Clase 13: preliminares matemáticos II

Fernando Virdia, versión: 0.0.1, junio 2024

8 Grupos, y Suposiciones de Dificultad

A la base de gran parte de la PKC hay objetos de naturaleza algebraica: grupos, anillos, cuerpos. Nosotros vamos a intentar cubrir la menor cantidad posible, quedando cerca de lo utilizado en la practica.

Definición 21 (grupo abeliano) *Sea G un un conjunto, $\times$ una operación binaria $\times : G \times G \to G$. Decimos que $\mathbb{G} = (G, \times)$ es un grupo abeliano si*

1. *$\times$ es asociativa: $(a \times b) \times c = a \times (b \times c), \quad \forall a, b, c \in G$.*
2. *Existe un elemento neutro $e \in G$ tal que $a \times e = e \times a = a, \quad \forall a \in G$.*
3. *Cada elemento a tiene un inverso a^{-1}, tal que $a \times a^{-1} = a^{-1} \times a = e, \quad \forall a \in G$.*
4. *$\times$ es conmutativa: $a \times b = b \times a, \forall a, b \in G$.*

Si $|G| \leq \infty$, decimos que $\mathbb{G}$ es finito, y que $|G|$ es el orden de $\mathbb{G}$. A menudo abusamos notación y escribimos $a \in \mathbb{G}$ en lugar de $a \in G$.

Ejemplo 4
- *$(\mathbb{Z}, +)$ es un grupo abeliano*
- *$(\mathbb{Z}, \cdot)$ **no es** un grupo abeliano. $(\mathbb{Q}, \cdot)$ tampoco. $(\mathbb{Q}\backslash\{0\}, \cdot)$ lo es. $(\mathbb{R}\backslash\{0\}, \cdot)$ también.*
- *Sea $\mathbb{Z}_n$ el conjunto de los enteros "modulo n". $(\mathbb{Z}_n, +)$ es un grupo abeliano.*

Comentario 44 *En un grupo podemos "exponenciar": si $a \in \mathbb{G}$, $a^n \coloneqq a \times a \times \cdots \times a$ (n veces). Las comunes reglas valen:*

- $a^n \times a^m = a^{n+m}$,
- $(a^n)^m = a^{nm} = a^{mn} = (a^m)^n$,
- $a^1 \cdot a^{-1} = a^0 = e$.

En el caso de un grupo donde usamos "+", como $(\mathbb{Z}, +)$, el exponente es un factor: $a + \cdots + a$ (n veces) $= n \times a$.

Definición 22 (subgrupo) *Sea $\mathbb{G} = (G, \times)$ un grupo, y sea $S \subset G$ un subconjunto de G. Si $\mathbb{S} = (S, \times)$ forma un grupo, decimos que $\mathbb{S}$ es un subconjunto de $\mathbb{G}$.*

Ejemplo 5 *Sea $\mathbb{G} = (\mathbb{Z}, +)$. $\mathbb{S} = (2\mathbb{Z}, +) = (\{2n \mid n \in \mathbb{Z}\}, +)$ es un subgrupo de $\mathbb{G}$.*

Definición 23 (grupo cíclico) *Un grupo $\mathbb{G} = (G, \times)$ se dice cíclico si existe $g \in G$ tal que el grupo $\langle g \rangle$ "generado" g,*

$$\langle g \rangle \coloneqq (\{g^n \mid n \in \mathbb{Z}\}, \times),$$

es $\mathbb{G}$, o sea $\mathbb{G} = \langle g \rangle$.

Ejemplo 6 *$(\mathbb{Z}, +)$ es cíclico, y generado por ± 1.*

Lemma 14 *Dado un grupo $\mathbb{G} = (G, \times)$ de orden primo $|G| = p$, $\mathbb{G}$ es cíclico y generado por cualquier elemento no neutro.*

Ejemplo 7 *$(\mathbb{Z}_p, +)$ es cíclico. Cualquier $1 \leq g < p$ lo genera. Por ejemplo, sea $p = 3$.*

1 es un generador		2 es un generador	
1	$\mod 3 = 1$	2	$\mod 3 = 2$
$1 + 1$	$\mod 3 = 2$	$2 + 2$	$\mod 3 = 4 \mod 3 = 1$
$1 + 1 + 1$	$\mod 3 = 3$	$2 + 2 + 2$	$\mod 3 = 6 \mod 3 = 0$
$1 + 1 + 1 + 1$	$\mod 3 = 4 \mod 3 = 1$	$2 + 2 + 2 + 2$	$\mod 3 = 8 \mod 3 = 2$

Aquí podríamos adentrarnos en mas detalles sobre los grupos usados en criptografía, pero se vuelve muy matemático. En su lugar, vamos a definir tres problemas matemáticos relacionados, y un postulado. En criptografía, usamos familias de grupos que satisfacen el postulado.

