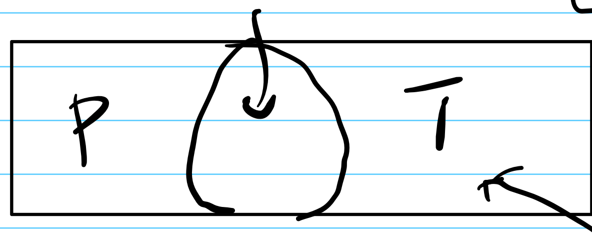
03/18 251 Lec 1

宋方 fang.song@pdx.edu
fangsong.info

163.DS



CS

P: coding. hands-on

T: Theory

250/251 Discrete math

Typical topics

250

- □ set theory
- □ Math proofs
- △ Graph theory
- ◇ probability theory

251

- ○ Logic
- ☆ Algebraic structure (a.k.a. abstract algebra)

others

- △ combinatorics
- ☆ number theory
- ◇ linear Algebra

• why bother?

- □ : foundations
- ◇ ML/AI / Data Science
- ○ : PL
- ☆ : ~~cryptography~~ / Communications / DL

1. A few motivating problems.

- **Factoring:** <u>Given</u>: $n = p \cdot q$ (p, q prime)

  <u>Find</u>: p. ($n = 33$, $p = 3$, $q = 11$)

- Pell's eqn:

  <u>Given</u>: d integer

  <u>Find</u>: <u>Integer</u> soln (x, y) s.t.

  $$x^2 - dy^2 = 1$$

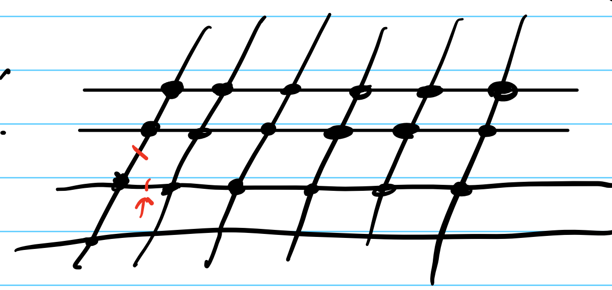
  x: unknown, d: known, y: unknown

  e.g. $d = 2$, $x^2 - 2y^2 = 1$

  $(x = 3,\ y = 2)$

  $$\{ (s,t) : s + \sqrt{2}\,t = (3 + \sqrt{2}\,2)^n \}$$

<u>Lattice</u>, (格).



- SVP (shortest vector problem)

  <u>Given</u> lattice Λ

  <u>Find</u>: $v \in \Lambda$ s.t. $\|v\|$ min.

All fundamental to modern crypto / comm!

· Diophantine eqn's:

find <u>integer</u> soln's. to eqn's.

- <u>linear</u>: $ax+by=c$. integers / unknown

- <u>q</u>uadratic: $ax^2+by^2=c$.

- $x^n+y^n=z^n$ $\begin{cases} n=1: & x+y=z \text{ easy} \\ n=2 & x^2+y^2=z^2 \text{ (勾股定理)} \\ \boxed{n\geq 3}: & \text{no non-trivial int. soln's.} \end{cases}$

Andrew Wiles.

Fermat's Last Theorem

- <u>Hilbert's</u> 10th <u>problem</u>

Is there an algorithm deciding if D'eqn. has a soln'?

$\Downarrow$

$\boxed{\text{HALTING problem}}$ ✗

uncomputable

∃ problems uncomputable by any computer!

2. Algebraic Structures

a. what an algebra?

$\boxed{\text{Set + operation}}$

- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$ $(\mathbb{R}, +, \cdot)$
- X : set

$\mathcal{P}(X) := \{ Y \subseteq X \quad \}$
(power set)

$(\mathcal{P}(X), \cup)$

ABSTRACT: $\longleftrightarrow$ Concrete
develop generic properties/techniques | gain intuition, sanity check

what's common?

$3+5 = 8 \in \mathbb{R}$

$\sqrt{2} \cdot 3 = \sqrt{2} \cdot 3 \in \mathbb{R}$

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

☆ $\Rightarrow$ set is closed under the operation

$\forall x, y \in S, \ x \text{ op'} y \in S.$

- DEF: An algebra (structure/system) consists a set $A \neq \emptyset$ and operations: $f_1, \cdots, f_k$

s.t. for all i, A is closed under f_i.

i.e. $\forall i$, $f_i : \underbrace{A \times \cdots \times A}_{n_i} \to \underline{\underline{S_i}}$

$\forall\ x_1 \cdots x_{n_i}$: $f_i(x_1 \cdots x_{n_i}) \in A$.

