Departamento de Tecnología Electrónica

CRIPTOGRAFÍA BÁSICA

Tecnologías Avanzadas de la Información

v19.1

Índice

- Funciones HASH
- Cifrado
- Certificados digitales
- Firma electrónica / digital
- Aplicaciones

Bibliografía

- Modern Cryptography Primer Theoretical Foundations and Practical Applications.
- Mathematics of Public Key Cryptography, Steven Galbraith.

Funciones HASH

Funciones HASH

- CRCs vs Checksums vs HASHs
  - CRC-16 / 32
  - Sum16 / 32, xor8
  - Corrección de errores ECC
- Funciones HASH:
  - Funciones deterministas
  - Toman como entrada una cadena de bits (bytes o words) de cualquier tamaño
  - Devuelven una cadena de bits (bytes) de tamaño fijo llamada huella o resumen

Funciones HASH

- Propiedades formales:
  - F(datos) = HASH
  - *preimage resistance*: dado un HASH no es computable encontrar una cadena de datos tal que F(datos) = HASH
  - *2nd preimage resistance*: dados unos datos no es computable encontrar otros datos con el mismo HASH
  - *collision resistance:* Es imposible/improbable encontrar 2 datos con el mismo HASH

Funciones HASH

- Se dividen en familias: Universales, Criptográficas, etc .
- Aplicaciones básicas
  - Integridad de datos
  - Verificación de datos
- Ejemplos:
  - MD5 ☹
  - SHA-1, SHA-256, SHA-512
  - BLAKE-256

Funciones HASH

md5(“1234”)	e7df7cd2ca07f4f1ab415d457a6e1c13
sha1(“1234”)	1be168ff837f043bde17c0314341c84271047b31
sha256(“1234”)	a883dafc480d466ee04e0d6da986bd78eb1fdd2178d04693723da3a8f95d42f4
sha512(“1234”)	7985558370f0de86a864e0050afdf45d7029b8798bcd72cddbf781329f99380e3f3b1afdca6765d89fc388b213df8f6a193cfc56d4ff2ef6e0a99bd883a6d98c

Departamento de Tecnología Electrónica

Cifrado: Simétrico / Asimétrico

Cifrado

- Utilizaremos técnicas criptográficas ampliamente utilizadas y estudiadas:
  - Cifrado simétrico
  - Cifrado asimétrico

Cifrado simétrico

- Cifrado simétrico:
  - Emisor y receptor utilizan la misma clave.
  - Ambos se ponen de acuerdo en la clave usada.
  - En caso de N nodos, todos tienen la misma clave (compartida).
- Desventajas:
  - Si un equipo está comprometido se tiene acceso a todas la comunicaciones.
  - Las claves precompartidas se pueden atacar por fuerza bruta (ejemplo claves WEP).

Cifrado simétrico

- Algoritmos de clave simétrica:
  - DES, IDEA, AES, RC5, Blowfish, etc…
  - Aunque se conozca el mensaje original enviado y el cifrado, obtener la clave debe ser costoso
  - La fortaleza depende de la complejidad del algoritmo y de la longitud de la clave
- Ventaja: Gran velocidad de ejecución

Cifrado simétrico

- Soluciones:
  - Cambiar la clave cada cierto periodo de tiempo (tiempo de vida)
  - El tiempo de vida debe ser menor que el tiempo requerido/estimado para descifrar la clave
- Se requiere un método de intercambio de claves seguro:
  - Complejo
  - Eslabón débil
  - Ejemplo: Algoritmo Diffie-Hellman

Cifrado asimétrico

- Cifrado asimétrico:
  - Basada en clave pública y privada
  - Cada parte tiene dos claves
- Algoritmos:
  - RSA, DSA, ECDSA, ElGamal, Diffie-Hellmanm
  - Basado en números primos y el problema de la factorización
  - Elliptic curve cryptography (ECC): Rápida y con claves más cortas

