

Herramientas para garantizar la Integridad y Autenticidad Documental.

Diego Sebastian Escobar.

Cita:

Diego Sebastian Escobar (Julio, 2017). *Herramientas para garantizar la Integridad y Autenticidad Documental*. 3º Reunión: CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL. CPCECABA, CABA.

Dirección estable: <https://www.aacademica.org/escobards/7>

ARK: <https://n2t.net/ark:/13683/ptuD/sDU>



Esta obra está bajo una licencia de Creative Commons.
Para ver una copia de esta licencia, visite
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: <https://www.aacademica.org>.

CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL

3º REUNIÓN: Herramientas para garantizar la Integridad y Autenticidad Documental.

Exposición

Dr. C.P. y L.A. Diego Sebastián Escobar

Coordinación

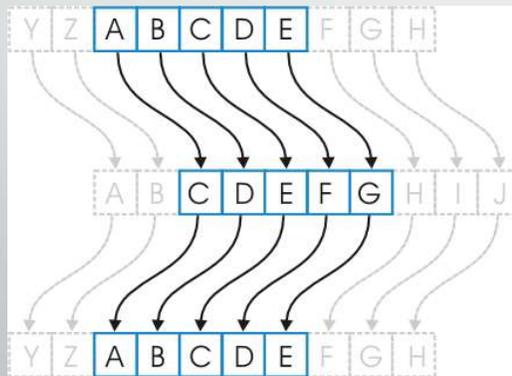
Dra. C.P. Esteban Mazzitelli



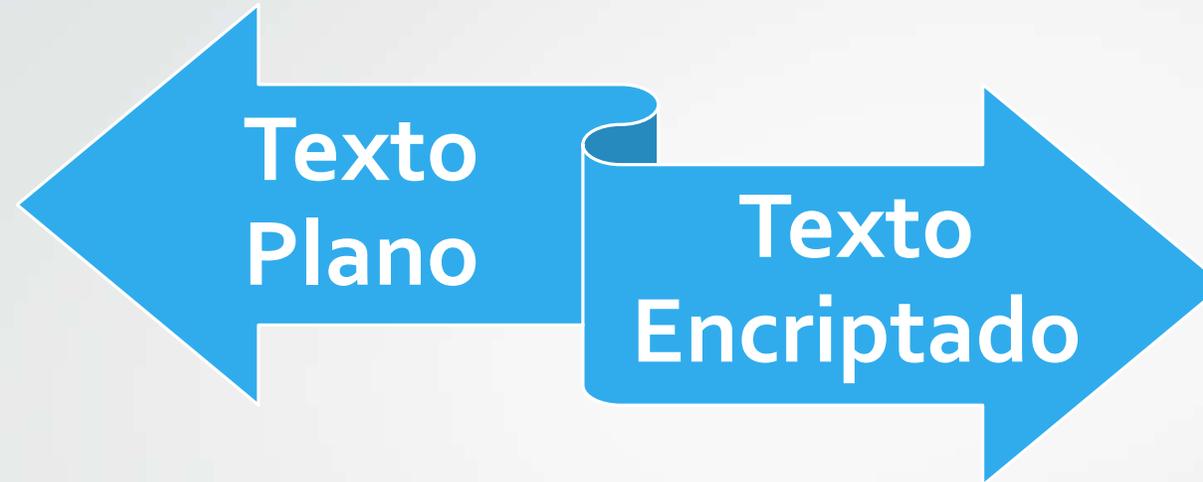
¿Qué es la criptografía?

¿Qué es la criptografía?

- La criptografía que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.



