3º Reunión: CICLO DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD DOCUMENTAL. CPCECABA, CABA, 2017.

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

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

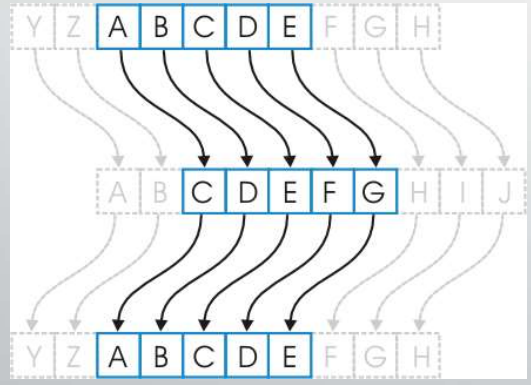
Dra. C.P. Esteban Mazzitelli

consejo
Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

¿Qué es la criptografía?

¿Qué es la criptografía?

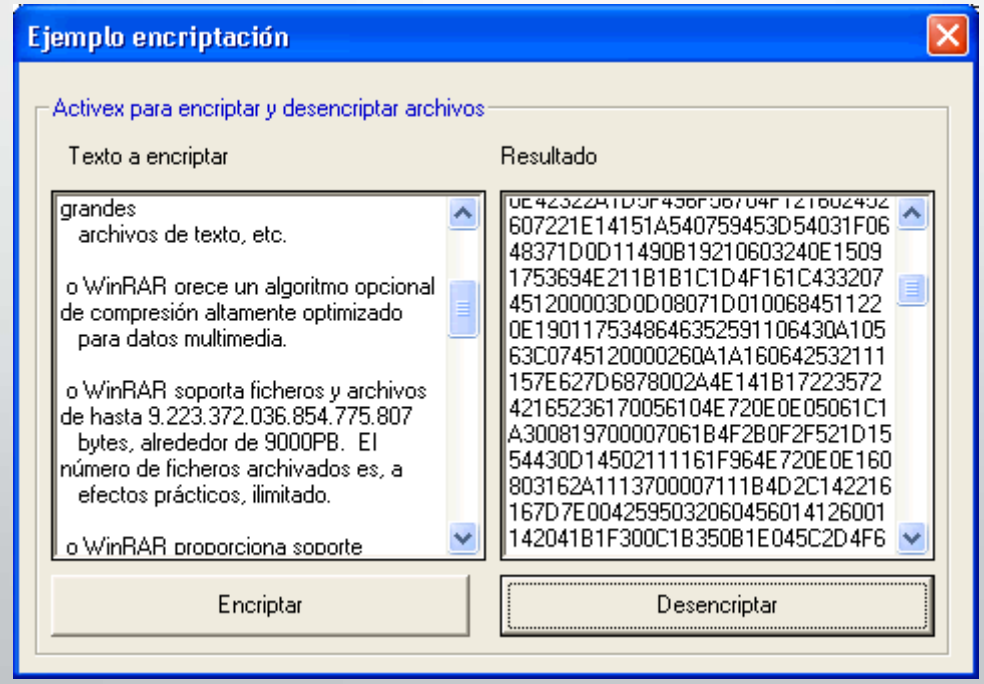
- La criptografía que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.



