

CSCI 1510

This Lecture:

- Basic Group Theory
- Factoring / RSA Assumptions
- DLOG / CDH / DDH Assumptions

Basic Number Theory

- $a \mid b$: a divides b ($b = a \cdot c$)
- Primes: an integer $p > 1$ that only has 2 divisors: 1 & p .
- Modular Arithmetic:

$a \bmod N$: remainder of a when divided by N

$$a \cdot b \bmod N = (a \bmod N) \cdot (b \bmod N) \bmod N.$$

$a \equiv b \pmod{N}$: a and b are congruent modulo N

How to compute $a^b \bmod N$? Time complexity?

a, b, N all $O(n)$ bits

Basic Number Theory

- $\gcd(a, b)$: greatest common divisor

How to compute $\gcd(a, b)$? Time complexity?

a, b both $O(n)$ bits

Euclidean Alg.

$$\gcd(17, 12) = 1$$

$$17 \bmod 12 = 5$$

$$12 \bmod 5 = 2$$

$$5 \bmod 2 = 1$$

$$2 \bmod 1 = 0$$

$$\gcd(18, 12) = 6$$

$$18 \bmod 12 = 6$$

$$12 \bmod 6 = 0$$

- $\gcd(a, N) = 1$: a & N are coprime

$\Rightarrow \exists b$ st. $a \cdot b \equiv 1 \pmod{N}$: a is invertible modulo N ,

b is its inverse, denoted as a^{-1} .

How to compute b ?

Extended Euclidean Alg.

$$\gcd(17, 12) = 1$$

$$17 \bmod 12 = 5$$

$$12 \bmod 5 = 2$$

$$5 \bmod 2 = 1$$

$$2 \bmod 1 = 0$$

$$5 = 17 - 12 \times 1$$

$$2 = 12 - 5 \times 2$$

$$1 = 5 - 2 \times 2$$

$$\gcd(a, N) = 1$$

$\Downarrow$

$$1 = a \cdot x + N \cdot y$$

$\Downarrow \pmod{N}$

$$1 \equiv a \cdot x$$

Basic Number Theory

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

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

Thm Let $N = \prod_{i=1}^k p_i^{e_i}$. p_i : distinct primes. $e_i \geq 1$.

$$\text{Then } \phi(N) = \prod_{i=1}^k p_i^{e_i-1} (p_i - 1).$$

Example: N is prime. $\phi(N) = N - 1$.

$$N = p \cdot q. \quad \phi(N) = (p-1) \cdot (q-1).$$

Euler's Theorem $\forall a, N$ where $\gcd(a, N) = 1$, $a^{\phi(N)} \equiv 1 \pmod{N}$.

Corollary If $d \equiv e^{-1} \pmod{\phi(N)}$, then $(a^d)^e \equiv a \pmod{N}$.

