04/17 251 Lec3

0. Warm-up

a. $a^b \bmod N$

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

Ex:

$6^9 \bmod 11$ $\qquad \underbrace{6 \cdots\cdots 6}_{9 \text{ times}}$

R.S.

① $6^1 = 6$ $\qquad \bmod 11$

$6^2 = \underline{3}$

$6^4 = \underline{9}$ $\qquad 6^{2^k}$

$6^8 = \underline{4}$

$\vdots$

② $9 = 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$

$$6^9 = 6^{2^3+1} = 6^{2^3}\cdot 6^1 \qquad \bmod 11$$

$$= 6^8 \cdot 6^1$$

$$= 4 \cdot 6$$

$$= 2 \quad \bmod 11$$

b. RSA problem

- p, q $\quad$ n-bit prime.
- $N = p\cdot q$. $\quad \phi(N) = (p-1)(q-1)$

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

$$F_e: x \longmapsto x^e \mod N$$

$$F_d: y \longmapsto y^d \mod N.$$

$$F_d(F_e(x)) = x \mod N.$$

- Ex.
  - $p = 3$, $q = 11$, $N = p \cdot q = 33$
  - $\phi(N) = (p-1)(q-1) = 20$
  - pick $e = 7$, $\gcd(7, 20) = 1$
  - compute $d = \underline{3}$ s.t. $(d \cdot e = 1 \mod 20)$

$(N = 33, e = 7, \boxed{d = 3})$.

$x = 2$

$$F_e(x) = \boxed{2}^7 = \overset{16}{2^{2^2}} \cdot \overset{4}{2^{2^1}} \cdot \overset{2}{2^{2^0}} = \mod 33$$

29

$$7 = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$\begin{array}{cccc} 2^0, & 2^1, & 2^2, & 2^4 \\ \| & \| & \| & \| \\ 1 & 2 & 4 & 16 \end{array}$$

$x = 3$.

$F_e(x) = 3^7 = 3^4 \cdot 3^2 \cdot 3^1 = 3 \cdot 9 \cdot 15 \mod 33$

$= 9 \mod 33$

$3^1 = 3$, $\quad 3^2 = 9$, $\quad 3^4 = 9 \times 9 \mod 33 = 15$.

$F_d(9) = 9^3 = 9^2 \cdot 9^1 = 3 \mod 33$

$3 = 1 \cdot 2^1 + 1 \cdot 2^0$

$9^1 = 9$, $\quad 9^2 = 15$

---

config: (N, e, d) $\quad F_e, F_d$

$x^e \mod N$, d unknown

easy F_d $\downarrow$ x $\quad \cancel{\swarrow}$

RSA: Given $x^e \mod N$. Find x

Factoring: Given: $N = p \cdot q$. Find p.

- RSA vs. factoring.
- RSA $\overset{?}{\leq}$ factoring

Given: $N \rightarrow \boxed{\;} \rightarrow p, (q)$

Goal: use B-Box invert.

$x^e \longrightarrow x \pmod N$

$$(x^e)^d = x \mod N$$

Suffices to get d.

(N, e) is known.

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

Need $\phi(N) = (p-1)\cdot(q-1)$ ✓

$$N \to \boxed{S} \to p,\ q$$

↓

✓ Find d then $(x^e)^d = 1 \mod N$.

- factoring $\overset{?}{\leq}$ RSA

$$x^e \to \boxed{RSA} \xrightarrow{x} \quad \Rightarrow \quad N \to \boxed{\text{factoring ???}} \to p$$

? unknown

↳ $d \leftarrow (N, e) \equiv$ factoring.

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

Alice | (N, e) | Bob

(N, e, d) $\leftarrow$ $y = x^e$ | $x \in \mathbb{Z}_N^*$

$(x^e)^d = x$ | $y = x^e \mod N$

1. Cyclic groups.

a. $(\mathbb{Z}_N^*, \cdot \bmod_N)$ $\qquad \mathbb{Z}_N = \{0, \dots, N-1\}$

$= \{a \in \mathbb{Z}_N : \gcd(a, N)\}$ $\qquad$ identity $e = 1$

Spezial case: $N = p$ prime.

