



Programación de Servicios y Procesos

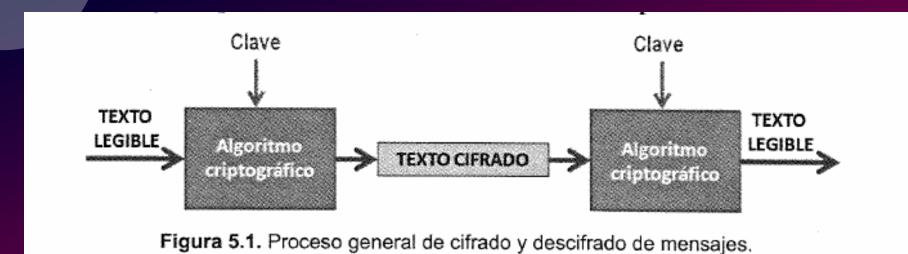
U.D.5 - TÉCNICAS DE PROGRAMACIÓN SEGURA (II)







Criptografía







Criptografía II



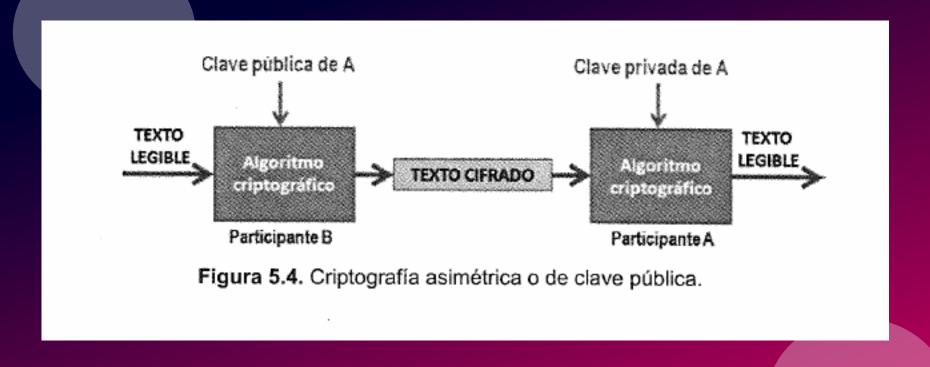
Figura 5.3. Criptografía simétrica o de clave privada.







Criptografía III



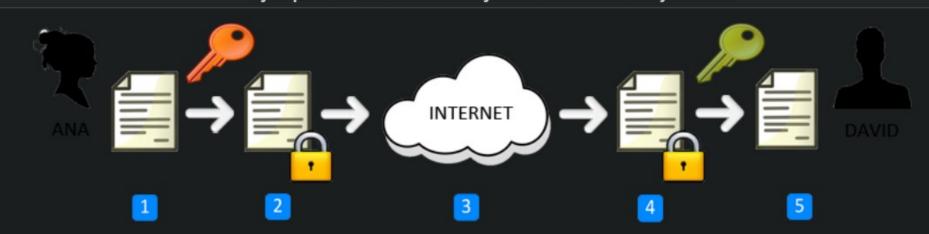






Criptografía IV

Ejemplo de cifrado de mensaje: Ana envía un mensaje a David



- 1. Ana redacta un mensaje.
- 2. Ana cifra el mensaje con la **clave pública** de David.
- 3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
- 4. David recibe el mensaje cifrado y lo descifra con su **clave privada**.
- 5. David ya puede leer el mensaje original que le mandó Ana.



ER - 0432/2007





Algoritmos Criptográficos Simétricos

- Cifrado César. → Uso
- **DES Data Encryption Standard**→ **Triple DES** → **AES Advanced Encryption Standard.**
- **Blowfish**







Algoritmos Criptográficos Asímétricos



- Diffie-Hellman \rightarrow es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima (no autenticada).
- RSA (Rivest, Shamir y Adleman) → sistema criptográfico de clave pública desarrollado en 1979, que utiliza factorización de números enteros. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
- El procedimiento de cifrado/descifrado ElGamal se refiere a un esquema de cifrado basado en el problema matemático del logaritmo discreto. Es un algoritmo de criptografía asimétrica basado en la idea de Diffie-Hellman y que funciona de una forma parecida a este algoritmo discreto. Es de uso libre.









GNU Privacy Guard

- "Un GNU Privacy Guard (GPG) es un software libre y de código abierto que proporciona cifrado y firma digital de datos. GPG se basa en el estándar OpenPGP (Pretty Good Privacy) y es compatible con la mayoría de los clientes de correo electrónico y aplicaciones de cifrado."
- "Enigmail añade a tu cliente de correo, cifrado y autenticación de mensajes mediante OpenPGP. Ofrece cifrado y descifrado automático y una funcionalidad integrada de administración de claves. Enigmail requiere GnuPG para las funciones criptográficas. Nota: GnuPG no es parte de la instalación."

https://msmk.university/ciberseguridad/que-es-un-gnu-privacy-guard-msmk-university https://addons.thunderbird.net/es/thunderbird/addon/enigmail/







Otros en seguridad

- AAA: Son tres características fundamentales de un sistema informático:
 - Autenticación: Quien hace algo es quien dice ser
 - Autorización: Quien hace algo tiene permiso y derecho para hacerlo.
 - Accountability (Responsabilidad o rendición de cuentas): Capacidad para registrar cada acción de tal manera que se pueda rastrear.