Definiciones



Ejemplo encriptación

Activex para encriptar y desencriptar archivos

| Texto a encriptar | Resultado |
|------------------------------------|---|
| grandes archivos de texto, etc. | UE42322A1D3F435F3B704F121602432 607221E14151A540759453D54031F06 48371D0D11490B19210603240E1509 1753694E211B1B1C1D4F161C433207 451200003D0D08071D010068451122 0E1901175348646352591106430A105 63C0745120000260A1A160642532111 157E627D6878002A4E141B17223572 42165236170056104E720E0E05061C1 A300819700007061B4F2B0F2F521D15 54430D14502111161F964E720E0E160 803162A1113700007111B4D2C142216 167D7E0042595032060456014126001 142041B1F300C1B350B1E045C2D4F6 |

Enciptar

Desencriptar

Tipos de Encriptación

Encriptación Simétrica

Encriptación Asimétrica

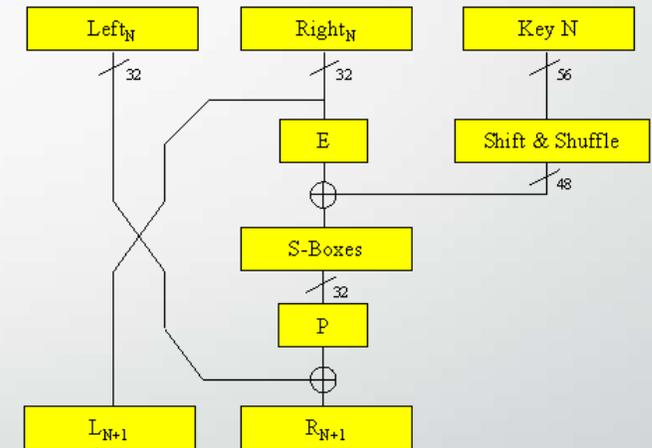
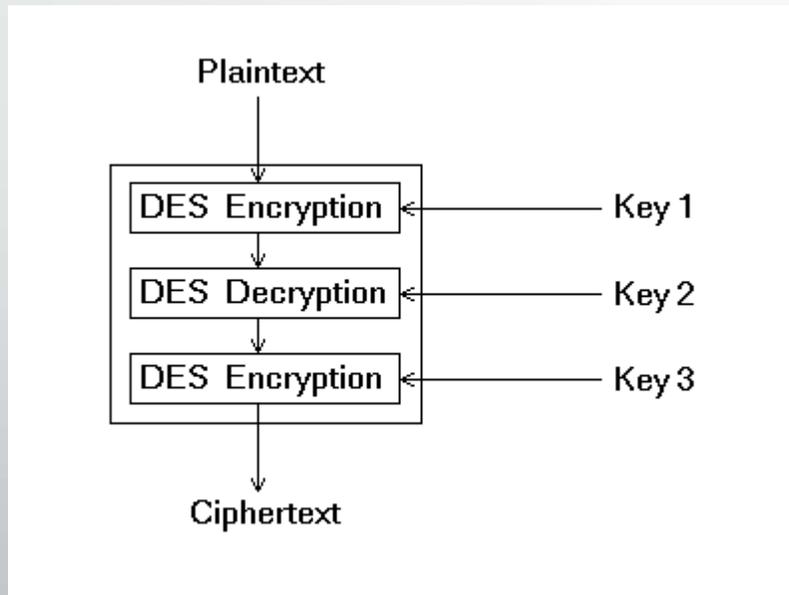
Encriptación Simétrica

Se utiliza la misma clave para encriptar y para desencriptar.



Ejemplos

DES - Data Encryption Standard
3DES - Data Encryption Standard
AES - Advanced Encryption Standard



Encriptación Asimétrica

Cada usuario tiene 2 claves.

Con una clave encriptamos y con otra clave desencriptamos.