Definición 24 (DLOG, informal) *Sea $\mathbb{G}$ un grupo cíclico. Dados $g, h \in \mathbb{G}$, el problema del logaritmo discreto (DLOG, "discrete logarithm") requiere recuperar $x \in \mathbb{Z}$ tal que $g^x = h$, o sea "$x = \log_g h$".*

Comentario 45 *DLOG es fácil de resolver en $(\mathbb{Z}, +)$ y $(\mathbb{R}\backslash\{0\}, \times)$:*

- *$(\mathbb{Z}, +)$: recordando que "g^x" es $x \cdot g$, $x \cdot g = h \iff x = h/g$.*
- *$(\mathbb{R}\backslash\{0\}, \times)$: $g^x = h \iff x = \log_g h$, donde $\log$ es el logaritmo "comun".*

Definición 25 (CDH, informal) *Sea $\mathbb{G}$ un grupo cíclico finito con generador g. Sean $x \xleftarrow{\$} [|G|]$, $y \xleftarrow{\$} [|G|]$ muestreados independientemente. El problema computacional de Diffie-Hellman (CDH, "computational Diffie-Hellman") requiere, dados (g, g^x, g^y), calcular $g^{xy} = (g^x)^y = (g^y)^x$.*

Comentario 46 *CDH no puede ser mas difícil de DLOG (o sea, resolver DLOG $\Rightarrow$ resolver CDH). Supongamos que $\mathcal{O}$ es un oráculo que calcula $(g, g^x) \mapsto x$. Dados (g, g^x, g^y), calculamos $(g^y)^{\mathcal{O}(g,g^x)} = (g^y)^x = g^{xy}$.*

Lemma 15 *Sea $\mathbb{G} = \langle g \rangle$ un grupo finito. Dada la variable aleatoria $z \sim U([|\mathbb{G}|])$, g^z es una variable aleatoria $g^z \sim U(\mathbb{G})$.*

Demostración.

$$\forall h \in \mathbb{G}, \quad \Pr_{z \sim U([|\mathbb{G}|])}[g^z = h] = \Pr[z = \log_g h] = \frac{1}{|\mathbb{G}|}.$$

□5

Definición 26 (DDH) *Sea $\mathbb{G} = \langle g \rangle$ un grupo cíclico. Para simplificar notación, supongamos que g es un "parámetro publico", o sea un elemento fijo y disponible públicamente. Definimos el juego $\mathsf{Exp}^{\mathrm{DDH}}$.*

$\mathsf{Exp}^{\mathrm{DDH}}(\mathcal{A}, b)$

```
1 : x ←$ [|G|]
2 : y ←$ [|G|]
3 : if b = 0
4 :     z ← x · y
5 : else
6 :     z ←$ [|G|]
7 : b' ← A(g^x, g^y, g^z)
8 : return b'
```

Decimos que DDH es (ε, t)-difícil en $\mathbb{G}$ si cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ tiene ventaja

$$\mathcal{A}(\mathsf{Exp}^{\mathrm{DDH}}, \mathcal{A}) \coloneqq \left|\Pr[\mathsf{Exp}^{\mathrm{DDH}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\mathrm{DDH}}(\mathcal{A}, 1) \Rightarrow 1]\right| \leq \varepsilon.$$

Finalmente introducimos un nuevo postulado:

Postulado 3 *Para cualquier valor de (ε, t), existe un grupo cíclico finito $\mathbb{G}$ tal que DDH es (ε, t)-difícil en $\mathbb{G}$.*

Comentario 47 *Por motivos criptoanalíticos, es generalmente deseable que $\mathbb{G}$ tenga orden primo.*