UNIVERSIDAD ABIERTA
INTERAMERICANA

Presentación
Facultad de tecnología

Criptografía

Profesor Adjunto: Ing. Mauricio Prinzo

Agenda

- ✓ **Criptografia**
  - ⌗ Cifrado

Criptografía

- ✓ **Estudio de la ....**
  - Escritura (Grafos)
  - Secreta (Cripto)

- ✓ **Escritura oculta, Disciplina que estudia los principios métodos y medios de ocultar la información contenida en un mensaje**

- ✓ **Mecanismo que codifica un mensaje de manera tal que solo el emisor y el receptor autorizado pueden comprenderlo**

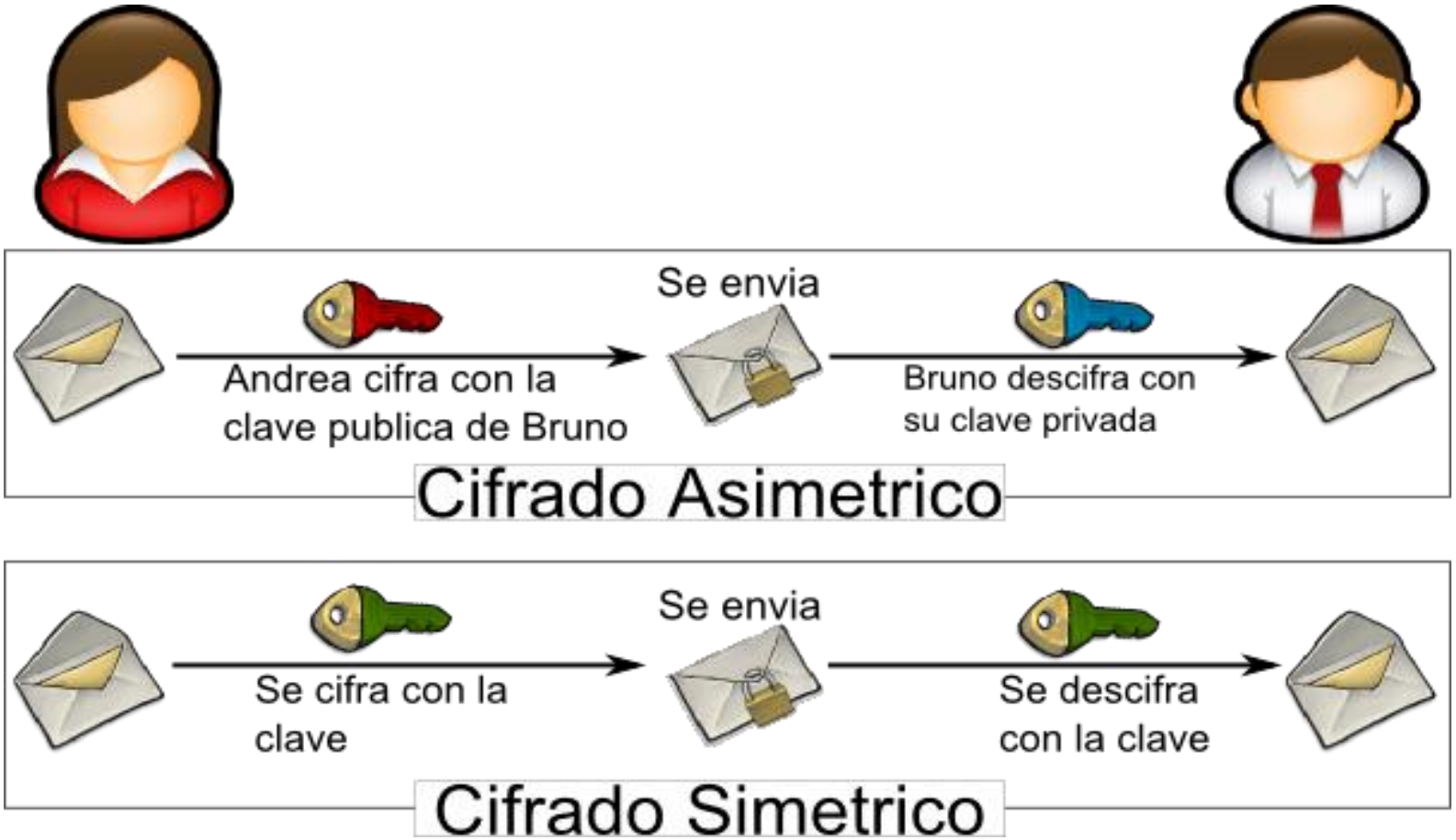
Utilidad

- ✓ Se utiliza para lograr los objetivos siguientes:
  - Confidencialidad: para ayudar a proteger la identidad de un usuario o evitar que se lean sus datos.
  - Integridad de los datos: para ayudar a evitar su alteración.
  - Autenticación: para garantizar que los datos provienen de una parte concreta.
  - Sin rechazo: para evitar que una determinada parte niegue que envió un mensaje.

