Seguridad Informática

Fundamentos Matemáticos de la Criptografía

Ramón Hermoso y Matteo Vasirani

Universidad Rey Juan Carlos

Índice

Índice

Divisibilidad I

- Sea $\mathbb{Z}$ el conjunto de los números enteros
- Se dice que $a|b$ (a divide a b) si $\exists c : b = a \cdot c$
- Si $a > 0$, $a \neq 1$, $a \neq b$, decimos que a es factor de b
- Un número b es **primo** si no tiene factores, es decir, sus únicos divisores son 1 y b
- Si un número no es primo, se llama **compuesto**

Divisibilidad II

- **Teorema de la división**

$$\forall a, b > 0, \quad \exists\, q, r \text{ únicos tales que:}$$
$$a = b \cdot q + r \text{ con } 0 \leq r \leq b$$

donde q se denomina cociente y r resto

Índice

Aritmética modular I

- Sea $a \in \mathbb{Z}$ y $n > 0$

$$a \ mod \ n \equiv \text{resto al dividir } a \text{ entre } n$$

Definición: $a \equiv b \ mod \ n$ si $[a \ mod \ n] = [b \ mod \ n]$

$a \equiv b \ mod \ n \Leftrightarrow n \mid (b-a) \Leftrightarrow \exists \ k : \ b - a = k \cdot n$

- **Operaciones: suma y producto**

$$[a+b \ mod \ n] = [a \ mod \ n] + [b \ mod \ n]$$
$$[a \cdot b \ mod \ n] = [a \ mod \ n] \cdot [b \ mod \ n]$$

Aritmética modular II

Congruencias

Cierto número a es **congruente** con otro cierto número b módulo n, si y solo si se obtiene el mismo resto al hacer ambas divisiones. Se denota mediante:

$$a = b \ mod \ n$$

Aritmética modular III

- **Operaciones: división**
  - $a/b \ mod \ n$ (si la división es entera no hay problema)
  - La división se define como la multiplicación con el inverso
  - El inverso de un número es otro número que multiplicado por el primero sea igual a 1
  - Si dado b, $\exists \ c$ tal que $b \cdot c = 1 \ (mod \ n)$, decimos que b tiene inverso $c = b^{-1}$
  - Por lo tanto, definimos $a/b = a \cdot b^{-1} \ (mod \ n)$

Aritmética modular IV

- **Inversos mod n**
  - **Teorema**: b es invertible mod n si y sólo si $mcd(b,n) = 1$

Ejemplo

- $3 \cdot 11 = 33 = 1 \ (mod\ 16) \Rightarrow 3$ es invertible y $3^{-1} = 11$
- En la igualdad $6 = 22\ mod\ 16$ podemos dividir entre 3:

$$6/3 = 22/3 = 22 \cdot 11 = 242 = 2\ mod\ 16$$

Ejercicio: Dividir por 5 la siguiente congruencia: $27 = 10\ mod\ 17$. Hacer lo mismo para $27 = 61\ mod\ 17$

Índice

Grupos I

- Un **grupo** es un conjunto G de elementos y de una operación binaria interna $\circ$ que cumple:
  - $a \circ (b \circ c) = (a \circ b) \circ c$ (Asociativa)
  - $\exists\, e:\ a \circ e = e \circ a = a$ (Elem. neutro)
  - $\forall g\ \exists h : g \circ h = h \circ g = e$ (Elem. Inverso)
- Si $a \circ b = b \circ a$ (Conmutativa), entonces G es un grupo **abeliano**
- Un **subgrupo** es un grupo contenido dentro de otro

Grupos II

- Notación **aditiva**: $g + h$
  - Elemento neutro: 0
  - El elemento inverso de g se denota $-g$
  - $g + g + ... + g = m \cdot g$
- Notación **multiplicativa**: $g \cdot h$
  - Elemento neutro: 1
  - El elemento inverso de g es g^{-1}
  - $g \cdot g \cdot ... \cdot g = g^m$
  - Por convenio: $g^0 = 1$ y $g^{-m} = (g^{-1})^m$

Grupos III

- El **orden** de un grupo finito es el número de elementos que lo compone
- **Teorema**: G es un grupo de orden m $\Rightarrow \forall\ g \in G : g^m = 1\ mod\ N$
- Corolario: $\forall\ g : g^i = g^{[i\ mod\ m]}$
- Corolario: $e > 0$ con $MCD(e,m) = 1 \Rightarrow$
  1. $f_e : g \rightarrow g^e$ es una **permutación** de G
  2. Si $d = e^{-1}\ mod\ m \Rightarrow f_d$ es la **inversa** de f_e

Permutaciones

Permutación e **inversión** permiten cifrar y descifrar!!!

