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 1

Pregunta 1

Se define la relación de congruencia modular:

$$a \equiv b \bmod n \iff n|(a-b)$$

1. Demuestre que la relación de congruencia es una relación de equivalencia.
2. Dado que $a \equiv b \bmod n$, $c \equiv d \bmod n$ y $k \in \mathbb{Z}$, demuestre las siguientes propiedades:
   - *a)* $ka \equiv kb \bmod n$
   - *b)* $a + c \equiv b + d \bmod n$
   - *c)* $ac \equiv bd \bmod n$
   - *d)* $a + k \equiv b + k \bmod n$
   - *e)* $a - c \equiv b - d \bmod n$
   - *f)* $a \equiv a + kn \bmod n$
   - *g)* $a^k \equiv b^k \bmod n$, con $k \geq 1$
   - *h)* $ka \equiv kb \bmod n \rightarrow a \equiv b \bmod n$, si solo si $MCD(k, n) = 1$
   - *i)* $ka \equiv kb \bmod kn \rightarrow a \equiv b \bmod n$

Pregunta 2

Se define el Teorema de Shannon: Dado un esquema criptográfico (Gen, Enc, Dec) sobre un espacio de mensajes M tal que $|M| = |K| = |C|$. El esquema cumple Perfect Secrecy si y solo si:

1. La distribución de probabilidades Gen es uniforme ($Gen(k) = \frac{1}{|K|}, \forall k \in K$)
2. Para todo mensaje $m \in M$ y para todo texto cifrado $c \in C$ existe una única llave $k \in K$ tal que $\text{Enc}(k, m) = c$

Demuestre el Teorema de Shannon.