

Tarea práctica

Criptografía

Universidad Católica del Uruguay

Consigna

Desarrollar un prototipo de aplicación web que permita:

- Identificar, Autenticar y Autorizar a sus usuarios, almacenando las contraseñas de forma que se preserve en todo momento su seguridad utilizando el algoritmo de hash SHA-2.
- Cifrar y descifrar archivos por medio del uso del algoritmo simétricos AES.
- Firmar digitalmente (y verificar la firma) de archivos. Para la firma se deberá utilizar SHA-2 y RSA.

Utilice algoritmos probados, implementados por bibliotecas criptográficas.

Consigna

Recordar validar con los docentes las decisiones de diseño antes de realizar el desarrollo.

El grupo utilizara un repositorio en GitHub para desarrollar la aplicación en forma colaborativa.

Entrega

Se entregara a través de webasignatura un único archivo por grupo que contenga la documentación elaborada para la aplicacion en formato pdf, incluyendo alli la URL al repositorio de GitHub.

Evaluación

La entrega será evaluada en los siguientes aspectos:

- Presentación
- Completitud
- Comprensión de la temática
- Profundidad en el análisis

?