Tecnología Digital IV: Redes de Computadoras

Teorema de Euler y Teorema Chino del Resto en Criptografía de Clave Pública

Marcelo Romeo

Licenciatura en Tecnología Digital
Universidad Torcuato Di Tella

17 de junio de 2025

Agenda

- Introducción a la seguridad en redes
- Criptografía
  - Simétrica: **DES**, **AES**
  - De clave pública: **RSA**
- Autenticación e integridad
  - Firmas digitales
  - Funciones de hash criptográficas
  - Certificados
- El protocolo **TLS**
- *Firewalls* e IDSs/IPSs

Introducción a la criptografía de clave pública

Claves pública y privada
Seguridad basada en problemas matemáticos difíciles

Conceptos previos

Aritmética modular: Ejemplo: $7 \bmod 3 = 1$

Números coprimos: Definición de coprimos (MCD = 1)

Ejemplo: 7 y 10 son coprimos

Función Totiente de Euler:

Definición de $\varphi(n)$

Ejemplo: $\varphi(10) = 4$

Teorema de Euler

Enunciado: $a^{\varphi(n)} \equiv 1 \pmod{n}$

El Teorema de Euler dice que si a y n son coprimos, entonces a elevado a $\varphi(n)$, módulo n, es siempre igual a 1. Esto es clave para el funcionamiento de RSA.

Ejemplos del Teorema de Euler

Ejemplo con a=3, n=10: $3^4 \bmod 10 = 1$
Ejemplo con a=7, n=10: $7^4 \bmod 10 = 1$

Aplicación en RSA

$n = p*q$
$\varphi(n) = (p-1)(q-1)$
Cálculo de e y d

En RSA, elegimos dos primos p y q, calculamos $n=pq$ y $\varphi(n)=(p-1)(q-1)$. Luego, seleccionamos e coprimo con $\varphi(n)$ y calculamos d como el inverso de e módulo $\varphi(n)$. Este d es la clave privada

Garantía de reversibilidad en RSA

$(M^e)^d \equiv M \pmod{n}$

El Teorema de Euler garantiza que si $e*d \equiv 1 \pmod{\varphi(n)}$, entonces al cifrar y luego descifrar un mensaje M, obtenemos nuevamente M. Es la base de la reversibilidad de RSA

Introducción al Teorema Chino del Resto (CRT)

Permite reconstruir un número a partir de varios residuos modulares

El Teorema Chino del Resto resuelve sistemas de congruencias con módulos coprimos. Permite calcular un número completo a partir de varios residuos

Introducción al Teorema Chino del Resto (CRT)

$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$
$x \equiv 2 \pmod{7}$
Solución: $x = 23 \bmod 105$

Cálculo detallado del ejemplo con CRT

Producto total: N = 3 * 5 * 7 = 105

$N_1 = 35$, $N_2 = 21$, $N_3 = 15$

Inversos: $M_1 = 2$, $M_2 = 1$, $M_3 = 1$

Cálculo final: x = (2*35*2) + (3*21*1) + (2*15*1) mod 105

Resultado: x = 233 mod 105 → x = 23

Aplicación del CRT en RSA

Aceleración del descifrado

En RSA, el CRT permite hacer los cálculos de descifrado en dos pasos más pequeños: calcular C^d mod p y C^d mod q, y luego combinar los resultados. Esto es mucho más eficiente que calcular directamente C^d mod n

Ventajas del CRT en Criptografía

- Aceleración 2x a 4x
- Uso en dispositivos de recursos limitados

Resumen final

- Euler: garantiza reversibilidad en RSA
- CRT: optimiza el rendimiento

En resumen, el Teorema de Euler garantiza que el cifrado y descifrado de RSA funcionen correctamente, mientras que el Teorema Chino del Resto permite que estas operaciones se realicen más rápido. Ambos son esenciales para la criptografía moderna