# Trabajo Práctico N°2

## Hash

**Fecha Límite de Entrega:** 27 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. 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. Explique brevemente qué es una rainbow table.

5. Escriba un pequeño programa que almacene contraseñas (y permita realizar logon/login) utilizando algún algoritmo de hash. Tenga en cuenta consideraciones de seguridad.
El programa puede ser de línea de comandos, aplicación de escritorio, web, etc. y puede estar desarrollado en lenguaje a elección.