Universidad Pontificia Bolivariana SECCIONAL BUCARAMANGA	**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA** **ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA** **Asignatura: CRIPTOGRAFÍA – NRC: 47016** Facilitador: Julián Darío Miranda (julian.miranda@upb.edu.co) Semestre: 2019 - II

QUIZ # 1

CONCEPTUALIZACIÓN MATEMÁTICA Y MÉTODOS CRIPTOGRÁFICOS DE SUSTITUCIÓN

Desarrollar los siguiente numerales teniendo en cuenta el alfabeto definido por el intervalo [0, 26], en el que la A corresponde al índice 0 y la Z al índice 26. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

1. Cifrar mediante el Cifrado Afín el siguiente texto: "ES HORA DE GANAR", teniendo en cuenta la llave $(a, b) = (2, 49)$

2. Descifrar mediante el Cifrado Afín el siguiente texto: "JTTCQTGXZYAFNIC", teniendo en cuenta la llave $(a, b) = (37, 125)$.

3. Se ha logrado recuperar una comunicación cifrada en la que se presenta el siguiente fragmento de interés: "CZOQENTN IRVWYEAD WCTDAVNT PSBCBWLZ", cifrado a partir del método de Playfair. Aunque no se tiene la clave para descifrarlo, se ha logrado recuperar la matriz de Playfair, que luce como se muestra a la derecha. Con base en esta información, descifrar el criptograma, entregando como resultado el mensaje en claro y la clave usada para descifrarlo.

	I/J			O
A	B	C	D	E
F	G	H		N
	Q	R	S	T
U	V		Y	Z

4. ¿Qué diferencia existe entre cifrar con la clave "ARAR" y cifrar con el patrón de claves "$(AR)^n$" donde n es un número natural que representa la cantidad de repeticiones de la cadena? Justificar la respuesta.

5. De acuerdo con el criptograma: "6171B19131200040D101A1C020C1E0C0E01" que se ha generado a partir del mensaje "RETIRADA A CONFIRMAR" (sin espacios), ¿cuál es la clave de generación del criptograma?