(i.e. $S_i \subseteq A$)

- usually consider binary op's: $f_i : A \times A \to A$.

Notation: $\begin{pmatrix} \circ \\ \cdot \\ + \\ \times \\ * \end{pmatrix}$

b. Special algebras.

- Commutative algebra: $\forall\ a, b \in A$
  $a * b = b * a$
- DEF: [Semigroup]. $(A, *)$ algebra.
  is called a semigroup, if $*$ is associative
  $\forall\ x, y, z \in A$, $(x * y) * z = x * (y * z)$

$\Rightarrow$ Can define (abstract) exponentiation.

$$a^n := \underbrace{a * a * \cdots * a}_{n \text{ times}}.$$

Ex: $(\mathbb{R}, \cdot)$ a^n is ordinary exp.
$(\mathbb{R}, +)$, $a^n := a + \cdots + a \ (= na)$

- DEF: [monoid (独异点)]

$\parallel$

Semigroup + identity (单位元)

$\exists\, e \in A$, s.t. $\forall x \in A$, $x * e = e * x = x$

Ex: $(\mathbb{R}, +)$ $e = \underline{0}$

$(\mathbb{R}, \times)$ $e = \underline{1}$

$(P(X), \cup)$ $e = \underline{\phi}$

- Thm: If $(S, *)$ is a semigroup.

& S is finite.

Then: $(S, *)$ has an element b

w/ $b^k = b$ $\forall k \geq 1$

$(b = e?) \rightarrow$ if $(S, *)$ monoid ✓

if NOT, $\nexists$ identity.

How to show it?

- pf: $\boxed{\forall a} \in S$ consider

$a^1, a^2, a^3, \cdots\cdots a^i, \cdots a^j, \cdots \in S$

B/c S finite, must repeat

[pigeon hole principle]

say $a^i = a^j \quad (i<j)$

$l = j - i$

$$a^j = \boxed{a^l * a^i = a^i}$$

$\boxed{\forall\ q \geq i}$ $a^q = \cancel{a^{q-i} * \boxed{a^i}}$ $a^i * a^{q-i}$

$= \cancel{a^{q-i} * a^l * a^i}$ $a^l * (a^i * a^{q-i})$

$= a^l * a^q$

B/c $l \geq 1$, $\exists$ integer $t > 0$, s.t. $t \cdot l \geq i$

$$a^{tl} = \underline{a^l} * \underline{a^{tl}}$$

$$= \underline{a^l * (a^l} * a^{tl})$$

$\vdots$ t times

$$= a^{tl} * a^{tl}$$

$b := a^{tl}$ $\quad b = b * b * b * \cdots * b$

$= b^k \quad \forall k \geq 1$

$\#$

03/19 251 Lec 2

0. Warm-up

Algebra $(A, \circ, *, \cdot, + \cdots)$ [Closure]

$(A, \circ)$: $\circ : A \times A \to A$

Semigroup $(a \circ b) \circ z = a \circ (b \circ z)$ [Associativity]

monoid. semigroup [identity e]

a. where do they belong?

$(\mathbb{R}, +)$ ✓, $(P(X), \cup)$ ✓, $(M_n, \cdot)$ ✗

monoid

$M_n := \{n \times n \text{ matrices}\}$,

$\cdot$: matrix mult.

Associativity ~~?~~ ✓

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

Algebra

$(\mathbb{Q}, +)$ ✓, $(\mathbb{Q}, \div)$ ✗, $\boxed{(\mathbb{Z}, \div)}$

$(6 \div 3) \div 2 \neq 6 \div (3 \div 2)$

$3 \div 2 \notin \mathbb{Z}$ NOT An Algebra.

b. which are commutative? $a \circ b = b \circ a$

c. subalgebra.

· DEF $(A, *)$ algebra.

$S \subseteq A$, if $(S, *)$ is an algebra.

i.e. $\forall a, b \in \boxed{S}$
$a * b \in \boxed{S}$

then $(S, *)$ call it a <u>subalgebra</u> of $(A, *)$.

<u>Example</u>: $(\mathbb{Q}, +)$ is $(\mathbb{R}, +)$ a subalgebra.

