

	<p align="center">FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA Asignatura: CRIPTOGRAFÍA – NRC: 47016</p> <p align="center">Facilitador: Julián Darío Miranda (julian.miranda@upb.edu.co) Semestre: 2019 - II</p>
---	---

QUIZ # 2

CRIPTOANÁLISIS DE MÉTODOS CLÁSICOS DE CIFRADO

Desarrollar el siguiente numeral teniendo en cuenta el alfabeto definido por el intervalo: [A, Z]U[0, 9] y su equivalente decimal de la codificación ASCII. No incluir vocales tildadas, espacios u otro carácter fuera de este alfabeto.

Se ha logrado recuperar una comunicación en castellano cifrada en la que se presenta el siguiente fragmento de interés cifrado usando el Cifrado de Vigenère, con una clave desconocida.

CEWCCRRFPBRFYCUSEIUBRVGBFCBOCVXJVFZFHNRFYIUSECUBZZHHZVQCCE
WCHHSKVTPRWCDIAOTBGKEWCJVSCGTFRPCCXNJZRFRGTFRPCDSMWVASVP
VOINQFPYIVEOTEKOWHSIEVCCSIVVTQREOTSEQFAQRVTQFZDIIICTNGTSIOJCC
TELQFCOJGHAGESTSFCTBAGVXDFPOJGHDRDFGTGTBDRWIOXNFVXHHFGCD
EMSKVHRXHARZOKIRMFZSKSFCKBRRQBHRMOUIVVFPCCEMS

Con base en este criptograma:

- Marcar las secuencias repetidas de 4 o más caracteres.
- Hallar la longitud más probable de llave utilizada (la llave tiene una longitud mayor a 3 caracteres) mediante el cálculo de repeticiones y mediante el cálculo del IC.
- Mostrar los sub-criptogramas que pueden construirse a partir de la longitud(es) más probable(s) determinada(s).
- Extraer las letras más probables para las subclaves utilizadas.
- Expresar las combinaciones de clave que pueden obtenerse con las subclaves del punto anterior.
- Descifrar el criptograma con las combinaciones de clave y escribir el mensaje en texto claro original.
- Calcular el valor del IC del mensaje final y muestre su valor.
- Calcule el valor del IF del mensaje final y muestre su valor.