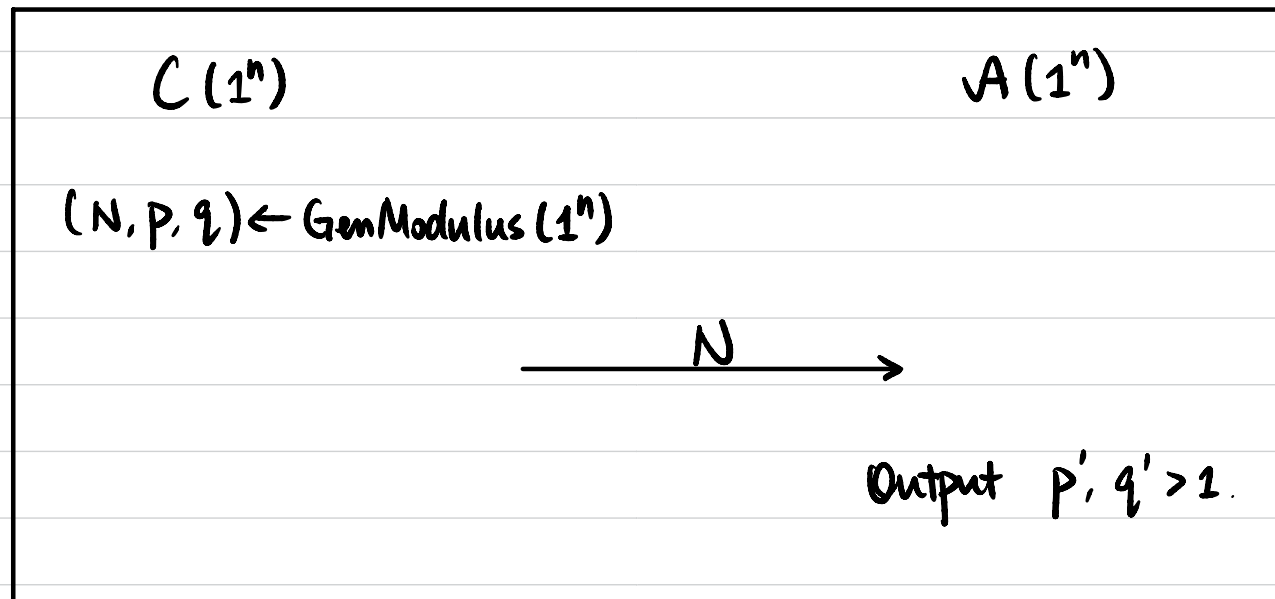
Factoring Assumption

GenModulus (1^n): PPT algorithm, generates $(N, p, q) \leftarrow$ How to generate?

p, q : n -bit primes, $p \neq q$. $N = p \cdot q$

Def Factoring is hard relative to GenModulus if

$\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t. $\Pr[p' \cdot q' = N] \leq \epsilon(n)$.



Factoring $\Rightarrow$ OWF (GenModulus)

RSA Assumption

GenModulus (1^n): generates (N, p, q) . p, q : n -bit primes, $p \neq q$. $N = p \cdot q$

GenRSA (1^n):

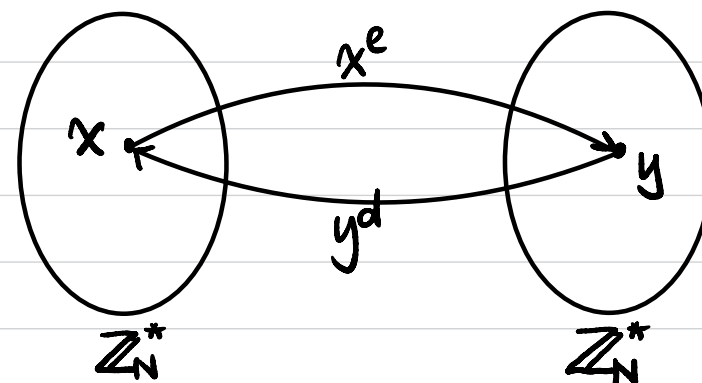
$(N, p, q) \leftarrow \text{GenModulus}(1^n)$

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

Choose $e > 1$ s.t. $\gcd(e, \phi(N)) = 1$

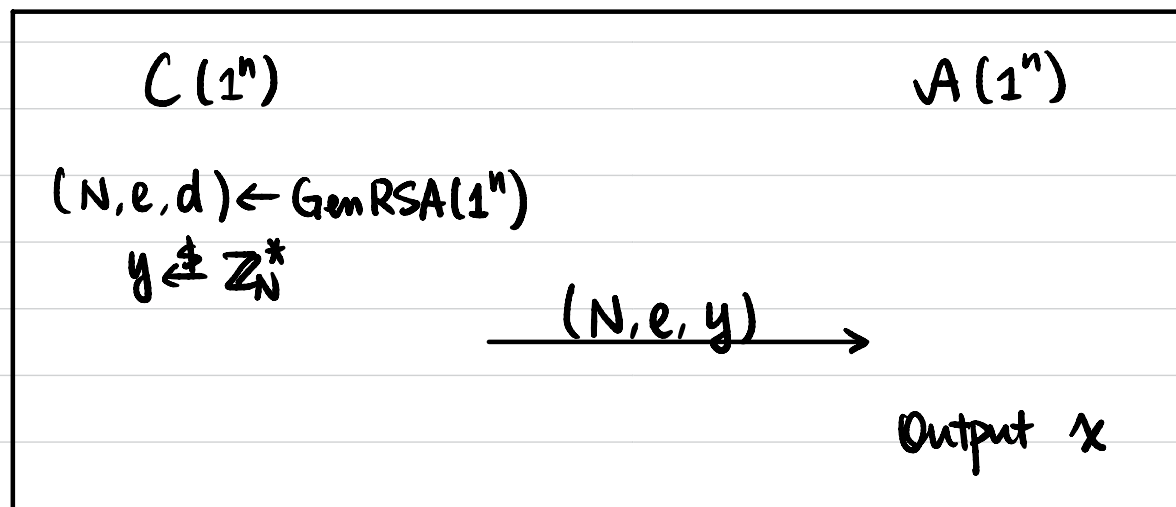
Compute $d := e^{-1} \bmod \phi(N)$

Output (N, e, d)



Def The RSA problem is hard relative to GenRSA if

$\forall \text{PPT } A, \exists \text{negligible function } \epsilon(\cdot)$ s.t. $\Pr[x^e = y \bmod N] \leq \epsilon(n)$.



