Criptografía Y Firma Digital.

Modulo 1.
Introducción Y Fundamentos Básicos

Laboratorio de Seguridad de la Información

CRIPTOGRAFÍA: KRIPTOS (oculto) + GRAPHOS (escribir)

CRIPTOGRAFÍA según Real Academia de la Lengua Española:

"Arte de escribir con clave secreta o de un modo enigmático"

Origen e Historia:

- La criptografía es tan antigua como la escritura misma: los egipcios, guerras de Atenas contra Esparta, el General Julio César, …
- En tiempos de guerra siempre ha sido crucial ocultar información y que sólo unos pocos sean capaces de entenderla.
- Los últimos años han sido cruciales en el desarrollo y la evolución de la criptografía: telegrama Zimmerman, máquina Enigma y desarrollo de los fundamentos matemáticos para los algoritmos de la criptografía moderna.

Clasificación de los algoritmos criptográficos:

- Criptografía Clásica
  - o Por sustitución de caracteres
  - o Por transposición de caracteres
- Criptografía Moderna
  - o Simétrica o de clave secreta
  - o Asimétrica o de clave pública
  - o Funciones Hash

Seguridad:

- La criptografía moderna utiliza problemas matemáticos que no se saben (aún) solucionar o al menos, que computacionalmente no son resolubles sin un esfuerzo inmenso de recursos y tiempo.

El uso conjunto de los tres tipos de funciones de la criptografía moderna permite que se pueda garantizar

- ✔ CONFIDENCIALIDAD de la información almacenada o enviada.
- ✔ NO REPUDIO frente a la realización de una operación o transacción.
- ✔ AUTENTICIDAD sobre quién ha enviado algo (origen).
- ✔ AUTENTICIDAD sobre a quién se enviará algo (destino).
- ✔ INTEGRIDAD de la información enviada.

Criptografía Simétrica o de clave Secreta:

Utilizan la misma clave para cifrar y descifrar.

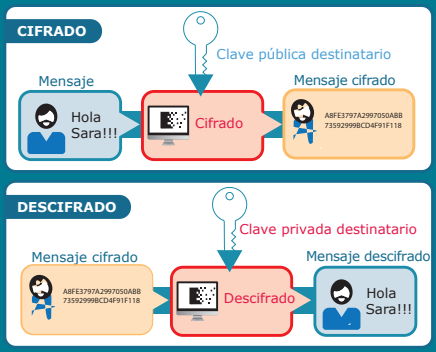
Muy rápidos.

Criptografía Asimétrica o de Clave Pública:

Claves diferentes para cifrar y descifrar.

La clave pública se puede distribuir libremente: ¡¡la seguridad se mantiene!!

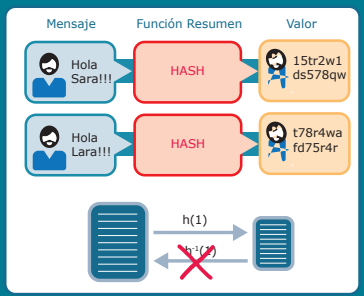
Son lentos.



Funciones resumen - Hash:

No cifran mensajes, hacen un resumen.

Propiedad especial: el cambio de un único carácter del mensaje original, provoca un resumen diferente. ¡¡Útil para garantizar la integridad!!



XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE
SERVIZO GALEGO de SAÚDE
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa