CSCI 1510

- 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? $O(n)$

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

$$b = \sum_{i=0}^{n} b_i \cdot 2^i$$

$a \bmod N$

$a^2 \bmod N$

$a^4 \bmod N$

$\vdots$

$a^{2^n} \bmod N$

$$a^b \equiv a^{\sum_{i=0}^{n} b_i \cdot 2^i} \equiv \prod_{i=0}^{n} (a^{2^i})^{b_i} \bmod N$$

Basic Number Theory

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

How to compute $\gcd(a,b)$? Time Complexity? $O(n)$

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

$\Rightarrow \exists b$ s.t. $a \cdot b \equiv 1 \pmod N$: a is invertible modulo N,
b is its inverse, denoted as a^{-1}.

How to Compute b?

Extended Euclidean Alg.

$\gcd(17, 12) = 1$
$17 \bmod 12 = 5$
$12 \bmod 5 = 2$
$5 \bmod 2 = 1$
$2 \bmod 1 = 0$

$5 = 17 - 12 \times 1$
$2 = 12 - 5 \times 2$
$1 = 5 - 2 \times 2$

$\gcd(a, N) = 1$
$\Downarrow$
$1 = a \cdot x + N \cdot y$
$\Downarrow$ mod N
$1 \equiv a \cdot x$

Basic Number Theory

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

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. $e_i \geq 1$.

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

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

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

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

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

$$\Downarrow$$

$$d \cdot e \equiv 1 \bmod \phi(N)$$

$$\Downarrow$$

$$d \cdot e = \phi(N) \cdot c + 1$$

$$\Downarrow$$

$$a^{de} \equiv a^{\phi(N)\cdot c + 1} \bmod N$$

$$\equiv 1^c \cdot a \bmod N$$

$$\equiv a \bmod N$$

Factoring Assumption

randomly sample $\to$ primality test

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

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

Def Factoring is hard relative to GenModulus if

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

$C(1^n)$		$\mathcal{A}(1^n)$
$(N, p, q) \leftarrow \text{GenModulus}(1^n)$		
	$\xrightarrow{\quad N \quad}$	
		Output $p', q' > 1$.

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):

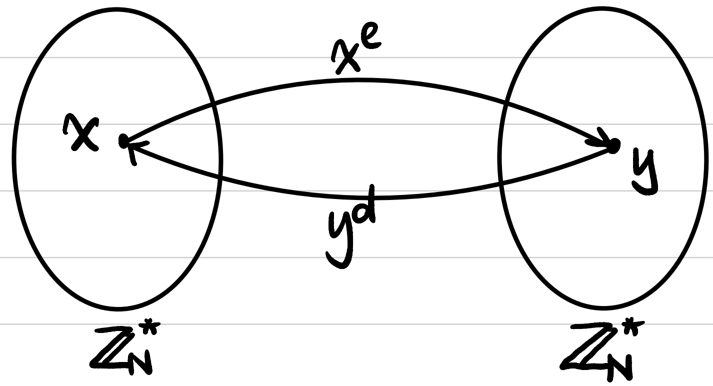
$(N, p, q) \leftarrow \text{GenModulus}(1^n)$

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

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

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

$C(1^n)$		$\mathcal{A}(1^n)$
$(N, e, d) \leftarrow \text{GenRSA}(1^n)$		
$y \xleftarrow{\$} \mathbb{Z}_N^*$		
	$\xrightarrow{(N, e, y)}$	
		Output x

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**: $\exists e \in G$ s.t. $\forall g \in G$, $e \circ g = g \circ e = g$.

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

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?

- $(\mathbb{Z}, +)$ Yes
- $(\mathbb{Z}, \cdot)$ No
- $(G = \{0, 1, \cdots, N-1\}, + \bmod N)$ Yes
- $(\mathbb{Z}_N^*, \cdot \bmod N)$ Yes

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 $(G, \cdot)$, $\quad g^m := \underbrace{g \cdot g \cdots g}_{m \text{ times}} \quad g^0 := 1 \quad g^{-m} := (g^{-1})^m$

$g^{m_1} \cdot g^{m_2} = g^{m_1 + m_2} \quad (g^{m_1})^{m_2} = g^{m_1 \cdot m_2} \quad g^m \cdot h^m = (g \cdot h)^m \quad g^{-m} = (g^m)^{-1}$

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

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

$g_1 \cdot g_2 \cdots g_m = (g \cdot g_1) \cdot (g \cdot g_2) \cdots (g \cdot g_m)$

Basic Group Theory

Def Let G be a finite group of order m.

$\forall g \in G$, $\langle g \rangle := \{g^0, g^1, \cdots, g^{m-1}\}$

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

$|\langle g \rangle|$ is the order 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 cyclic group of prime order q.

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

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

Discrete-Log Assumption

$\mathcal{G}(1^n)$: PPT algorithm, generates $(\mathbb{G}, q, g)$

description of a cyclic group $\mathbb{G}$ of order q with generator g.

n-bit integer

Def Discrete-Log (DLOG) is hard relative to $\mathcal{G}$ if

$\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[g^x = h] \le \varepsilon(n)$.

$\mathcal{C}(1^n)$		$\mathcal{A}(1^n)$
$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$		
$h \xleftarrow{\$} \mathbb{G}$		
	$\xrightarrow{(\mathbb{G}, q, g, h)}$	
		Output x

DLOG $\Rightarrow$ CRHF

CRHF from DLOG Assumption

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

  prime

  $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

  $h \xleftarrow{\$} \mathbb{G}$

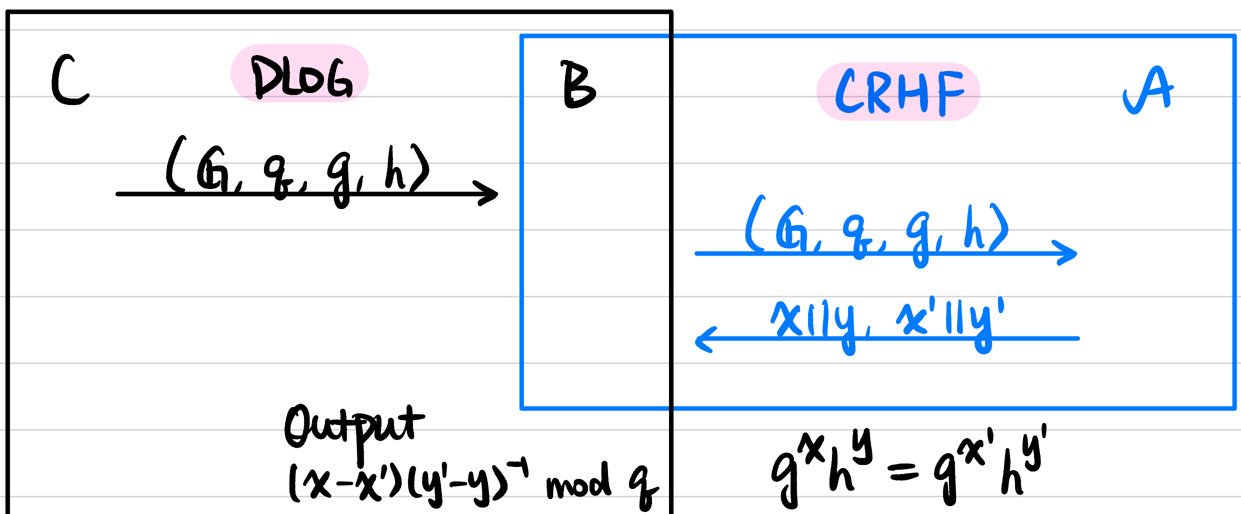
  Output $s = (\mathbb{G}, q, g, h)$

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

Thm If DLOG is hard relative to $\mathcal{G}$, then this is a CRHF.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks collision resistence.

We construct PPT $\mathcal{B}$ to break DLOG.



$$g^x h^y = g^{x'} h^{y'}$$

$$\Rightarrow g^{x-x'} = h^{y'-y}$$

$$\Rightarrow g^{(x-x')(y'-y)^{-1}} = h$$

Computational Diffie-Hellman (CDH) Assumption

$\mathcal{G}(1^n)$: PPT algorithm, generates $(\mathbb{G}, q, g)$

Def CDH is hard relative to $\mathcal{G}$ if

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

$C(1^n)$		$\mathcal{A}(1^n)$
$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$		
$x, y \xleftarrow{\$} \mathbb{Z}_q$		
	$\xrightarrow{(\mathbb{G}, q, g, g^x, g^y)}$	
		Output h

CDH $\Rightarrow$ DLOG

Decisional Diffie-Hellman (DDH) Assumption

$\mathcal{G}(1^n)$: PPT algorithm, generates $(\mathbb{G}, q, g)$

Def DDH is hard relative to $\mathcal{G}$ if

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

$C(1^n)$		$\mathcal{A}(1^n)$
$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$		
$x, y, z \xleftarrow{\$} \mathbb{Z}_q$		
$b \xleftarrow{\$} \{0,1\}$		
If $b=0$, $h := g^{xy}$		
If $b=1$, $h := g^{z}$		
	$\xrightarrow{(\mathbb{G}, q, g, g^x, g^y, h)}$	
		Output b'

DDH $\Rightarrow$ CDH