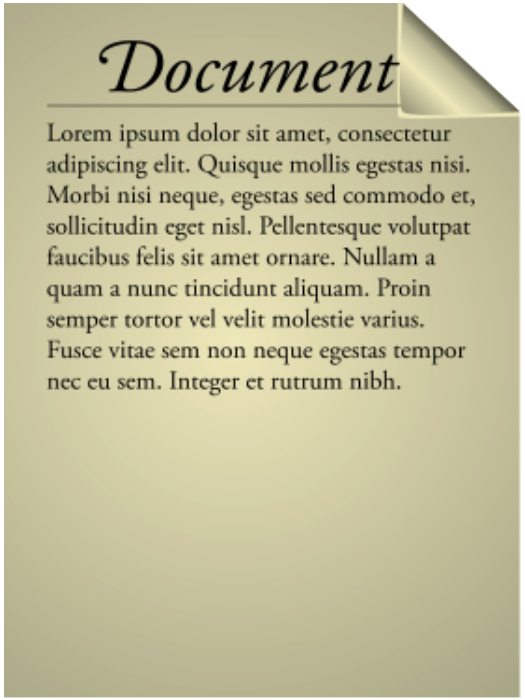
Cifrado asimétrico

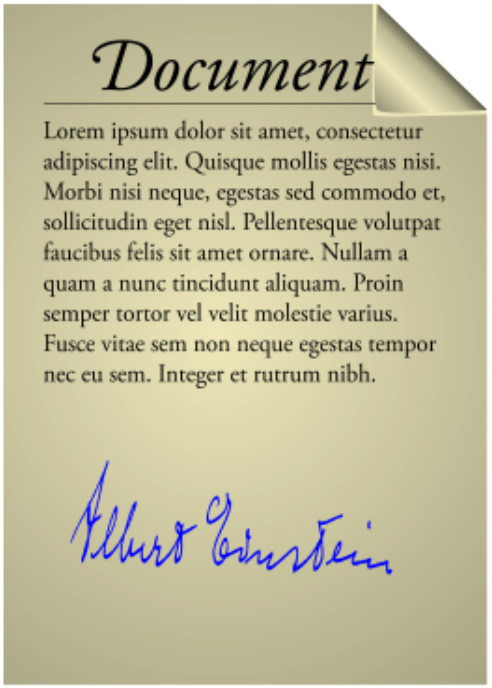
- Ventaja: No hay problemas de distribución de claves, sólo se intercambian las públicas
- Inconveniente: Algoritmos lentos y costosos
- Para asegurar el intercambio de claves aparecen las autoridades de certificación (CA) y certificados digitales.
- Todos estos elementos = PKI (Public Key Infraestructure)

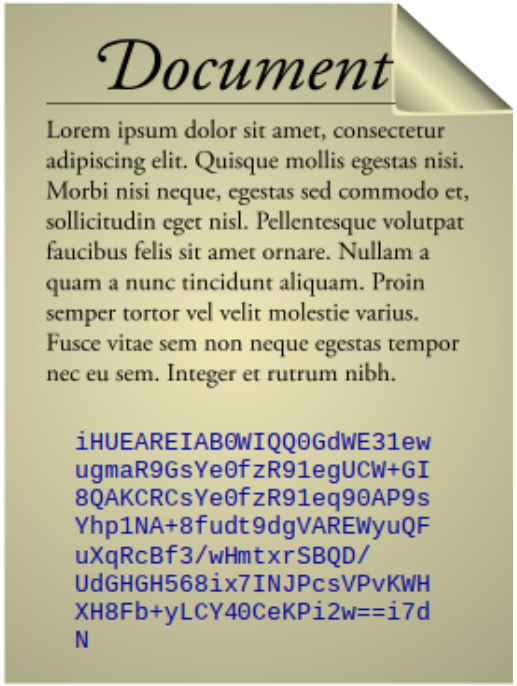
Cifrado asimétrico

- Objetivo: Asegurar la identidad de las partes cliente y servidor
- Firma electrónica:
  - Se aplica una clave secreta al HASH del contenido.
  - Asegura que el documento no sufre cambios
  - Esta firma puede ser comprobada por cualquier persona que disponga de la clave pública del autor.

