EXAMEN - 16 DE DICIEMBRE DE 2015. DURACIÓN: 3 HORAS Y MEDIA.

| N° de examen | Cédula | Apellido y nombre |
|---|---|---|
| | | |

**Ejercicio 1.**

**a**. Sea la función $\varphi$ de Euler y dos enteros $m$, $n > 1$ tales que $\text{mcd}(m, n) = 1$. Probar que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

**b**. Mostrar con un ejemplo que lo anterior es falso si $\text{mcd}(m, n) \neq 1$.

**c**. Calcular $\varphi(297)$.

**d**. Reducir $629^{362} \pmod{297}$.

**Ejercicio 2.**

**a**. Sea $G$ un grupo finito y $x, y \in G$ tales que $xy = yx$ y $\text{mcd}(\text{o}(x), \text{o}(y)) = 1$. Probar que

$$\text{o}(xy) = \text{o}(x)\,\text{o}(y).$$

**b**. Sea $G = U(47)$ y $g = 2 \in G$. Probar que $\text{o}(g) = 23$.

**c**. Utilizando lo anterior encontrar una raíz primitiva módulo 47.

**d**. ¿El grupo $U(15)$ es cíclico? Justique su respuesta.

**Ejercicio 3.**

**a**. Sean $n = 253$ y $e = 9$. Para los datos anteriores hallar la función de descifrado $D : \mathbb{Z}_n \to \mathbb{Z}_n$ definida por el protocolo RSA.

**b**. Reducir $22^{666} \pmod{253}$.

**Ejercicio 4.**

**a**. i) Sean $n, m \in \mathbb{Z}$ tal que $n \mid m$ y $a, b \in \mathbb{Z}$. Probar que

$$a \equiv b \pmod{m} \Longrightarrow a \equiv b \pmod{n}.$$

ii) ¿Vale el recíproco de lo anterior? Justificar.

**b**. Para el siguiente sistema investigar si tiene solución, y en caso de que tenga solución, hallar todas sus soluciones:

$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 83 \pmod{286} \end{cases}.$$