1. Basics of <u>Groups</u>.

Group = Monoid + <u>Inverse</u>

· <u>DEF</u>: $(G, \circ)$ $\circ: G \times G \to G$. is group.

if satisfying.

monoid $\begin{cases} \text{- (closure under } \circ) \\ \text{- (Associativity)} \\ \text{- (identity)} \quad e \end{cases}$

- (Inverse): $\forall a \in G$, $\exists a' \in G$

s.t. $a \circ a' = a' \circ a = e$

a' is called <u>inverse</u> of a.

$(\mathbb{R}, +)$ ✓ ? $\forall a \in \mathbb{R}$ $\exists a' \in \mathbb{R}$ s.t. $a + a' = 0$

$(\mathbb{R} / \{0\}, \times)$ ✓ $\forall a \in \mathbb{R}$. $\exists a' \in \mathbb{R}$ s.t. $a \cdot a' = 1$

- **Abelian group** Commutativity:
  $\forall a, b \in G.\ a \circ b = b \circ a$

(Abel)
Hermite (反*)

- $(A = \{0,1\}^n, \oplus)$ $\oplus$: bitwise XOR.

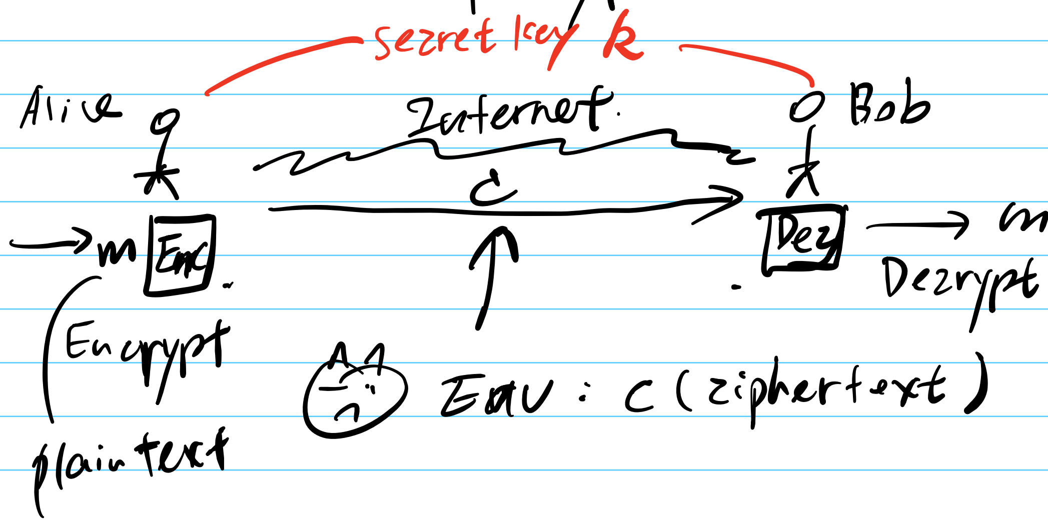
$x = x_1 \cdots x_n$
$y = y_1 \cdots y_n$
$x \oplus y = z = z_1 \cdots z_n$
$z_i = x_i \oplus y_i$

a	b	a⊕b
0	0	0
0	1	1
1	0	1
1	1	0

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

Pf:
- Closure.
- Assoziatity: $\forall x, y, z$
  $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- identity. $e \in \{0,1\}^n, \forall x \in \{0,1\}^n$ $x \oplus e = e \oplus x = x$
  $\Rightarrow e = 0^n$
- inverse. $\forall x \in \{0,1\}^n$
  $\exists x' \in \{0,1\}^n$ s.t. $x \oplus x' = 0^n$
  $a \oplus a = 0$
  $x' = x$ is inverse of x
- commutativity: $\forall x, y$ $x \oplus y = y \oplus x$

2. A first touch of crypto



$$\text{Enc}: \ (m, k) \to c$$

$$\text{DEC}: \ (c, k) \to m$$

<u>Kerckhoff's</u> Law: Enc / Dec Alg's are known by all, esp. <u>attackers</u>.

c. <u>one-time pad</u> (OTP)

- <u>KeyGen</u>: $k \xleftarrow{\$} \{0,1\}^n$ (uniformly random)
- E: on input $m \in \{0,1\}^n$

