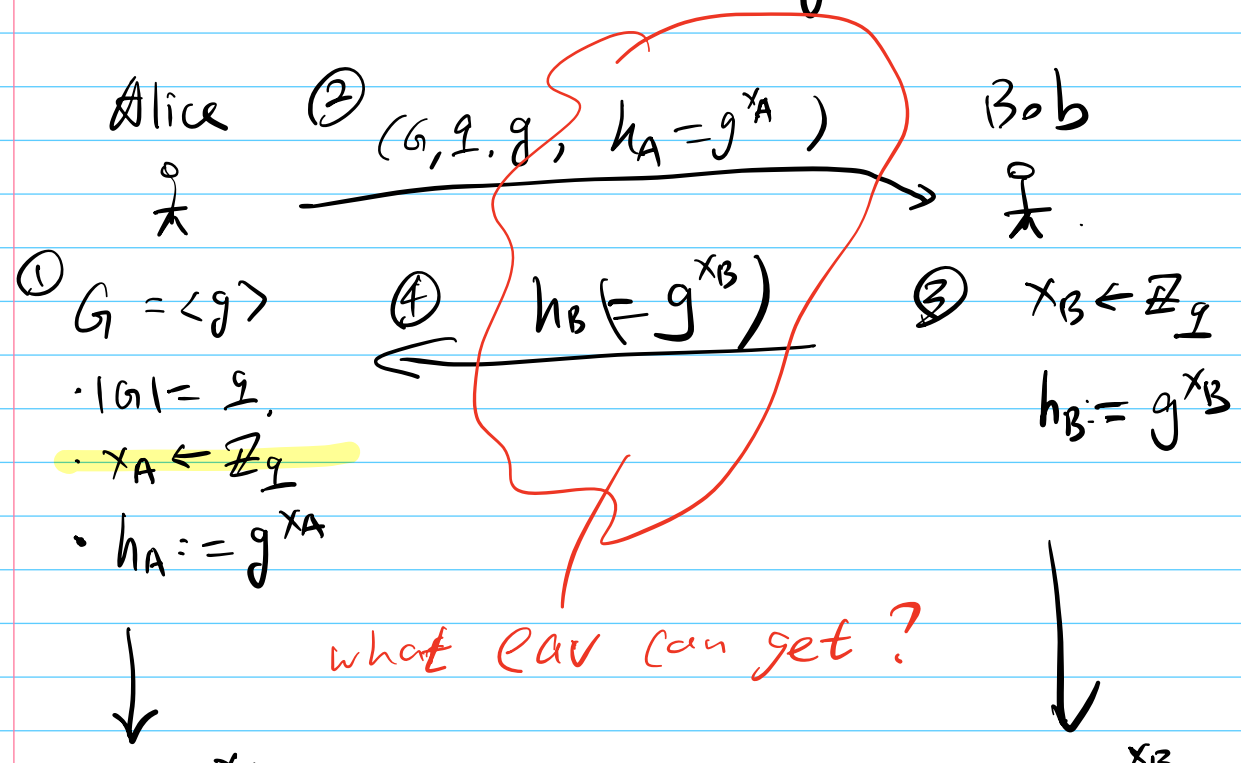
Goal: Find $x \ (:= \log_g y)$

Time: is measured in $\log|G| = n$

→ Best (classical) alg: $\sim 2^{n^{1/3}} \log^c n$

> DL assumption:
> inverting $g^x \mapsto x$ is hard.

c. Diffie-Hellman key exchange



Correctness: $k_A = h_B^{x_A} = (g^{x_B})^{x_A} = g^{x_B \cdot x_A}$

$k_B = h_A^{x_B} = (g^{x_A})^{x_B} = g^{x_A \cdot x_B}$

Security: eav see $h_A = g^{x_A}$, $h_B = g^{x_B}$

$? \Rightarrow k = g^{x_A x_B}$

04/09 251 Lec 4

1. DL Cont'd.

a. DH KE Recap

b. ElGamal Public-Key Encryption

(KeyGen, E, D)

- KeyGEN:

G, $|G| = q$, $G = \langle g \rangle$

$x \leftarrow \mathbb{Z}_q$ $\quad h := g^x$

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

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

- E: on pk, msg. m.

$y \leftarrow \mathbb{Z}_q$.

$c_1 = g^y$

$c_2 = h^y \cdot m$

$(k = g^{xy})$

$c = (c_1, c_2)$.

ciphertext.

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

(knows sk: x)

$\rightarrow k = c_1^x = g^{xy}$

$\rightarrow k^{-1} \cdot c_2 = \underbrace{k^{-1} \cdot k}_{= 1} \cdot m$

$= m$

#

* DDH assumption $\Rightarrow$ ElGamal security.