* $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

Ex. $\mathbb{Z}_7^* = \{1, 2, \dots, 6\}$.

mod 7

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

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

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

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

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

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

2: NOT a gen.

• **Def.**: G a group. $|G| = n$.

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

$$\underbrace{g^1, g^2, \cdots, g^n}_{n \text{ of them}} \quad \text{all } \underline{\text{distinct}}.$$

(hence all of G.)

<u>Then</u>: G is called a <u>cyclic group</u>.

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

g is called a generator.

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

($\cdot \bmod p$)

b. Discrete logarithm.

• setup:

- $G = \langle g \rangle$, $|G| = \underline{q}$
- $\mathbb{Z}_{\underline{q}} = \{0, \cdots, \underline{q} - 1\}$

$$\boxed{\begin{aligned} F^{GExp}: \mathbb{Z}_q &\to G \\ x &\mapsto g^x \end{aligned}}$$

RSA

$\underline{x} \mapsto \underline{x}^e$

- Suppose : $\underbrace{y = g^x}$ $\in G$.

$x := \log_g y$

x is discrete log of y wrt g

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

$3^3 = 6$ $\quad 3^4 = 4$ $\quad 3^5 = 5$ $\quad 3^6 = 1$

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

$\to \log_3 4 = x = 4$ i.e. $g^x = 4$

$\log_3 6 = 3$

. DL problem.

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

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

[meas. complexity in $\log |G|$]

exhaustive search $\sim |G|$ $\quad$ $\log|G| = n$

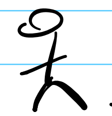
$\to$ Best (classical) Alg : $\sim 2^{n^{1/3} \cdot \log^c n}$

$$\boxed{\begin{array}{c}\text{DL assumption} \\ \text{Inverting } (g^x \mapsto x) \text{ is hard.}\end{array}}$$

2. D.H.K.E (Diffie-Hellman key exchange).

a. D.H.K.E

Alice 

Bob 

$$\xrightarrow{(\overbrace{G, q}^{\text{about } G}, g, h_A = g^{x_A})}$$

$$\xleftarrow{h_B = g^{x_B}}$$

Alice:

$G = \langle g \rangle$

$|G| = q$.

$x_A \leftarrow \mathbb{Z}_q$

$h_A := g^x$

$$\downarrow$$

$$K := h_B^{x_A} = (g^{x_B})^{x_A}$$

$$= g^{x_A \cdot x_B}$$

Bob:

$x_B \leftarrow \mathbb{Z}_q$; h_A

$h_B := g^{x_B}$

$$\downarrow$$

$$K := h_A^{x_B} = (g^{x_A})^{x_B}$$

$$= g^{x_A \cdot x_B}$$

Eav sees: $(h_A, h_B) \xrightarrow{???} K = g^{x_A \cdot x_B}$

$h_A = g^{x_A}$, $h_B = g^{x_B}$

x_B $\quad$ x_A

$$h_A^{x_B} = K$$

Compute $x_B := \log_g h_B$ OR $x_A := \log_g h_A$

DL hard!

hard!

Eav needs $\boxed{\begin{matrix} g^{x_A} & g^{x_B} \\ \parallel & \\ (h_A, & h_B) \mapsto g^{x_A x_B}\end{matrix}}$

b. Computational DH assumption (CDH)

$\rightarrow$ computing $g^{x_A x_B}$ from g^{x_A} & g^{x_B} is hard!

$\Rightarrow$ Eav cannot compute $k = g^{x_A x_B}$.

☹ $k = g^{x_A x_B}$ if treated as a key

k better look random.

$\downarrow$

Decisional DH (DDH).

$$(G, q, g, g^{x_1}, g^{x_2}, g^{x_1 x_2})$$
$$\approx$$
$$(G, q, g, \underbrace{g^{x_1}, g^{x_2}, g^{x_3}}_{\text{indep.}})$$