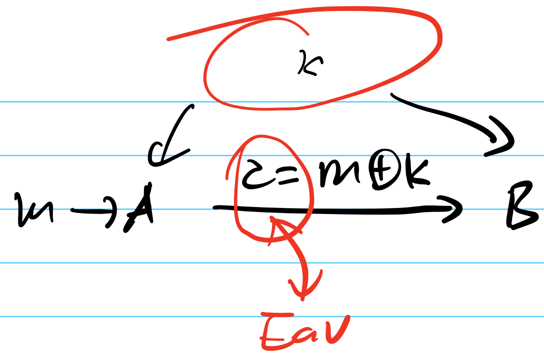
  $c := m \oplus k$

- D: on ciphertext c

  $$\begin{aligned} m &:= c \oplus k \\ &= (m \oplus k) \oplus k \\ &= m \oplus (k \oplus k) \\ &= m \oplus 0^n = m \end{aligned}$$

→ correctness

→ security



Eav: observe c.

$\longrightarrow$ infer m?

★ <u>Observation</u>: works in any group.

? key exchange

3. Number theory in 20 mins

a. modular arithmetic.

- $a, N \in \mathbb{Z}$, $N \geq 2$.

$$a = \underbrace{q}_{\text{quotient}} \cdot N + \underbrace{r}_{\text{remainder}}$$

N: Modulus

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

$a = b \mod N$

iff a, b have same remainder divided by N.

- $\mathbb{Z}_N := \{0, \cdots, N-1\}$.
  - mod N add: $+_{\text{mod}_N}$ $(+_N)$
  - mod N mult: $\cdot_{\text{mod}_N}$ $(\cdot_N)$

$N = 15$, $\mathbb{Z}_N = \{0, \cdots, 14\}$.

$7 + 14 = 6 \mod N$

$3 \cdot 9 = 12 \mod N$

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

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

Cor. $(\mathbb{Z}_N, +_N)$ is a group.

$\forall a \in \mathbb{Z}_N, ?\exists a' \in \mathbb{Z}_N.$

s.t. $a \cdot a' = 1 \mod N$

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

$2 \cdot 1 = 2$

$2 = 4$ $\quad ?\, 1 \mod 6.$

$3 = 0$

$4 = 2$

$5 = 4$

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

  gcd(6, 10) = 2

  - Euclidean Alg. computing gcd(a, b)

- Thm: $a \in \mathbb{Z}_N$ has a mult. inverse iff. $\underline{\gcd(a, N) = 1}$.

  → (coprime)

|

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

Ex $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}.$

$\gcd(a, 6) = 1.$

$\mathbb{Z}_6^* := \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$

<u>Cor</u>: $(\mathbb{Z}_N^*, \cdot \bmod N)$ is a group.

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

  <u>FACT</u>: $\phi(p \cdot q) = (p-1) \cdot (q-1)$

  <u>Ex</u>: $\phi(6) = (2-1)(3-1) = 2$

- Modular exponentiation
  - $a \in \mathbb{Z}_N$, $b > 0$
  - $a^b \bmod N := \underbrace{a \cdot \ldots \cdot a}_{b \text{ times}} \bmod N$ $\quad \|\cdot\|$: size
  - <u>Repeated</u> squaring alg: $\mathrm{poly}(\|a\|, \|b\|, \|N\|)$.

- <u>Thm</u> (Euler's Thm).

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

03/25 251 Lec 3

0. warm-up

a. Repeated squaring

$6^{\boxed{9}} \bmod 11$ $\qquad a=6,\ b=9,\ N=11$

① : $6^1 = 6$

$6^2 = 36 = 3 \quad \bmod 11$

$6^4 = 9$ $\qquad (a^{2^k} \cdots)$

$6^8 = 9^2 = 81 - 11 \times 7 = 4$

$\vdots$

② exponent $9 \overset{\text{binary rep.}}{=} 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$

③ $6^9 = 6^{2^3+1} = \underline{6^{2^3}} \cdot \underline{6^{2^0}} = 4\cdot 6$

$= 2 \quad \bmod 11$

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

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

- $\phi(N) = \phi(33) = (3-1)\cdot(11-1) = 20.$
- $\mathbb{Z}_{33}^* := \{1, 2, 4, 5, 7, 8, \cdots \}.$

$\gcd(a, 33) = 1$ $\qquad \phi(N) = |\mathbb{Z}_N^*|$

- $2^{22} \bmod 33 = \underset{\underset{1\ \text{(By Euler thm)}}{\parallel}}{2^{20}} \cdot 2^2 = 4 \bmod 33$
- let $e = 7$, $\gcd(e, \phi(N)) = \underline{\gcd(7, 20)} = 1$

$\checkmark \exists ? d$ s.t. $e\cdot d = 1 \bmod \underline{20}$ $\quad [\bmod \phi(N)]$

$d = 3$. ✓

1. Factoring & RSA

a. Factoring:

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

Goal: find p (& q).

