

Sesión 4. Cifrado Asimétrico.

---

1. Considera que Alice y Bob establecen una clave con el intercambio de Diffie-Hellman en  $\mathbb{Z}_{17}^*$  tomando como generador  $g = 3$ . Alice envía un 12, mientras que Bob envía un 14. ¿Puedes obtener (por fuerza bruta) la clave que Alice y Bob han establecido?
2. Considerar un esquema RSA con clave pública  $N = 187, e = 7$ . Descifra el texto  $C = 13$  (puedes dejar el resultado indicado sin terminar las cuentas).
3. Dado un esquema RSA con clave pública  $N = 55, e = 7$ , cifra el mensaje  $M = 12$ , encuentra  $p, q, d$  y descifra  $c = 37$  (puedes dejar el resultado indicado sin terminar las cuentas).
4. Supongamos que un adversario que ataca el criptosistema RSA es capaz de calcular la función de Euler del módulo,  $\varphi(N)$ . ¿A qué tiene acceso?
5. Considera que hay dos usuarios del sistema, Bob y Berto, que tienen claves públicas RSA con el mismo módulo  $N$  pero distintos exponentes  $e_1$  y  $e_2$ .
  - a) Demuestra que Bob puede descifrar mensajes enviados a Berto
  - b) Demuestra que un adversario es capaz de descifrar cualquier mensaje que se haya enviado a la vez a Bob y a Berto, si  $m.c.d.(e_1, e_2) = 1$
6. Considera una modificación del esquema de cifrado de Bellare y Rogaway en la que el cifrado de un texto  $m$  conste de tres componentes:
  - $f(r)$ , con  $r$  aleatorio y  $f$  una función *one-way*,
  - $m \cdot f(r)$ ,
  - $H(r)$ , con  $H$  un oráculo aleatorio

Analiza informalmente la seguridad del esquema resultante.