Programación IV
Profesora Cynthia Estrada

Fecha: 13/08

"Cifrados"

Integrantes:

- "Díaz Rossini Juan José",
- "Gallo Genaro"
- "Navarro Victor Leandro"

---

1. **Explica el cifrado simétrico, el cifrado asimétrico y el cifrado polialfabético**
2. **¿Cuáles son los requisitos de certificación SSL?**
3. **¿Cuáles son los delitos de los hackers?**

Explica el cifrado simétrico, el cifrado asimétrico y el cifrado polialfabético

El cifrado simétrico es un método en el cual se utiliza la misma clave para cifrar y descifrar la información. Su principal ventaja es la rapidez y eficiencia, lo que lo hace ideal para grandes volúmenes de datos. Sin embargo, presenta un problema: la distribución de la clave, ya que si un tercero la obtiene, puede acceder a toda la información. Ejemplos modernos de este tipo de cifrado son AES y DES.

El cifrado asimétrico, en cambio, utiliza un par de claves diferentes: una pública y otra privada. La clave pública sirve para cifrar la información, mientras que la clave privada se emplea para descifrarla. Esto permite un intercambio seguro de datos sin necesidad de compartir la clave privada. Aunque es más seguro para la transmisión inicial de información, suele ser más lento que el simétrico. Ejemplos conocidos son RSA y ECC.

El cifrado polialfabético es un método clásico que consiste en usar varios alfabetos de sustitución para dificultar el reconocimiento de patrones. A diferencia del monoalfabético, en el cual una letra siempre se reemplaza por la misma, el polialfabético puede cambiar según la posición o la clave. Esto lo vuelve mucho más resistente a los ataques de frecuencia. El ejemplo más famoso es el cifrado de Vigenère.

¿Cuáles son los requisitos de certificación SSL?

Para obtener un certificado SSL, que permite asegurar la comunicación entre el navegador y el servidor, existen ciertos requisitos básicos:

1. **Dominio válido y registrado: El solicitante debe demostrar que es dueño o tiene control sobre el dominio.**
2. **Generación de una CSR (Certificate Signing Request): Documento que contiene la clave pública y los datos del dominio u organización.**
3. **Validación del dominio: La autoridad certificadora (CA) puede pedir la verificación mediante correo electrónico, un registro DNS o un archivo en el servidor.**

4. **Documentación adicional (OV y EV):**
    - **En certificados OV (Organization Validation), se debe presentar información legal de la empresa como registro mercantil o CUIT.**
    - **En certificados EV (Extended Validation), la validación es más estricta: incluye entrevistas, comprobación de identidad y verificación exhaustiva de la organización.**
5. **Requisitos técnicos: El servidor debe estar configurado con protocolos seguros como TLS 1.2 o superior, además de soportar algoritmos de cifrado robustos.**

En resumen, un SSL garantiza la seguridad y la autenticidad del sitio web, protegiendo tanto a la organización como a los usuarios que acceden.

¿Cuáles son los delitos de los hackers?

Los delitos informáticos relacionados con hackers abarcan distintas acciones ilegales que atentan contra la confidencialidad, integridad y disponibilidad de los sistemas. Algunos de los más comunes son:

1. **Acceso ilícito a sistemas: Entrar en redes, servidores o dispositivos sin autorización.**
2. **Robo o filtración de información: Obtener datos personales, financieros o empresariales con fines ilegales.**
3. **Fraudes electrónicos: Incluye el phishing, clonación de tarjetas y engaños a través de plataformas digitales para obtener beneficios económicos.**
4. **Propagación de malware: Crear y distribuir virus, troyanos o ransomware con el objetivo de dañar sistemas o extorsionar a las víctimas.**
5. **Sabotaje digital: Atacar sistemas para inutilizarlos, como ocurre en ataques de denegación de servicio (DDoS), que dejan páginas o servidores fuera de línea.**

Estos delitos están tipificados en la legislación de la mayoría de los países y pueden acarrear severas penas, ya que afectan tanto a individuos como a empresas e incluso a la seguridad nacional.