(Decisional DH assumption)

2. Migrating to abstract Algebra

a. $(\mathbb{Z}_N, +)$ $(\mathbb{Z}_N^*, \cdot)$

- closure: $a, b \in \mathbb{Z}_N$ $a+b \bmod N \in \mathbb{Z}_N$
- Associativity (结合律)

  $(a+b)+c \bmod N = a+(b+c)$

  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \bmod N$
- Identity (单位元) e

  $(\mathbb{Z}_N, +)$ 0 $\forall a \in \mathbb{Z}_N$, $a+0 = 0+a = a$

  $(\mathbb{Z}, \cdot)$ 1 $\forall a \in \mathbb{Z}_N^*$ $a \cdot 1 = 1 \cdot a = a$
- Inverse (逆)

  $\forall a$, $\exists a'$ s.t. $a+a' = 0 \bmod N$

  $a \cdot a' = 1 \bmod N$

↓

b. **Group**

Def: $(G, \circ)$ $\circ : G \times G \to G$ is a group.

if satisfying

- closure (under $\circ$)
- Associativity
- Identity
- Inverse.

→ $(\mathbb{Z}_N, +)$, $(\mathbb{Z}_N^*, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$

- (Abelian group) Commutativity.

$\forall a, b \in G \quad a \circ b = b \circ a$.

- Example: $A = \{0,1\}^n$, $\oplus$: bit-wise XOR

$x = x_1 \cdots x_n$

$y = y_1 \cdots y_n$

$x \oplus y = z = z_1 \cdots z_n$

$z_i = x_i \oplus y_i$

a	b	a⊕b
0	0	0
0	1	1
1	0	1
1	1	0

Claim: $(A, \oplus)$ is a group (Abelian)

Pf:
- closure ✓
- Associativity:

$\forall a, b, c \in \{0,1\}^n : (a \oplus b) \oplus c \stackrel{?}{=} a \oplus (b \oplus c)$ ✓

- identity

$e \in \{0,1\}^n$ s.t. $\forall x \in \{0,1\}^n$

$e \oplus x = x \oplus e = x$

✓ $e = 0^n$

- inverse $\forall x \in \{0,1\}^n$

$\exists x' \in \{0,1\}^n$ s.t. $x \oplus x' = e = 0^n$

$x' = \bar{x}_1 \bar{x}_2 \cdots \bar{x}_n$

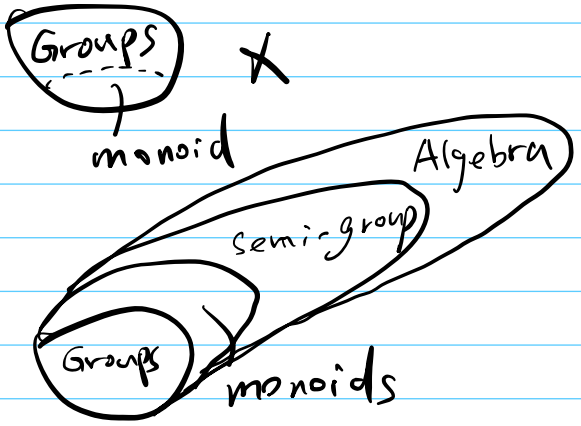
- Commutativity: $\forall x, y \quad x \oplus y = y \oplus x$

c. Monoid

- closure
- Associativity
- Identity
- ~~Inverse~~

] → Group.

(G, ∘) : All but inverse is called a monoid [幺半群]



d. Semi-group

(G, ∘) : closure + Assoc.

NOT : identity, inverse

is called a semi-group.

e. Algebra (structure / system)

Def: An algebra consists of a set $A \neq \emptyset$, and operation $\circ : A \times A \to A$ s.t. closure holds

$\forall x, y \in A, \quad x \circ y \in A$.

- Exercise:

- $(\mathbb{R}, +)$: Group ✓

- $(\mathcal{P}(X), \cup)$ X: set.

$\mathcal{P}(X)$: powerset $= \{S : S \subseteq X\}$.

$\cup$: $S_1, S_2 \subseteq X$, $S_1 \cup S_2$

~~inverse~~

monoid.

- $(\mathbb{Q}, \div)$ $(6 \div 3) \div 2 \neq 6 \div (3 \div 2)$ Algebra

- $(\mathbb{Z}, \div)$ ~~nothing~~

- $(M_n, \cdot)$ M_n: $n \times n$ matrix

$\cdot$: matrix mult.

→ $(A \cdot B) \cdot C \stackrel{?}{=} A \cdot (B \cdot C)$ ✓

→ $\mathbb{1} = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$

→ ~~Inverse~~

monoid ✓

- Algebra
- semigroup
- monoid
- group

↑ IU