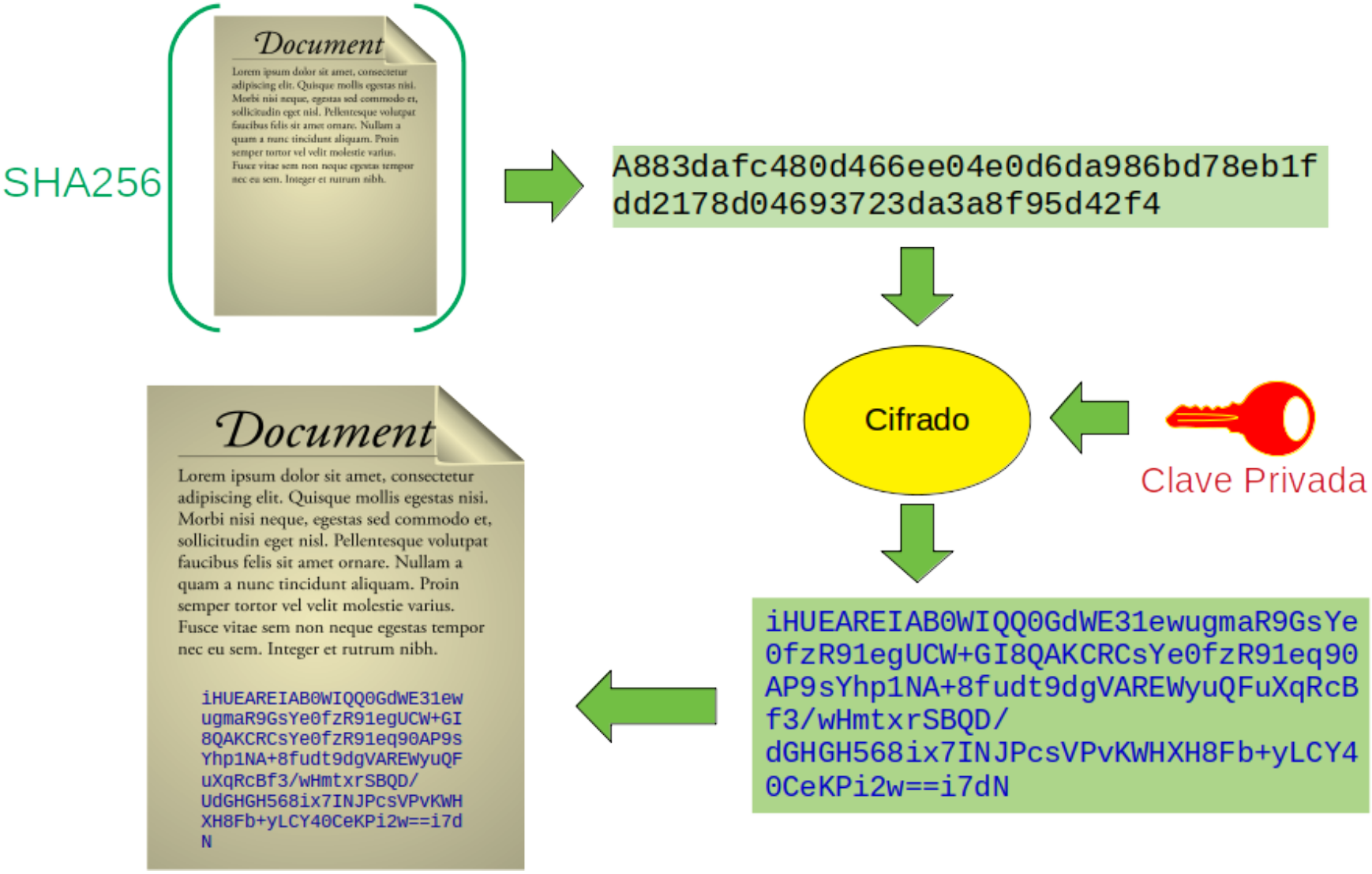
Cifrado asimétrico: Firma electrónica







Cifrado asimétrico: Firma electrónica



Cifrado asimétrico: Firma electrónica

- ¿Qué diferencia hay entre cifrar y firmar?
- ¿Cómo se comprueba si la firma es válida?
- Si se modifica el documento: ¿Cómo se detecta?
- ¿Se puede generar un nuevo documento con una firma válida? = Falsificar
- Para entender el procedimiento siga el siguiente ejemplo:

