PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

Criptografía y Seguridad Computacional - IIC3253
1er semestre - 2022
Lothar Droppelmann

Ayudantía 8

Definiciones

1. Teorema Chino del Resto

Se define $N = p * q$ y suponga que p y q son coprimos, es decir, MCD$(p, q) = 1$. Para todo a y b enteros tal que $0 \leq a < p$ y $0 \leq b < q$, existe un x tal que:

$$a = x \bmod p$$
$$b = x \bmod q$$

Además, todas estas soluciones son congruentes en módulo N, es decir, la solución es única en $\{0, ..., N\}$.

2. Identidad de Bézout

Para cada $a, b \in$ tales que $a \neq 0$ y $b \neq 0$ existen $s, t \in$ tal que:

$$\text{MCD}(a, b) = s \cdot a + t \cdot b$$

3. Teorema

Sea $\phi(N)$ la función phi de Euler, tal que $\phi(N) =$ cantidad de enteros coprimos a N en $\{1, ..., N-1\}$. Para todo $a < N$ y coprimo con N es siempre cierto que:

$$a^{\phi(n)} \equiv 1 \bmod N$$

Preguntas

1. Demuestre el Teorema Chino del Resto.
2. Calcule a mano:
   a) $11^{53} \bmod 15$
   b) $29^{100} \bmod 35$
   c) $46^{51} \bmod 55$