**PRIMERA PRÁCTICA DE LABORATORIO**

**FUNCIONES ELEMENTALES DE CRIPTOGRAFIA**

1. **OBJETIVOS:**

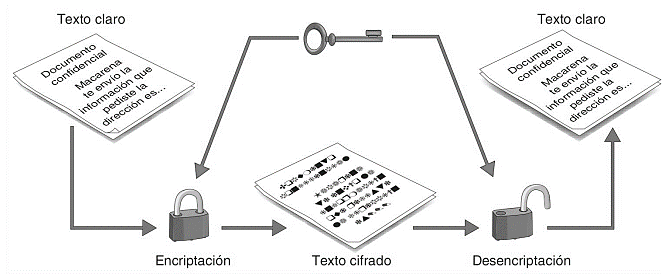
* Conocer e implementar funciones básicas comunes usadas en la aplicación de técnicas criptográficas

1. **EQUIPO Y SOFTWARE**

* Computadora personal
* Software de desarrollo (libre elección c++, phyton, java u otro previa autorización del docente)

1. **MARCO TEÓRICO**
   1. **Cifrado**

Se entiende el cifrado como el proceso que convierte cualquier mensaje o dato(s) en otro ilegible,



Criptosistema

En todo proceso de cifrado se identifica:

* El texto claro o texto plano (*plain text*) es el mensaje legible u original que debe protegerse mediante el cifrado.
* El criptograma o texto cifrado es el mensaje ilegible que se obtiene al aplicar el proceso de cifrado
* La encriptación es la aplicación de un algoritmo de cifrado o cifra sobre el texto claro, este requiere un dato protegido denominado clave o llave de cifrado
* La desencriptación o descifrado es el proceso de convertir el texto cifrado en el texto plano original a partir de la aplicación de un algoritmo que revierte el proceso anterior, requiere también el conocimiento de la clave o llave

Todo este conjunto estructurado de elementos recibe el nombre de Criptosistema.

Se denomina **alfabeto** al conjunto de caracteres posibles de encontrar en el texto claro, que no necesariamente coincide con el juego de caracteres que se usa en el mensaje cifrado. Finalmente, en algunos algoritmos, el texto cifrado se escribe en base a bloques de longitud constante, denominados grupos, lo que se usa como verificación adicional al comprobar que el texto cifrado tiene un número entero de los mismos, para ello se puede aplicar un **padding** o relleno del texto claro inicial con ceros o algún carácter especial.

* 1. **Preprocesado**

Se denomina preprocesado al conjunto de funciones aplicadas sobre el texto claro antes de aplicarle el algoritmo de cifrado, con la finalidad de que este corra apropiadamente y el texto cifrado resultante sea más resistente al criptoanálisis o ataque para romper el cifrado, dentro de ello tenemos

1. *Modificación del alfabeto por sustitución*

Hay algoritmos de cifrado definidos sobre algún alfabeto en particular lo que exige sustituir los caracteres que no corresponden a este por otros, es típico los problemas del español con las letras **h,j,ñ,k,u,w,y** que no pertenecen al alfabeto latino, por lo que deben sustituirse por otros; también es común los alfabetos que usan sólo mayúsculas

1. *Inclusión de caracteres nulos*

Son palabras o grupos de caracteres sin significados insertados en medio del texto claro o para romper letras repetidas, por ejemplo, **rr**, **ll** u otro.

