Seguridad Informática

Unidad II. Criptografía

Universidad Tecnológica de Coahuila

Objetivo

- El alumno desarrollará aplicaciones de software integrando algoritmos criptográficos para mantener la confidencialidad de la información.

Dosificación

Horas Teóricas	3
Horas Prácticas	9
Horas Totales	12

Rubricas

SABER	Identificar Algoritmos de cifrado simétrico	1
	Identificar Algoritmos de cifrado asimétrico	1
	Identificar Algoritmos Hash	1
SABER HACER	Caso práctico: Algoritmos de cifrado simétrico	1
	Caso práctico: Algoritmos de cifrado asimétrico	1
	Caso práctico: Algoritmos Hash	1
	Caso práctico: Funcionalidad	1
SER	Puntualidad y Asistencia	1
	Entrega en Tiempo y Forma	1
	Responsabilidad, disciplina y Proactividad	1

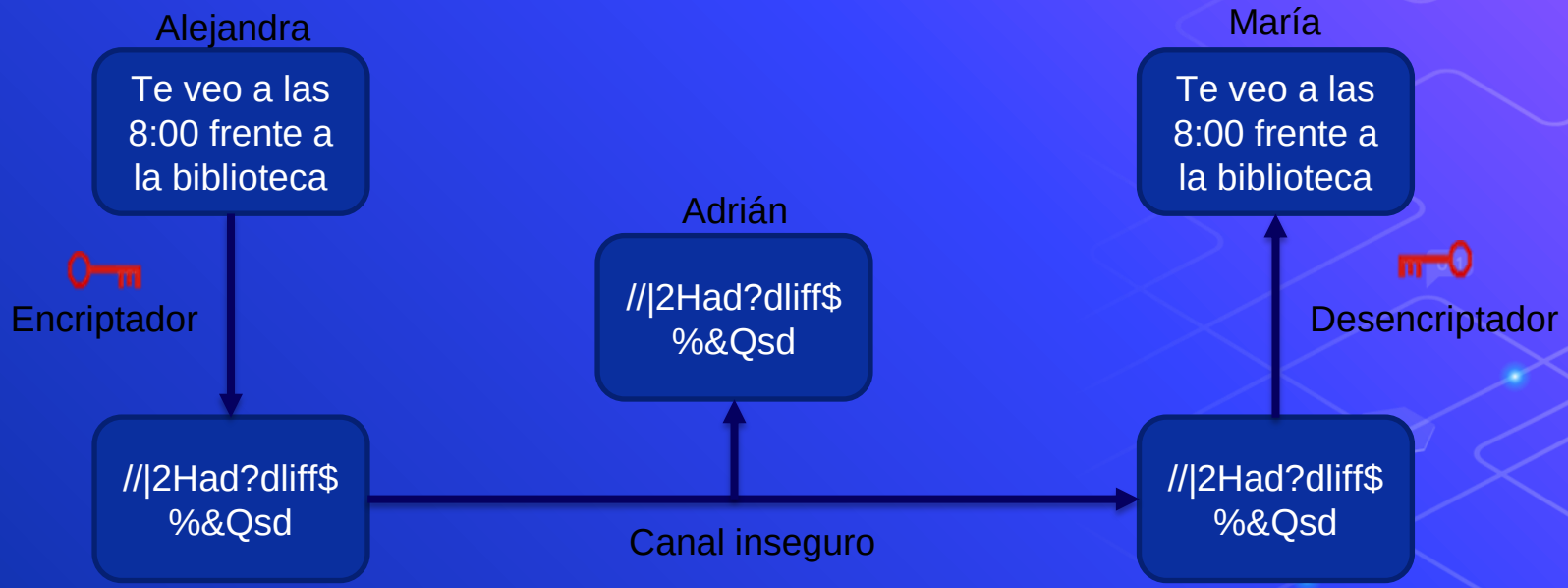
Temas

- Algoritmos de cifrado
- Algoritmos hash

Criptografía simétrica

- Utilizan una clave con la cual se encripta y desencripta el documento.
- Todo documento encriptado, deberá desencriptarse,

