Trabajo Práctico N°2

Hash

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

Porque son funciones de un solo sentido, dada una operación hash es computacionalmente imposible obtener el anti-hash. Cifrar un mensaje con esta técnica implicaría no poder recuperarlo. Ademas es una función con pérdida, ya que dado un mensaje de tamaño m, el hash generado con una determinada función dará como salida un hash de tamaño fijo para todo m.

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

Brinda soporte agregando una marca al final del criptograma. Esta marca depende del mensaje, pero como queda protegida por clave secreta, el destinatario sabrá que ese hash solo lo pudo generar el remitente (autenticacion de usuarios). Cuando el remitente genera su propio hash con la función conocida, podrá compararlo con el hash enviado (integridad del mensaje).

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

Es un campo de datos extra y en algunos casos diferente para cada usuario, como fecha de creación de la cuenta o una parte del nombre del usuario, aunque también puede ser algún valor que sea igual en todos ellos. Esta información se agrega a la contraseña de esa persona antes de encriptarla. De esta forma, dos usuario que haya elegido la misma clave de sesión, tendrá contraseñas encriptadas deferentes. Por lo tanto, protege al sistema de ataques con tabla arcoiris (buscar coincidencias en base a patrones de claves comúnmente usadas).

4. Explique brevemente qué es una rainbow table.

Es una table que contiene las claves que usan generalmente las personas. Se representan encriptadas, y reduce el espacio de búsqueda de un atacante al momento de probar claves.

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

   Ver https://github.com/poximan/ARS/tree/master/tp2.