Grupos IV

- Ejemplos:
  - $\mathbb{Z}_N = \{0,1,...,N-1\}$, donde $\circ =$ '+'$mod\ N$ es un grupo. ORDEN: N (**GRUPO ADITIVO** - $\oplus$)
  - $\mathbb{Z}_N^* = \{a \in \{1,...,N-1\}\} : MCD(a,N) = 1$ con $\circ = \cdot\ mod\ N$ es un grupo. ORDEN $\phi(N)$ (**GRUPO MULTIPLICATIVO** - $\odot$) (función de Euler)
- **Función de Euler**
  - Si p es primo $\Rightarrow \phi(p) = p-1$
  - Si p,q son primos $\Rightarrow \phi(p \cdot q) = (p-1) \cdot (q-1)$
- En general:
  - $\phi(ab) = \phi(a) \cdot \phi(b)$ si a y b no tienen factores primos comunes
  - $\phi(p^e) = p^{e-1} \cdot (p-1)$

Grupos cíclicos I

- Sea G un grupo finito de orden m y $g \in G$
- $< g >= \{g^0, g^1, g^2, ...\}$ (subgrupo generado por g)
- Orden de g: menor i tal que $g^i = 1 \ mod \ N$
- $< g >= \{g^0, g^1, g^2, ..., g^{i-1}\}$
- $g^x = g^y \leftrightarrow x = y \ (mod \ i)$

Grupos cíclicos II

- Si g tiene orden $m \Rightarrow < g >= G$ y decimos que G es **cíclico**, es decir,

$$G = \{g^0, g^1, g^2, ..., g^{m-1}\}$$

  y g recibe el nombre de **generador** de G
- Si g tiene orden i entonces $i \mid m$
- Consecuencia: si G tiene orden primo p entonces G es cíclico y todos los elementos de G menos el 1 son generadores

Grupos cíclicos III

- **Ejemplos**
  - $\mathbb{Z}_N$ es cíclico para todo N
  - $\mathbb{Z}_p^*$ es cíclico si p es primo
  - En $\mathbb{Z}_{15} \rightarrow 2$ es generador, 3 no
  - $\mathbb{Z}_8^*$ no es cíclico
  - $\mathbb{Z}_{10}^*$ es cíclico
  - En $\mathbb{Z}_7^* \rightarrow 3$ es generador, 2 no

Índice

El problema del logaritmo discreto (DLP) I

- $G =< g >$ de orden q
- Dado $h \in G$ existe un único $x \in \mathbb{Z}_q$ tal que $g^x = h$
- Decimos que $x = log_g(h)$
- Ejemplo:

$$\mathbb{Z}_{11}^* =< 7 >$$
$$log_7(4) =?$$

- Solución: 6

El problema del logaritmo discreto (DLP) II

El problema del logaritmo discreto (DLP)

- Consiste en obtener el valor de $\mathbf{y}$ en $\mathbf{x = a^y \bmod n}$
- Equivalente a $\mathbf{y = \log_a(x)}$
- Problema ”duro” o difícil si ningún adversario PPT A lo resuelve con probabilidad no despreciable
- Especialmente en los grupos $\mathbb{Z}_p^*$ con p primo (y suficientemente grande)
- Se usa comúnmente en criptosistemas de clave pública (p. ej. en el de Diffie-Hellman o en el de ElGamal)

Índice

Notas: Intercambio de claves Diffie-Hellman I

- Problemas Diffie-Hellman:
  1. Diffie-Hellman computacional (CDH):
     - Dados $h, k \in G$ encontrar $l \in G$ tal que cumpla que:
       si $h = g^x, k = g^y$ entonces $l = g^{xy}$
  2. Diffie-Hellman decisional (DDH):
     - Distinguir entre

       $$(g^x, g^y, g^z) \text{ vs. } (g^x, g^y, g^{xy})$$

       donde x, y, z se eligen al azar
- Relación de resolución de problemas:

  Resolver DLP $\rightarrow$ **Resolver CDH** $\rightarrow$ **Resolver DDH**

El problema de factorizar I

1. Se eligen x, y enteros de n bits al azar
2. Se calcula $N = x \cdot y$
3. El adversario A recibe N y devuelve x', y'
4. Si $x' \cdot y' = N$ entonces se dice que $Succ(A, n) = 1$

El problema de factorizar II

- No parece muy complicado. Por ejemplo, podemos inferir que, con probabilidad del 75% N es par
- También es fácil si x o y tienen factores primos pequeños
- Esto sugiere elegir x, y primos
- Se cree que, de esta forma, el problema de factorizar es difícil

Índice

El problema RSA

1. Se generan p, q primos de n bits al azar
2. $N = p \cdot q$
3. Se genera e tal que $mcd(e, \phi(N)) = 1$
4. Se elige $y \in \mathbb{Z}_N^*$ al azar
5. El adversario A recibe (e, y); devuelve x
6. Si $x^e = y$ entonces decimos que $Succ(A) = 1$

Relación de RSA con factorizar I

Teorema

Si se sabe factorizar N se puede resolver RSA

- Se calcula $\phi(N) = (p-1) \cdot (q-1)$
- Se calcula $d = e^{-1} \ mod \ \phi(N)$
- Solución: y^d
  porque $(y^d)^e = y^{de} = y \ mod \ N$

Relación de RSA con factorizar II

- Por lo tanto, RSA podría ser tan difícil como factorizar o algo más fácil
- No se conoce respuesta a esta conjetura

Generando primos al azar

- Para producir instancias de RSA o DLP hemos visto que se necesita generar números primos, a veces cumpliendo ciertas condiciones
- ¿Cómo se hace? Se generan números al azar a los que se pasa un test de primalidad

Pruebas de primalidad

- En la década de los 70 aparece el primer test de primalidad eficiente (probabilístico)
- Los más eficientes (por ejemplo el Miller-Rabin) son probabilísticos:
  - Entrada primo devuelve ”primo” siempre
  - Entrada número factorizable devuelve ”compuesto” excepto con pequeña probabilidad (*falsos positivos*)