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

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 2 functions:

$$F_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \qquad x \longmapsto x^e \mod N$$

$$F_d : \mathbb{Z}_N^* \to \mathbb{Z}_N^* \qquad y \longmapsto y^d \mod N$$

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

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

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

$ed = 1 \mod \phi(N)$

$ed = k \cdot \phi(N) + 1$

$= \underbrace{x^{k \cdot \phi(N)}}_{1} \cdot x = x \mod N$ ✗

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

<u>Conj</u>: inverting F_e $(x^e \bmod N) \mapsto x$
is <u>hard</u> w.o. d.

c. RSA app: exchange a secret key in public

Alice ② publish (N, e) Bob

④ $\xleftarrow{\quad y \quad}$

① Generate $(N = p \cdot q,\ e,\ d)$

③ choose $x \leftarrow \mathbb{Z}_N^*$ at random

compute $\boxed{y} = x^e \bmod N$

Eav

$\underbrace{x := y^d \bmod N \qquad\qquad x}_{\text{key}}$ ⑤

- correctness ✓
- security: eav sees $(N,\ e,\ y = x^d \bmod N)$

$\downarrow$

Computing x is hard (w.o. knowing d)

2. Cyclic groups (循环群).

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

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

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

- $3^0 = \underline{1}$ $\quad 3^1 = \underline{3}$ $\quad 3^2 = \underline{2}$ $\quad$ mod 7

$3^3 = \underline{6}$ $\quad 3^4 = \underline{4}$ $\quad 3^5 = \underline{5}$ $\quad 3^6 = \underline{1}$

- $2^0 = \underline{1}$ $\quad 2^1 = \underline{2}$ $\quad 2^2 = \underline{4}$

$2^3 = \underline{1}$ $\quad 2^4 = \underline{2}$ $\quad 2^5 = \underline{4}$ $\quad 2^6 = \underline{1}$

<u>OBS</u>: $\mathbb{Z}_7^*$ can be generated by (3)

using <u>one element</u>

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

2: NOT a generator.

. <u>DEF</u>: G: a group. $|G| = n$.

suppose $\exists g \in G$ s.t.

$\underbrace{g^1, \dots\dots g^n}_{n}$ all <u>distinct</u>.

$(\Rightarrow$ cover all of $G)$

Then G is called a cyclic group.

$G = \langle g \rangle \qquad (\mathbb{Z}_7^* = \langle 3 \rangle).$

g : a generator.

<u>Thm</u>: $\mathbb{Z}_p^*$ is cyclic for any prime p.

b. Discrete logarithm (DL)

· Setup: $G = \langle g \rangle$, $|G| = q$

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

$$F^{Gexp} : \mathbb{Z}_q \to G$$
$$x \mapsto g^x$$

$$\boxed{\begin{array}{l} \text{vs. RSA} \\ x \mapsto x^e \end{array}}$$

<u>Suppose</u>: $y = g^x \in G$

Denote: $x := \log_g y$

Say: x is <u>discrete log</u> of y <u>w.r.t g</u>

<u>Ex</u>: $\mathbb{Z}_7^* = \langle 3 \rangle$ $\quad 3^0 = 1$

$g = 3$ $\quad 3^1 = 3$

$3^2 = 2$ $\quad$ mod 7

$3^3 = 6$

$3^4 = 4$

$3^5 = 5$

$\log_3 4 = \underline{4}$ $\qquad$ (i.e. $3^? = 4$ in $\mathbb{Z}_7^*$)

$\log_3 6 = \underline{3}$

- DL problem

  <u>Given</u>: $G = \langle g \rangle$, $y (= g^x)$

  <u>Goal</u>: Find x $(:= \log_g y)$

  <u>Time</u>: is measured in $\log|G| = n$.

