Pontificia Universidad Católica de Chile
Facultad de Matemáticas
2° semestre 2020

Ayudantía 08

16 de Octubre

MAT2225 - Teoría de Números

1) Se encriptan las letras del alfabeto usando la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Tambien se eligen los primos $p = 11, q = 17$ y el exponente $e = 107$.

a) Calcule $\varphi(pq)$ y $d = e^{-1} \pmod{\varphi(pq)}$

b) Suponga que quiere enviar las letras de la palabra "HOLA" por separado. ¿Qué números se necesitan enviar?

c) Llega el mensaje codificado $108, 86, 146, 51, 28$. ¿Qué dice?

d) ¿Qué letras podrían presentar problemas al intentar codificarlas? ¿Por qué?

e) ¿Cuál es el módulo más pequeño en el que se pueden enviar todas las letras con esta codificación sin problemas?

Bonus: Un hacker empieza a recolectar claves, y encuentra los siguientes productos de primos:

$$1065023, 1916927, 2060969, 3301453.$$

El hacker descubre que hay dos claves vulnerables. Encuéntrelas.
Hint: Revise si hay claves con factores primos en común.