Ayudantía 11

IIC3253 - Criptografía y Seguridad Computacional

Christian Klempau

1 Repaso y T3

1.1 Grupos

- Defina qué es un grupo y explique cuáles son sus componentes
- Enumere y defina las propiedades que debe cumplir

1.2 ¿Qué es $\mathbb{Z}_N$?

- Defina el grupo y sus componentes
- Demuestre que $\mathbb{Z}_N$ es un grupo
- En este caso, ¿qué es la multiplicación y exponenciación de elementos?

1.3 ¿Qué es $\mathbb{Z}_N^*$?

- Defina el grupo y sus componentes
- ¿Qué representa $\phi(N)$?

1.4 ¿Qué es $\mathbb{Z}_p^*$?

- Defina el grupo y sus componentes
- ¿Cuánto vale $\phi(p)$? ¿Por qué?

1.5 ¿Cómo funciona ElGamal?

- ¿Qué componentes deben estar previamente definidos?
- ¿Cuál es la clave pública y privada?
- ¿Cómo se cifra y descifra?

1.6 ¿Cómo funcionan las firmas de Schnorr?

- ¿Qué componentes deben estar previamente definidos?
- ¿Cómo se firma y verifica?

1.7 ¿Cómo funcionan las curvas elípticas?

- Considere la forma de Weierstrass, ¿Cómo se define el grupo? ¿Qué componentes debe tener?
- ¿Cómo se define el operador "+"? Vea caso a caso su funcionamiento