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

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

03/26 251 Lec4

0. Warm-up.

a. RSA exercise

$N = 33 = 3 \times 11$, $\phi(N) = 20$

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

$d = 3$ $e \cdot d = 1 \mod \phi(N)$

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

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

<u>RSA problem</u>: $y = x^e$ find x $(\mathrm{mod}\, N)$

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

① $7 = 2^2 + 2^1 + 2^0$

② $3^1 = 3$ $\mod 33$

$3^2 = 9$

$3^{2^2} = 3^4 = 9^2 = 81 - 33 \times 2 = 15$

$\vdots$

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

$= 15 \cdot 9 \cdot 3 \mod 33$

$= 9$

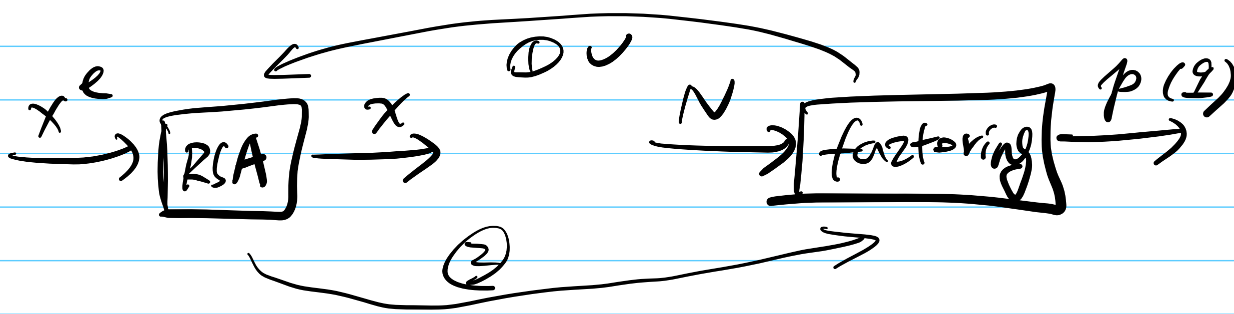
$F_e(3) = 9$

$$\text{Fd: } 9 \mapsto 9^3 = 9^2 \cdot 9 \qquad \mod 33$$
$$= 3^4 \cdot 3^2$$
$$= 15 \cdot 9 = 3$$

6. RSA vs. factoring

RSA problem
Given: $y = x^e$, (N, e)
Goal: find x

Factoring:
Given $N = p \cdot q$
Goal: find p (& q)



① RSA $\leq$ factoring

$N \curvearrowright p \cdot q$

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

$\Rightarrow d = e^{-1} \mod \phi(N)$

② factoring $\leq$ RSA ??? unknown

Big open question

Known: $d \leftarrow (N, e)$

$\phi(N) \leftarrow (N, e)$ $\equiv$ factoring

1. DL Cont'd

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

Goal: Find $x := \log_g y$

a. Diffie-Hellman Key Exchange (DHKE).

Alice ② $(\underbrace{G, q, g}_{\text{Group}}, h_A = g^{x_A}) \longrightarrow$ Bob

④ $\longleftarrow h_B = g^{x_B}$

eav

① $G = \langle g \rangle$

- $|G| = q$
- $x_A \leftarrow \mathbb{Z}_q$
- $h_A = g^{x_A}$

③ $x_B \leftarrow \mathbb{Z}_q$

$h_B := g^{x_B}$

⑤

$$\underbrace{K_A := h_B^{x_A} \qquad\qquad K_B := h_A^{x_B}}_{\text{Same key}}$$

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, h_B

Eav's <u>Goal</u>: $(g^{x_A}, g^{x_B}) \longmapsto g^{x_A \cdot x_B}$

One sufficient approach:

<u>Compute</u>: $x_B := \log_g h_B$ (then $h_A^{x_B}$)

$x_A := \log_g h_A$ (then $h_B^{x_A}$)

This approach is infeasible:

if we believe DL is hard!

$(g^{x_A}, g^{x_B}) \longmapsto g^{x_A \cdot x_B}$ is hard ?

by any approach

b. computational DH (CDH).

$\boxed{\text{Computing } g^{x_A \cdot x_B} \text{ from } (g^{x_A}, g^{x_B}) \text{ is hard!}}$

$\Rightarrow$ Eav cannot compute key: $g^{x_A x_B}$

$g^{x_A \cdot x_B}$ will be treated as a key

better look <u>random</u>!

c. Dezisional DH (DDH)

$(G, q, g, g^{x_A}, g^{x_B}, \underline{g^{x_A \cdot x_B}})$ real world

$\approx (G, q, g, g^{x_A}, g^{x_B}, g^{x_z})$ ideal world.

