Trabajo Práctico N°1

Criptografía simétrica (primera parte)

Fecha Límite de Entrega: 20 de abril 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 `ARS2018/Entregas/[nombre]` del Google 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

1. Implemente el cifrador/descifrador Caesar. El programa debe tener tres entradas:
   - Acción a realizar (cifrar/descifrar)
   - Clave (para cifrar o descifrar, según sea el caso)
   - 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. Puede utilizarse un archivo de texto de diccionario para sugerir una salida como la más probable.

3. Implemente el cifrador/descifrador Vigenère. El programa debe tener tres entradas:
   - Acción a realizar (cifrar/descifrar)
   - Clave (para cifrar o descifrar, según sea el caso)
   - Mensaje (a cifrar o descifrar, según sea el caso)

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

4. Cifrar la frase
`"Vivir solo cuesta vida"` con el cifrador de Hill con la matriz ((11, 8) (3, 7)) y luego descifrarla. Detallar todos los pasos.

5. Si se aplica dos veces el cifrador Affine, ¿se mejora la seguridad?

6. ¿Qué protocolos populares utilizan cifrado DES?