Ejemplos:

- - Diffie-Hellman (distribución de claves)
- - ElGamal
- - RSA (Encriptación, firmas digitales)
(ESTÁNDAR INTERNACIONAL DE FACTO)

Ejemplo



Encriptación Asimétrica vs Simétrica



Cifrado Asimetrico

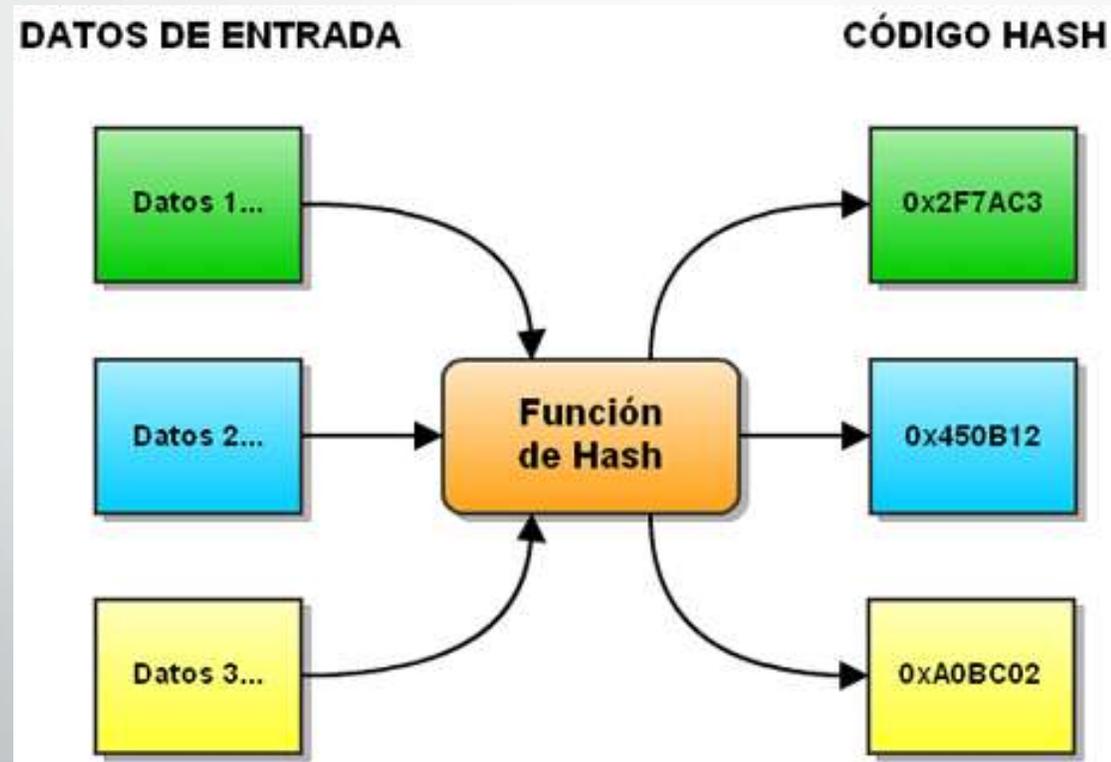


Cifrado Simetrico

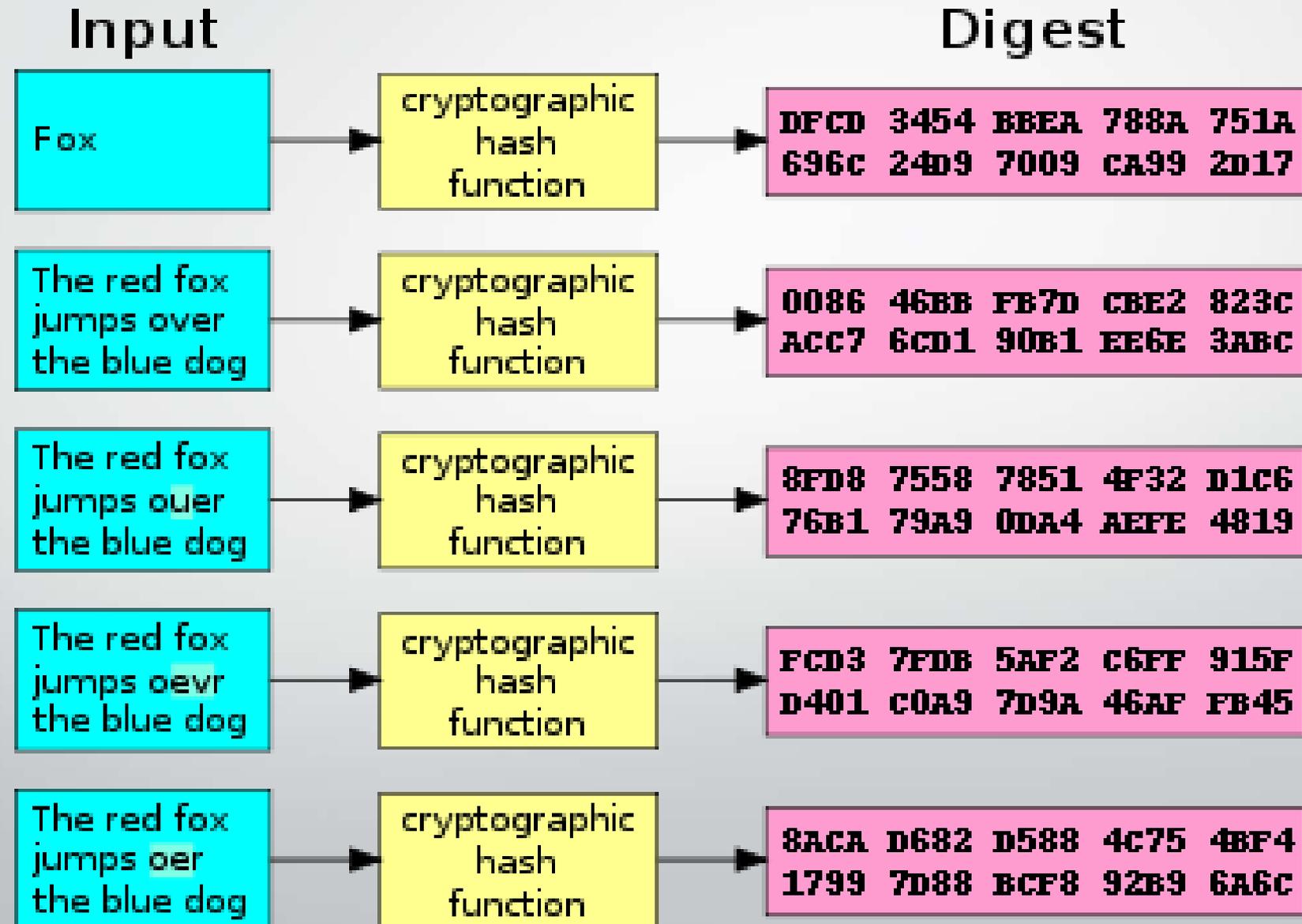
Función de HASH

¿Qué es una función de hash?

¿En qué se puede calcular?



Función de HASH



Ejemplo de función de Hash

 **Rentas**
de la Ciudad

Presentación de DJ por Internet
Acuse de recibo de DJ

Organismo Recaudador: D.G.R. GCBA
Formulario: 5202 v100 - IIBB - GOB. CIUDAD BS.
AS.
CUIT:
Impuesto: 5100 - IIBB-DGR.GOB.CIUDAD DE
BS.AS.
Concepto: 19 - OBLIGACION MENSUAL/ANUAL
Subconcepto: 19 - OBLIGACION MENSUAL/ANUAL
Período:
Nro. verificador:
Cantidad de registros:

NUMERO DE ISIB:

Fecha de Vencimiento: 2013-11-16
Fecha de Presentación: 2013-11-16 Hora: 21:06:01
Nro. de Transacción: 341850451
Código de Control: cA5u#p
Usuario autenticado por: AFIP (ClaveFiscal)

[017539F5202.dat]

Verificador de integridad (algoritmo MD5)
[cbc7a17fb806c08d9eda4fa6bfo44e69]

Conserve este Acuse de Recibo como comprobante de presentación

Datos sujetos a verificación

¡Muchas gracias!