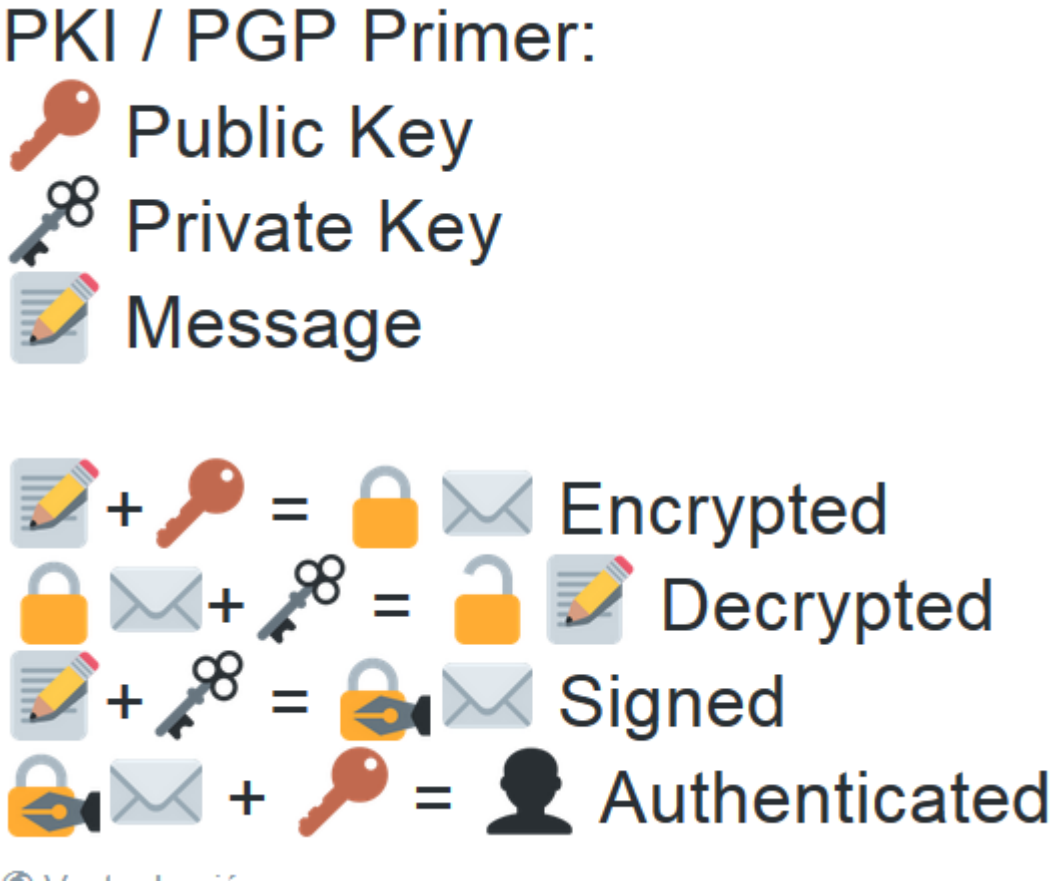
Tipos de Criptografía

Método	Descripción
Cifrado de clave secreta (criptografía simétrica)	Realiza la transformación de los datos para impedir que terceros los lean. Este tipo de cifrado utiliza una clave secreta compartida para cifrar y descifrar los datos.
Cifrado de clave pública (criptografía asimétrica)	Realiza la transformación de los datos para impedir que terceros los lean. Este tipo de cifrado utiliza un par de claves pública y privada para cifrar y descifrar los datos.
Firmas criptográficas	Ayuda a comprobar que los datos se originan en una parte específica mediante la creación de una firma digital única para esa parte. En este proceso también se usan funciones hash.
Valores hash criptográficos	Asigna datos de cualquier longitud a una secuencia de bytes de longitud fija. Los valores hash son únicos estadísticamente; el valor hash de una secuencia de dos bytes distinta no será el mismo.

Criptografía Simétrica y Asimétrica



Criptografía Simétrica y Asimétrica



Criptografía Simétrica y Asimétrica

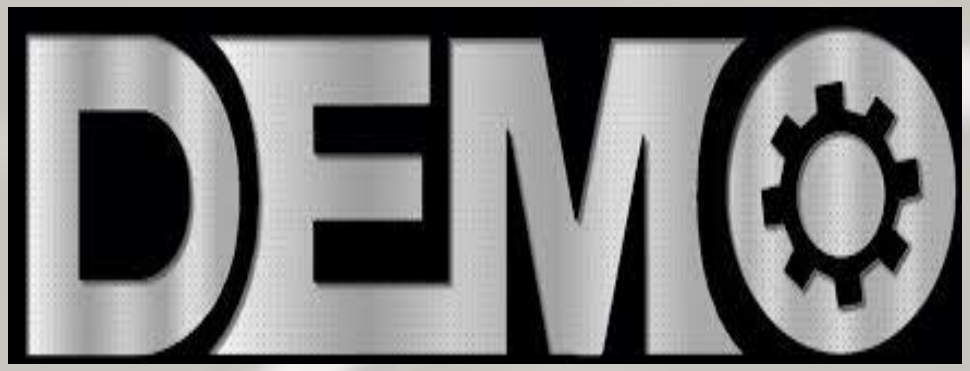
Longitudes de claves simétricas	Longitudes de claves asimétricas
64 bits.	512 bits.
80 bits.	768 bits.
112 bits.	1792 bits.
128 bits.	2304 bits.

VS Criptografia

Cifrado de clave secreta (criptografía simétrica)	AesManaged (introducida en .NET Framework 3,5). DESCryptoServiceProvider. RC2CryptoServiceProvider. RijndaelManaged. TripleDESCryptoServiceProvider.
Cifrado de clave pública (criptografía asimétrica)	DSACryptoServiceProvider RSACryptoServiceProvider ECDiffieHellman (clase base) ECDiffieHellmanCng ECDiffieHellmanCngPublicKey (clase base) ECDiffieHellmanKeyDerivationFunction (clase base) ECDsaCng
Firmas criptográficas	DSACryptoServiceProvider RSACryptoServiceProvider ECDsa (clase base) ECDsaCng
Valores hash criptográficos	HMACSHA1. MACTripleDES. MD5CryptoServiceProvider. RIPEMD160. SHA1Managed. SHA256Managed. SHA384Managed. SHA512Managed.

VS Criptografía - Sintaxis

- ✓ Crear la clase para encapsular los métodos de cifrado y descifrado, según el algoritmo
- ✓ Importación de espacio de nombres de criptografía :
  - C# : **Using System.Security.Cryptography**
- ✓ Crear un campo o variable con el proveedor de servicios criptográficos
  - **C#: AlgoritmoCyptoServiceProvider xxx = new AlgoritmoCyptoServiceProvider();**


DEMO

¿Preguntas?