RSA $\Rightarrow$ Factoring

Basic Group Theory

Def A group is a set G along with a binary operation $\circ$ with properties:

① Closure: $\forall g, h \in G, g \circ h \in G$

② Existence of an identity: $\exists e \in G$ st. $\forall g \in G, e \circ g = g \circ e = g$.

③ Existence of inverse: $\forall g \in G, \exists h \in G$ st. $g \circ h = h \circ g = e$

Inverse of g denoted as g^{-1} .

④ Associativity: $\forall g_1, g_2, g_3 \in G, (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

Exercises: Is this a group?

• $(\mathbb{Z}, +)$

• $(\mathbb{Z}, \cdot)$

• $(G = \{0, 1, \dots, N-1\}, + \text{ mod } N)$

• $(\mathbb{Z}_N^*, \cdot \text{ mod } N)$

Basic Group Theory

Def We say a group is **abelian** if it satisfies:

⑤ **Commutativity**: $\forall g, h \in G, g \circ h = h \circ g$

For a finite group, we use $|G|$ to denote its **order** (# of elements)

$(H, \circ)$ is a **subgroup** of $(G, \circ)$ if $(H, \circ)$ is a group and $H \subseteq G$.

Group Exponentiation

For a group $(G, \circ)$, $g^m := \underbrace{g \cdot g \cdots g}_{m \text{ times}}$

$$g^0 := 1$$

$$g^{-m} := (g^{-1})^m$$

$$g^{m_1} \cdot g^{m_2} = g^{m_1 + m_2}$$

$$(g^{m_1})^{m_2} = g^{m_1 \cdot m_2}$$

$$g^m \cdot h^m = (g \cdot h)^m$$

$$g^{-m} = (g^m)^{-1}$$

Thm Let G be a finite group of order m , then $\forall g \in G, g^m = 1$.

$$\forall \text{ integer } x, g^x = g^{x \bmod m}$$

Basic Group Theory

Def Let G be a finite group of order m .

$\forall g \in G, \langle g \rangle := \{g^0, g^1, \dots, g^{m-1}\}$ is a subgroup of G .

$|\langle g \rangle|$ is the order of g .

G is a cyclic group if $\exists g \in G$ s.t. $\langle g \rangle = G$. g is a generator of G .

Examples: ① If G is a group of prime order, then G is cyclic.

$\forall g \in G, g \neq 1, g$ is a generator of G .

p, q primes $p = 2q + 1$.

Let $g \in \mathbb{Z}_p^*$ be an element of order q .

$H = \langle g \rangle$ is a group of prime order.

② $\mathbb{Z}_p^*$ for a prime p is a group of order $p-1$.

