Página Web

Elaborar una página Web personal que contenga tu información general así como los links necesarios para descargar tu CV y tu llave pública (en su momento de ECDSA)

Elaborar una página Web personal que incluya

- Pantalla de presentación: Es lo primero que se verá al visitar la página. En ella debe verse el nombre completo, fotografía y las secciones de:
  - Formación Académica
  - Correo electrónico
  - Botones para tus redes sociales
  - Hobbies incluir al menos 3 fotografías con descripción
  - 2 vídeos sobre hobbies o actividades extracurriculares
  - 1 vídeo sobre PGP (En donde aparezcas hablando, 3-5 minutos)
  - Acerca de Criptografía (la biografía de algún criptógraf@, la historia de algún algoritmo, algún evento importante)

- Elaborar tu CV y guardarlo en formato PDF
  - Se debe incluir una link para poder descargar el pdf del CV
- Poner un link que diga Mi llave Pública
  - La llave Pública se generará en la práctica de ECDSA próximamente (por ahora solo debe estar el link)

Dra. Nidia A. Cortez Duarte

Despues de realizar la lectura de PGP responde las siguientes preguntas a mano.

1. ¿Quién fue el creador de PGP?
a) Phil Zimmermann b) Whitfield Diffie c) Ron Rivest d) Bruce Schneier

2.- ¿Cuál de los siguientes algoritmos NO es utilizado por PGP para cifrado simétrico?
a) CAST-128 b) AES-256 c) IDEA d) 3DES

3.- ¿Qué función tiene SHA-1 en PGP?
a) Cifrado simétrico b) Firma digital c) Generación de claves públicas d) Esteganografía

4.- ¿Cuál es el propósito del mecanismo de radix-64 en PGP?
a) Asegurar la confidencialidad del mensaje
b) Comprimir los mensajes antes de cifrarlos
c) Convertir datos binarios en un formato ASCII compatible con correos electrónicos
d) Firmar digitalmente los mensajes

5.-¿Cómo se generan las claves de sesión en PGP?
a) Mediante el uso de claves RSA de 2048 bits
b) Como un número aleatorio de 128 bits utilizado solo para una sesión
c) Mediante el uso de una contraseña proporcionada por el usuario
d) Utilizando el algoritmo Diffie-Hellman

Contesta de manera clara y con respecto a tus conocimientos previos en conjunto a la lectura para presentar en tu vídeo de PGP

1. ¿Cuáles son los servicios principales que ofrece PGP y cómo contribuyen a la seguridad de la información?
2. Describe el proceso de firma digital en PGP y explica su importancia en la autenticación de mensajes.
3. ¿Por qué PGP cifra primero el mensaje y luego cifra la clave de sesión con criptografía asimétrica?
4. ¿Cómo maneja PGP la segmentación de mensajes cuando estos superan el tamaño permitido en algunos sistemas de correo electrónico?
5. Explica el funcionamiento de los anillos de claves (key rings) en PGP y cómo contribuyen a la gestión de claves.
6. Explica la relación de PGP con lo visto en la U.A Introduction to Cryptography
7. Conclusiones personales

Dra. Nidia A. Cortez Duarte