Definiciones

Texto Plano

Texto Encriptado



Tipos de Encriptación

Encriptación Simétrica

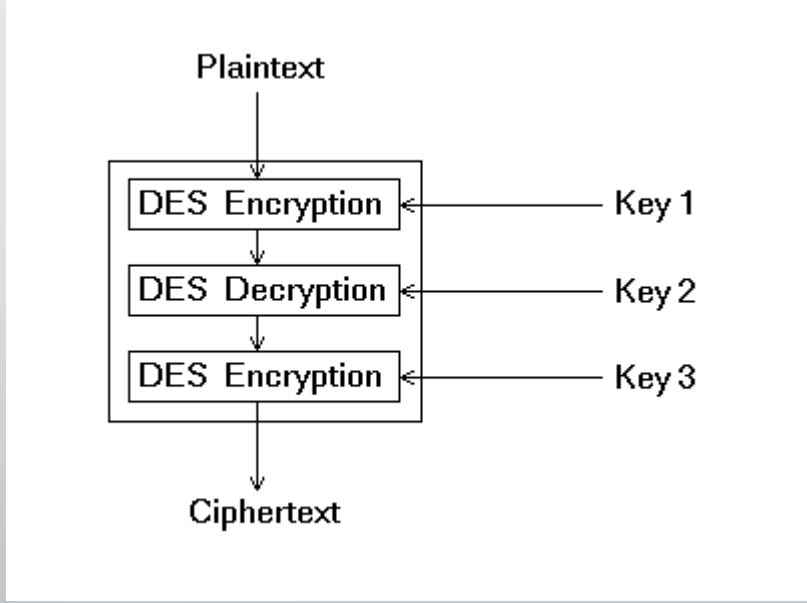
Encriptación Asimétrica

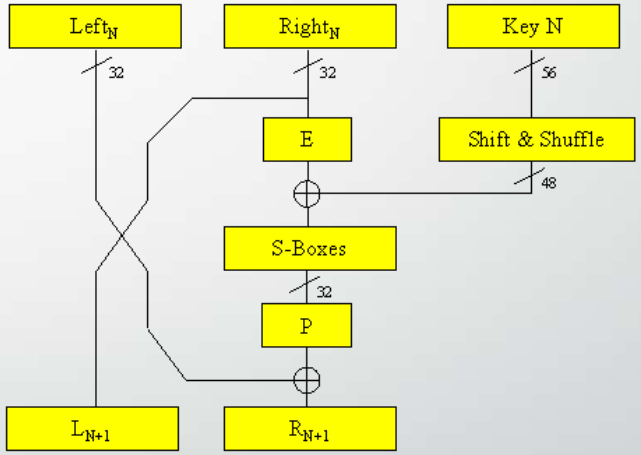
Encriptación Simétrica

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 (Encripción, firmas digitales)

(ESTÁNDAR INTERNACIONAL DE FACTO)