Criptografía simétrica

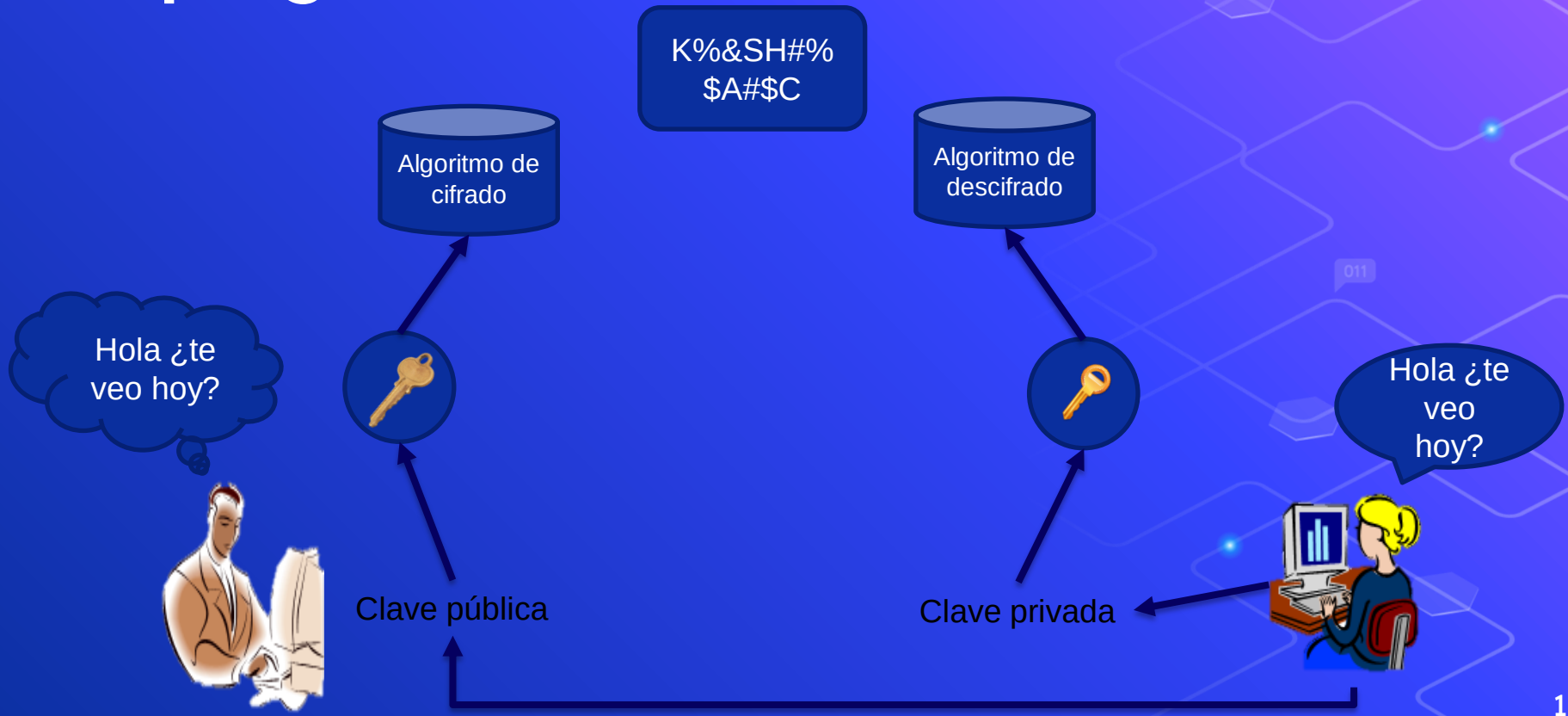


Clave Privada

Criptografía asimétrica

- Requieren dos Claves, una Privada y otra Pública
- El usuario, ingresando su PIN genera la clave Publica y Privada necesarias
- La clave pública podrá ser distribuida
- La Privada deberá ser celosamente guardada.
- Al desencriptar un mensaje se utiliza la Clave Publica

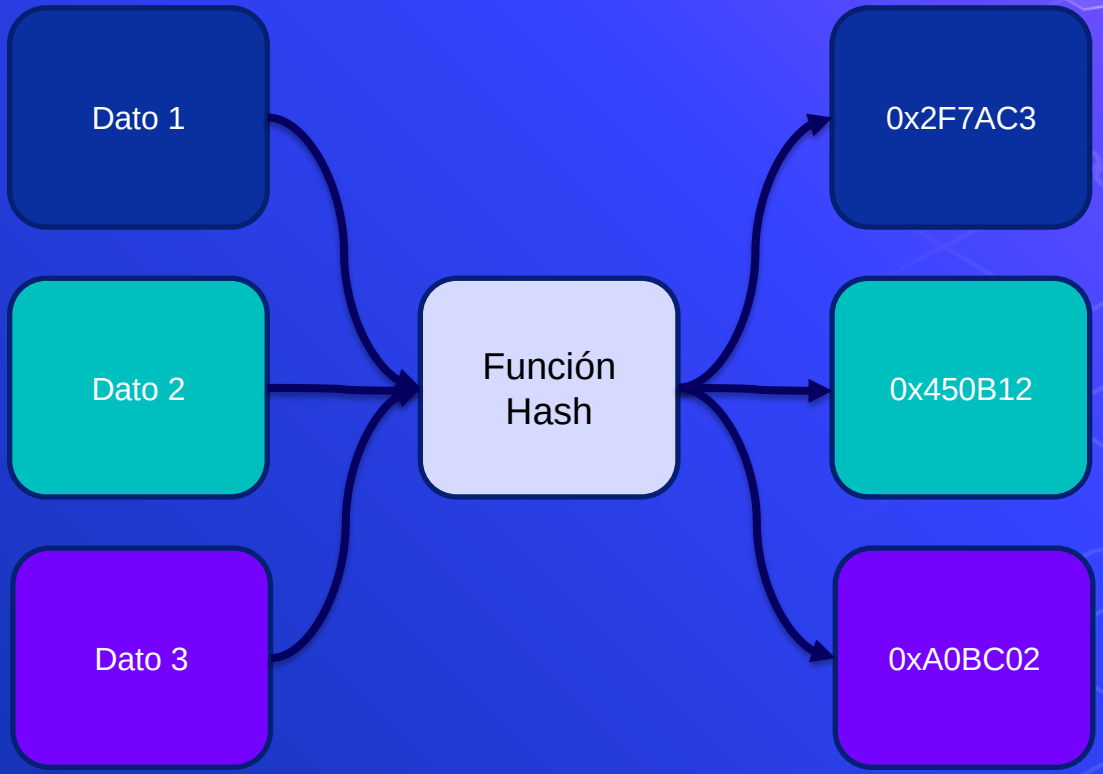
Criptografía asimétrica



Algoritmos Hash

- Efectúa un cálculo matemático sobre los datos que constituyen el documento.
- Da como resultado un número único llamado MAC.
- Un mismo documento dará siempre un mismo MAC.

Algoritmo HASH



Ejemplo en PHP

```
<?php
        $password = 'gabriel1234';
        $salt="sha512";
        $cifrado = crypt($password,$salt);
?>
```

¿Dudas?