$p = 7, \langle 3 \rangle = \{1, 3, 2, 6, 4, 5\}$

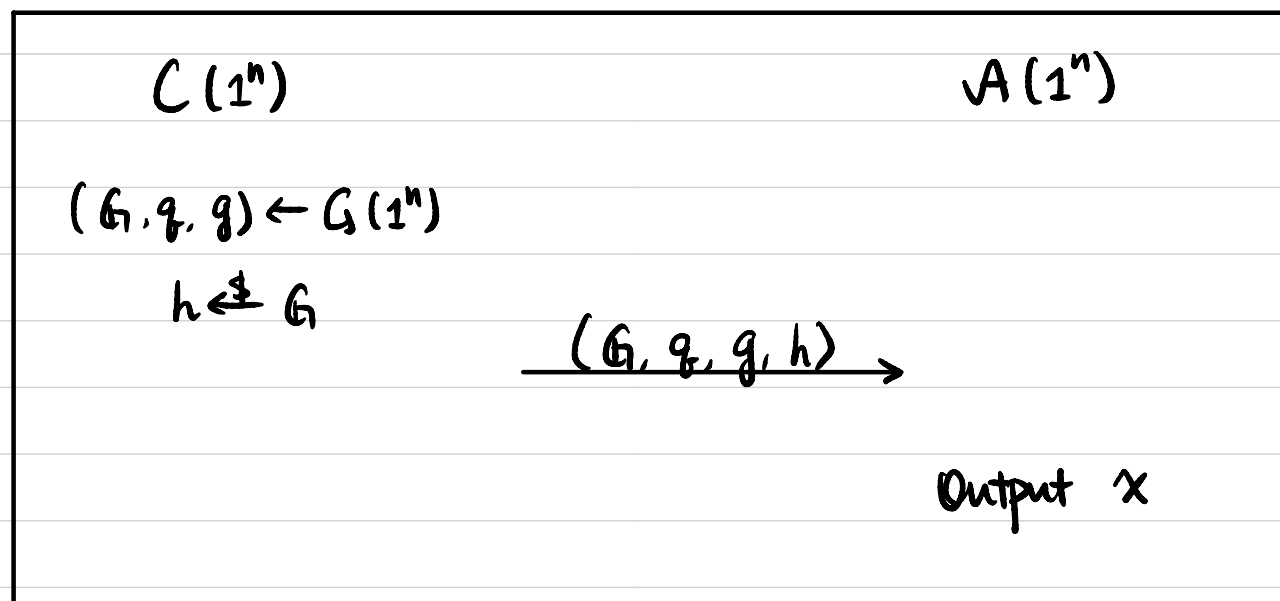
Discrete-Log Assumption

$G(1^n)$: PPT algorithm, generates (G, q, g)

description of a cyclic group G of order q with generator g .
↑
n-bit integer

Def Discrete-Log (DLOG) is hard relative to G if

$\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t. $\Pr[g^x = h] \leq \epsilon(n)$.



DLOG $\Rightarrow$ CRHF

CRHF from DLOG Assumption

- $\text{Gen}(1^n)$:

$$(G, \overset{\text{prime}}{q}, g) \leftarrow G(1^n)$$

$$h \leftarrow G$$

$$\text{Output } s = (G, q, g, h)$$

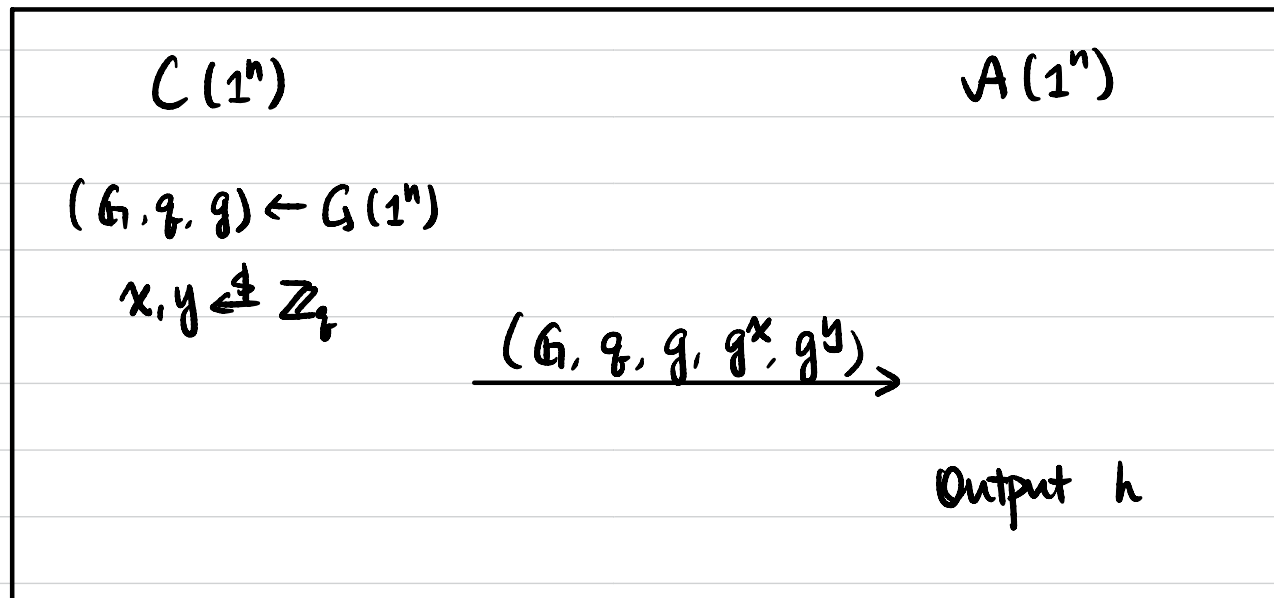
- $H^s(x || y) := g^x h^y$

Computational Diffie-Hellman (CDH) Assumption

$G(1^n)$: PPT algorithm, generates (G, q, g)

