

Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2, semipresencial

CUARTA PRUEBA (SEGUNDO PARCIAL) - 1 DE DICIEMBRE DE 2016. DURACIÓN: 3,5 HORAS

N° de parcial	Nombre y apellido	Cédula

Ejercicio 1. (15 puntos) (*Ejercicio 1 del segundo parcial del curso semipresencial de 2015*)

- a. Probar que 2 es raíz primitiva módulo 53.
- b. Hallar todos los $x \in \mathbb{Z}$ tales que $x^{19} \equiv 32 \pmod{53}$.
- c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo $p = 53$ y la raíz primitiva $g = 2$. Archibaldo selecciona el número $m = 28$ y le remite el número 49 a Baldomero. Éste selecciona el número $n = 5$. ¿Cuál es la clave común k que acordaron Archibaldo y Baldomero?

Ejercicio 2. (20 puntos)

- a. Calcular el número de raíces primitivas en $U(29)$.
- b. Encontrar todas las raíces primitivas de $U(29)$.
(Sugerencia: Calcular $2^n \pmod{29}$, para todo $0 \leq n \leq 14$, para facilitar los cálculos posteriores.)
- c. Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior: $r_1 \leq r_2 \leq r_3 \leq r_4 \leq r_5 \leq \dots$. Luego escribir la secuencia: $r_1 r_5 0 r_9 r_3 r_1 r_7$. Finalmente traducir usando la numeración de los símbolos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

- d. Utilizando el método de Vigenère **decodificar** el siguiente texto, usando la palabra clave hallada en el ítem anterior:

OZ_LPTSOKMS_BUCBRSNCG

Ejercicio 3. (10 puntos) Describir el “Método de Fermat” de ataque al RSA, y demostrar la validez del algoritmo planteado.