

# Criptografía

Profesor: Melvin Fernández Ch.

Video 3



fidÉlitas  
Virtual

# Historia y Evolución de la Criptografía

Módulo: 1




# Finalidad de la Criptología

- Un buen sistema criptográfico será aquel que ofrezca un descifrado imposible pero un encriptado sencillo.
- La finalidad es doble:
  - ✓ Mantener la confidencialidad del mensaje.
  - ✓ Garantizar la autenticidad tanto del mensaje como del remitente/destinatario.

# Servicios de Cripto Sistemas

- **Confidencialidad:** hace que la información sea ininteligible excepto para las entidades autorizadas.
- **Integridad:** los datos no han sido alterados de forma no autorizada desde que se creó, transmitió o almacenó.
- **Autenticación:** verifica la identidad del usuario o sistema que creó la información.

# Servicios de Cripto Sistemas

- **Autorización:** al proporcionar identidad, al individuo se le provee de la llave o contraseña que le dará acceso al recurso.
  - **No repudio:** garantiza que quien envía el mensaje no puede negarlo.
- 
- A decorative graphic consisting of several thin, parallel pink diagonal lines is located in the bottom left corner of the slide.

# Tipos de Cifrado

- **Definición:** es una serie de transformaciones que convierte texto plano a texto cifrado utilizando una llave.
- Proporciona confidencialidad a través de funciones matemáticas.
- **Tipos**
  - ✓ Simétricos o de Llave Privada (DES).
  - ✓ Asimétricos o de Llave Pública (RSA).
  - ✓ Híbrido (SSL).

# Tipos de Cifrado

## Ventajas

- Protege la información almacenada en la computadora contra accesos no autorizados.
- Protege la información mientras transita de un sistema de cómputo a otro.
- Puede detectar y evitar alteraciones accidentales o intencionales a los datos.
- Puede verificar si el autor de un documento es realmente quién es.

## Desventajas

- No puede prevenir que un agresor borre intencionalmente todos los datos.
- Acceder al archivo antes de que sea cifrado o después de descifrar.

# Gracias

