Trabajo Práctico N°1

Fecha Límite de Entrega: 25 de marzo a las 23:55
Profesor: Dr. Javier Echaiz
Auxiliar: Ing. Fernando Pap

Condiciones de Aprobación:

En líneas generales el trabajo debe dar evidencia del desarrollo realizado. En casos puntuales en los que sea conveniente, incluir un archivo `readme.txt` con notas correspondientes. Entregas individuales subiendo contenido al directorio `ARS2022/Práctica/Entregas/[nombre]` del Drive y enviando aviso al email fernandopap@gmail.com o al grupo de whatsapp. Se recomienda utilizar github/ Bitbucket/etc. El trabajo debe ser entregado completo. Pasada la fecha límite de entrega se descontará un punto por cada día transcurrido.

Enunciados

Criptografía simétrica

1. Implemente el cifrador/descifrador Caesar. El programa debe tener una única pantalla y debe permitir:
   - Seleccionar la acción a realizar (cifrar/descifrar)
   - Ingresar la clave (para cifrar o descifrar, según sea el caso)
   - Ingresar el mensaje (a cifrar o descifrar, según sea el caso)

El programa debe estar realizado en el lenguaje de programación PHP.

2. Implemente un mecanismo de fuerza bruta para descifrar el cifrador anteriormente desarrollado. Utilizar un archivo de texto de diccionario para sugerir una salida como la más probable.

3. Implemente el cifrador/descifrador Vigenère. El programa debe tener una única pantalla y debe permitir:
   - Seleccionar la acción a realizar (cifrar/descifrar)
   - Ingresar la clave (para cifrar o descifrar, según sea el caso)
   - Ingresar el mensaje (a cifrar o descifrar, según sea el caso)

El programa debe estar realizado en el lenguaje de programación PHP.

Hash

1. Los algoritmos de hash (md5, sha-x, etc.) no se utilizan para cifrar mensajes. ¿Por qué?

2. Explique conceptualmente la utilidad de algoritmos de hash para:
   a) Autenticación de usuarios
   b) Comprobación de integridad de archivos.

3. ¿Qué es salt? ¿Para qué se utiliza?

4. Escriba un pequeño programa que almacene usuarios/contraseñas (MySQL, PostgreSQL, etc.) y permita registrarse/autenticarse, utilizando algún algoritmo de hash. **Tenga en cuenta la utilización de salt**.
El programa debe estar realizado en el lenguaje de programación PHP.