Universidad de la República - Facultad de Ingeniería - IMERL. Matemática Discreta 2

Examen - 9 de febrero de 2017. Duración: 4 horas.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1. Hallar el menor entero positivo congruente a $7^{217^{38}} \pmod{34}$.

Ejercicio 2.

a. ¿Qué es una ecuación diofántica lineal? Decidir cuándo tiene solución y qué forma tiene ésta cuando existe. Probar ambas propiedades.

b. ¿Qué podemos decir sobre la existencia y el número de soluciones de la ecuación de congruencia:

$$ax \equiv b \pmod{m}?$$ Justificar.

c. Hallar todas las soluciones (módulo 64) de la ecuación de congruencia: $28x \equiv 44 \pmod{64}$.

Ejercicio 3. Hallar todas las soluciones en $\mathbb{Z}$ del sistema:

$$\begin{cases} 3x \equiv 10 \pmod{11} \\ 2x \equiv 7 \pmod{9} \\ x \equiv 8 \pmod{15} \\ 5x \equiv 10 \pmod{12} \\ x \equiv 18 \pmod{20}. \end{cases}$$

Ejercicio 4.

a. Describir el método de Diffie - Hellman para acuerdo de clave.

b. Donald y Mickey, para garantizar la seguridad del gobierno de su país, se ponen de acuerdo en utilizar Diffie - Hellman y fijan el primo $p = 73$ y $g = 11$. Donald elige el número secreto $n = 71$ y Mickey le envía $g^m = 23$. ¿Cuál es la clave secreta que acuerdan Donald y Mickey?

c. Asignamos valores a algunos caracteres según la tabla siguiente:

A	B	C	D	E	J	L	M	N	O	P	S	R
0	1	2	3	4	5	6	7	8	9	10	11	12

Definimos el criptosistema afín de la siguiente manera: para $a, b \in \mathbb{Z}$, con $1 \leq a \leq 12$, y $0 \leq b \leq 12$, consideramos la función de encriptado $E : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$ tal que $E(x) = ax+b \pmod{13}$. Sea $0 \leq W < 73$ la clave acordada por Donald y Mickey. Escribamos $W = a \cdot 13 + b$ con $0 \leq a < 13$ y $0 \leq b < 13$. El encriptado se hace letra a letra usando la función E definida arriba. Encriptar la palabra DJNP.

d. Supongamos que somos espías rusos y que Donald le envió a Mickey un mensaje encripado según el criptosistema anterior (desconociendo los valores de a y b de la función de encriptado). Espías ayudantes han descubierto que el mensaje original (sin encriptar) tiene como segunda letra A y como cuarta letra E. El mensaje encriptado es $OCEJM$.

i) Hallar la función de encriptado (o sea hallar los valores de a y b) que usan Donald y Mickey.

ii) Desencriptar el mensaje $OCEJM$.

Ejercicio 5.

a. Sea p un primo y k un entero positivo. Si g es un número par y raíz primitiva de p^k, probar que $g + p^k$ es raíz primitiva de $2p^k$.

b. Hallar explícitamente todos los homomorfismos de $U(54)$ en el grupo dihedral D_{12}.