$x_z \leftarrow \mathbb{Z}_q$

g^{x_z} is unif. random in G, indep of everything else

indistinguishable:

if no one can tell a differenze, then they are the "same"!

d. Relations DL, CDH, DDH

$$DDH \leq CDH \leq DL$$

??? Big open problem

2. Pub-key Enc.

Alice $\xrightarrow{g^x}$ Bob $(x_A \to x,\ x_B \to y)$

$\xleftarrow{g^y}$

key: g^{xy} $\quad\xleftarrow{c = g^{xy} \circ m}\quad$ g^{xy}

(group op). send $m \in G$

$(g^{xy})^{-1} \circ c =$

$\cancel{(g^{xy})^{-1} \circ g^{xy}} \circ m = m$

$x \leftarrow \mathbb{Z}_q$

$g^x \rightarrow$ g^x public

Bob

I want to send "m"

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

① Compute g^y

$(g^x)^y$

$g^{xy} \circ m$

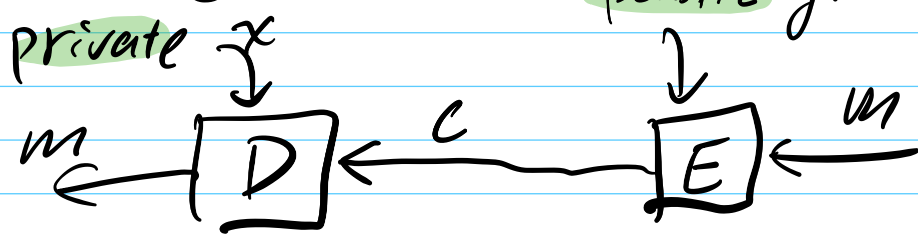
$\leftarrow (g^y, g^{xy} \circ m)$

② $C = (c_1, c_2)$

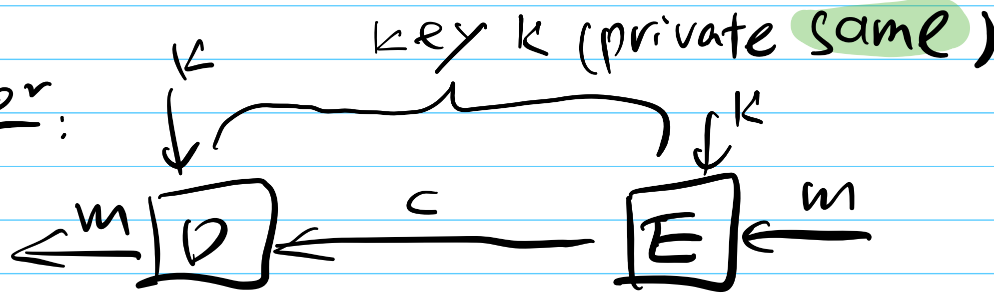
③ Compute. $c_1^x = g^{xy}$

$\cdot\ (g^{xy})^{-1} \cdot c_2 = m$

New setting



Prior:



Enc/DEC : same key & Private

Symmetric-key Enc

(private-key Enc)

Enc key $\neq$ dec key & Enc key Public

Asymmetric-key enc / Public-key ENC

- **DEF:** PubKE is a triple of alg's.

$\pi = (KG, E, D)$

- KG: $(pk, sk) \leftarrow KG(1^n)$

public key for Enc — secret key for dec.

- E: $c \leftarrow E(pk, m)$
- D: $m \leftarrow D(sk, c)$

<u>Correctness</u>: $D_{sk}(E_{pk}(m)) = m$

$\Downarrow$ DHKE $\Rightarrow$ El Gamal Pubkey Enc.

- KG: $G = \langle g \rangle$, $x \leftarrow \mathbb{Z}_q$, g^x

$pk = g^x$, $sk = x$

- E: $m \in G$:

$y \leftarrow \mathbb{Z}_q$

$c = (c_1 = g^y, \ c_2 = (g^x)^y \circ m)$

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

$(c_1^x)^{-1} \circ c_2 \rightarrow m$ #

[Post-quantum Cryptograph!]