1. *Eliminación de no significativos*

Eliminar signos de puntuación o espacios en blanco

1. *Reemplazo de carretillas*

Reemplazar por otro texto palabras o frases muy comunes o repetitivas

1. *Reemplazo numérico*

Los caracteres deben ser reemplazados por valores numéricos ASCII, UNICODE-8, como, por ejemplo

"Hello World"= 0x48656C6C6F20576F726C64

o cada palabra por el valor numérico resultante de sumar la posición de cada carácter en el alfabeto por el peso según la posición del carácter en la palabra

"HIJO"=7x263+8\*262+9\*261+14\*260=128688

1. **ACTIVIDADES**

Sobre el texto claro mostrado a continuación:

*Hay golpes en la vida, tan fuertes… ¡Yo no sé!*

*Golpes como del odio de Dios; como si ante ellos,*

*la resaca de todo lo sufrido*

*se empozara en el alma… ¡Yo no sé!*

*Son pocos; pero son… Abren zanjas oscuras*

*en el rostro más fiero y en el lomo más fuerte.*

*Serán tal vez los potros de bárbaros Atilas;*

*o los heraldos negros que nos manda la Muerte.*

*Son las caídas hondas de los Cristos del alma*

*de alguna fe adorable que el Destino blasfema.*

*Esos golpes sangrientos son las crepitaciones*

*de algún pan que en la puerta del horno se nos quema.*

*Y el hombre… Pobre… ¡pobre! Vuelve los ojos, como*

*cuando por sobre el hombro nos llama una palmada;*

*vuelve los ojos locos, y todo lo vivido*

*se empoza, como charco de culpa, en la mirada.*

*Hay golpes en la vida, tan fuertes… ¡Yo no sé!*

Implementar las siguientes operaciones de preprocesamiento, en cada caso debe mostrar el código de la solución y la salida parcial resultante en cada caso

1. Realizar las siguientes sustituciones: j x i, h x i, ñ,x n, k x l, u x v, w x,v, y x z
2. Elimine las tildes
3. Convierta todas las letras a mayúsculas
4. Elimine los espacios en blanco y los signos de puntuación

Guarde el resultado en el archivo “HERALDOSNEGROS\_pre.txt”

1. Abra el archivo generado e implementar una función que calcule una tabla de frecuencias para cada letra de la ’A’ a ’Z’. La función deberá definirse como

*frecuencias(archivo)*

deberá devolver un diccionario cuyos índices son las letras analizadas y cuyos valores son las frecuencias de las mismas en el texto (número de veces que aparecen). Reconozca en el resultado obtenido los cinco caracteres de mayor frecuencia

1. Aplicar el método Kasiski, que recorre el texto preprocesado y halla los trigramas en el mismo (sucesión de tres letras seguidas que se repiten) y las distancias (número de caracteres entre ellos) entre los trigramas
2. Volver a preprocesar el archivo cambiando cada carácter según UNICODE-8
3. Volver a preprocesar el archivo cambiando cada carácter según UNICODE-8230
4. Volver a preprocesar el archivo insertando la cadena AQUÍ cada 20 caracteres, el texto resultante deberá contener un número de caracteres que sea múltiplo de 4, si es necesario rellenar al final con caracteres X según se necesite
5. **CONCLUSIONES**

Emitir al menos ocho conclusiones en torno al preprocesamiento de texto claro

1. **CUESTIONARIO FINAL**
2. Describa los siguientes términos (áreas de la seguridad informática)

* Protección y seguridad de los datos
* Criptografía
* Seguridad y fortificación de redes
* Seguridad en aplicaciones informáticas,programas y bases de datos
* Gestión de seguridad en equipos y sistemas informáticos
* Informática forense
* Ciberdelito, ciberseguridad

1. Describa los siguientes términos (áreas de la seguridad de la información)

* Gestión de la seguridad de la información
* Asesoría y auditoría de la seguridad
* Análisis y gestión de riesgos
* Continuidad de negocio
* Buen gobierno
* Comercio electrónico
* Legislación relacionada con seguridad

1. Describa alguna otra operación o función de preprocesamiento que se implemente sobre el texto claro en los criptosistemas, en que afecta la complejidad de estas funciones al desempeño del mismo
2. Describa la máquina enigma, luego muestre usando un simulador en internet la encriptación de la frase QUERIDA HIJA, para tres posiciones distintas de los rotores
3. Describa la aplicación de Unicode-8

**BIBLIOGRAFÍA**