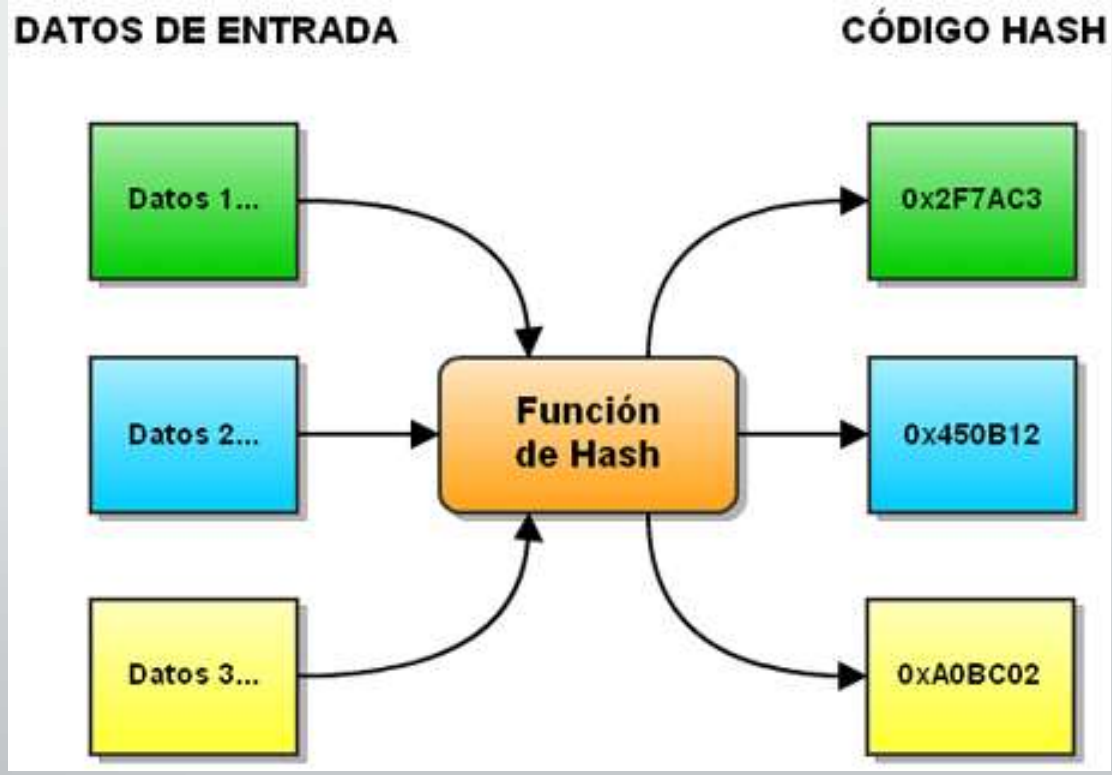
Ejemplo

Encriptación Asimétrica vs Simétrica

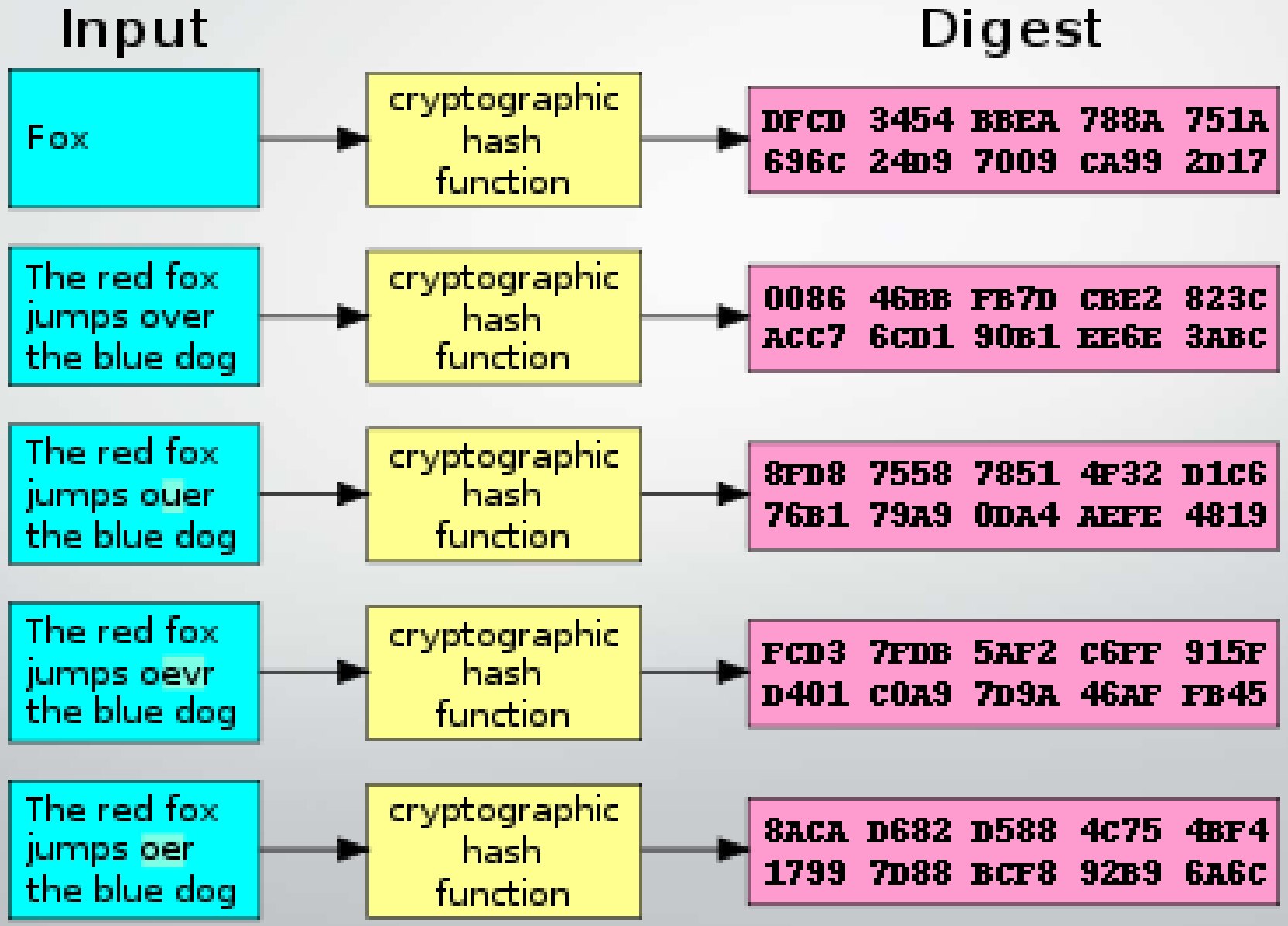
Función de HASH

¿Qué es una función de hash?

¿En qué de puede calcular?



Función de HASH



Ejemplo de función de Hash

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)

[cbc7a17fb806c08d9eda4fa6bfc44e69]

Conserve este Acuse de Recibo como comprobante de presentación

Datos sujetos a verificación

¡Muchas gracias!