Def CDH is hard relative to G if

$\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t. $\Pr[h = g^{xy}] \leq \epsilon(n)$.



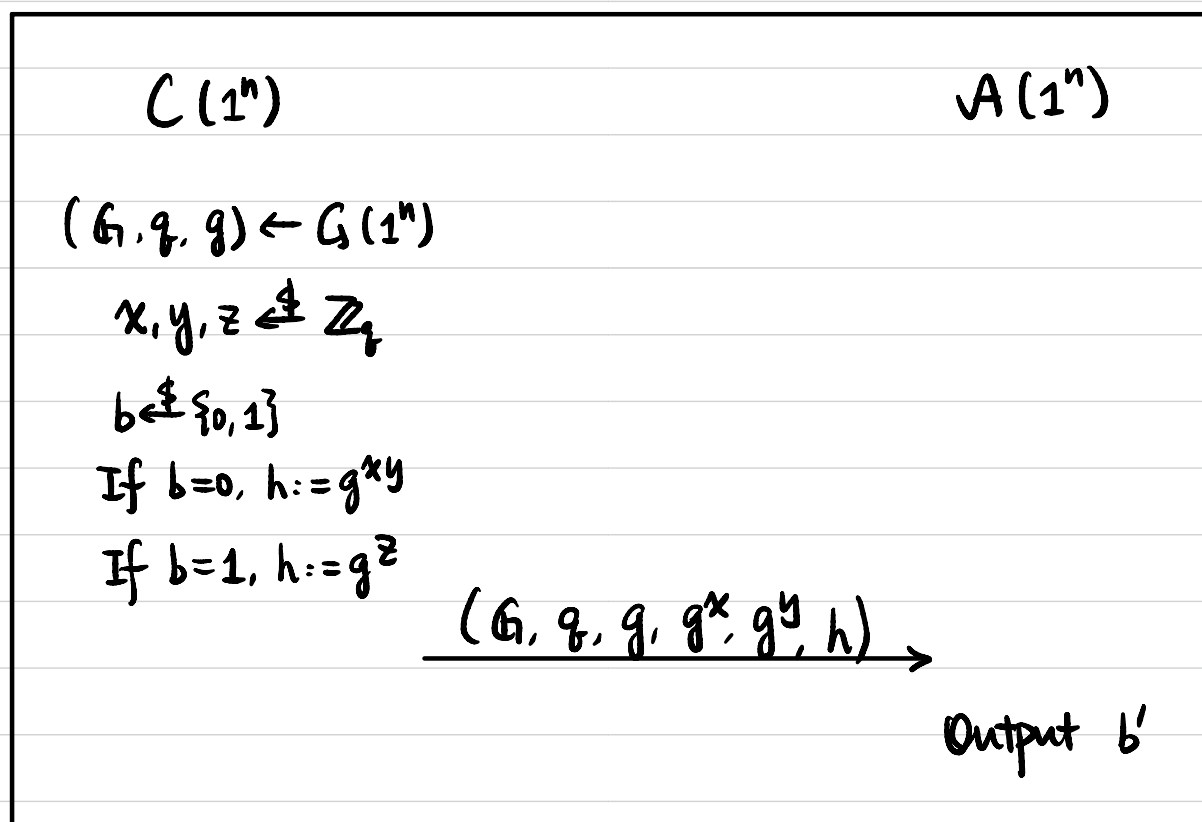
CDH $\Rightarrow$ DLOG

Decisional Diffie-Hellman (DDH) Assumption

$G(1^n)$: PPT algorithm, generates (G, q, g)

Def DDH is hard relative to G if

$\forall$ PPT A , $\exists$ negligible function $\epsilon(\cdot)$ s.t. $\Pr[b = b'] \leq \frac{1}{2} + \epsilon(n)$.



DDH $\Rightarrow$ CDH