Cifrado asimétrico: Firma electrónica

- La firma electrónica es el HASH del contenido cifrado con la clave privada:
  1) Texto a firmar: “Este texto no puede ser cambiado y lo firmé el 21 de diciembre de 2017”
  2) SHA1(“Este texto no puede ser cambiado y lo firmé el 21 de diciembre de 2017”) = 85906ec3902f0270491c532316b62eae902beec2
  3) Encrypt(“85906ec3902f0270491c532316b62eae902beec2”,clave_privada) = owGbwMvMwCG4JvGt/Fn50irG0/pJDJE/cpwsTC0NzFKTjS0NjNIMjMwNTCwNk02NjYwNzZLMjFITU4HiSampyUZcHXEsDIlcDGysTCBtDFycAjCzdnxk+Ct4xOZl7tbXfo9eVjokeM1YwST6/3KcaLCFWlJd43q+Y5sY/hckt6xm2lbu8/P2J8P2B4pZVrPtxZOUrTglTh8LkDxWXQwA=VZvu

Cifrado asimétrico: Firma electrónica

- Ejercicio: verificar si es real y correcta la firma del ejemplo anterior (hecha con GPG)
- Resultado del ejemplo anterior:

```
Este texto no puede ser cambiado y lo firmé el 21 de
diciembre de 2017


Firmado por:
     paulino@dte.us.es

Firma:
    owGbwMvMwCG4JvGt/Fn50irG0/pJDJE/cpwsTC0NzFKTjS0
    NjNIMjMwNTCwNk02NjYwNzZLMjFITU4HiSampyUZcHXEsDI
    IcDGysTCBtDFycAjCzdnxk+Ct4xOZI7tbXfo9eVjokeM1Yw
    ST6/3KcaLCFWIJd43q+Y5sY/hckt6xm2lbu8/P2J8P2B4pZ
    VrPtxZOUrTglTh8LkDxWXQwA=VZvu
```

Cifrado asimétrico: Firma electrónica

- Verificación de la firma electrónica:
  1) Obtener la clave publica del firmante (GPG)
  2) Autoridad de certificación: ¿Es realmente su clave pública?
  3) encrypt("owGbwMvMwCG4JvGt/Fn50irG0/pJDJE/cpwsTC0NzFKTjS0NjNIMjMwNTCwNk02NjYwNzZLMjFITU4HiSampyUZcHXEsDIlcDGysTCBtDFycAjCzdnxk+Ct4xOZI7tbXfo9eVjokeM1YwST6/3KcaLCFWIJd43q+Y5sY/hckt6xm2Ibu8/P2J8P2B4pZVrPtxZOUrTgITh8LkDxWXQwA=VZvu",clave_publica) = 85906ec3902f0270491c532316b62eae902beec2
  4) Lo obtenido: ¿es el HASH del documento?

Cifrado asimétrico: Firma electrónica

- El ejemplo anterior, GPG lo automatiza:
  - Firmar:
    ```
    gpg -a -b documento.txt
    ```
  - Comprobar:
    ```
    gpg --verify documento.txt.asc
    ```
  - Aunque no se disponga de la clave pública, la firma contiene información sobre el firmante
  - Obtener la clave pública desde:
    - https://keyserver.ubuntu.com/
    - https://pgp.mit.edu/
    - http://www.rediris.es/keyserver
    - https://pgp.mit.edu
  - Recomendación: instalar "*seahorse*"

```
Este documento
no se puede
falsificar
```

documento.txt

```
-----BEGIN PGP SIGNATURE-----

iHUEABEIAB0WIQQ0GdWE31ewugmaR
9GsYe0fzR91egUCW+VLEQAKCRCsYe
0fzR91el6uAP9bjA6bSCNv2gXwNNF
eAaxWmLW7nw0bhjAgj0onk1Y3uAD9
FyJD84hiC8OHPxHQKo+8Hq2EvbqVn
KJnY1T9dsspVtI==u7H5
-----END PGP SIGNATURE-----
```

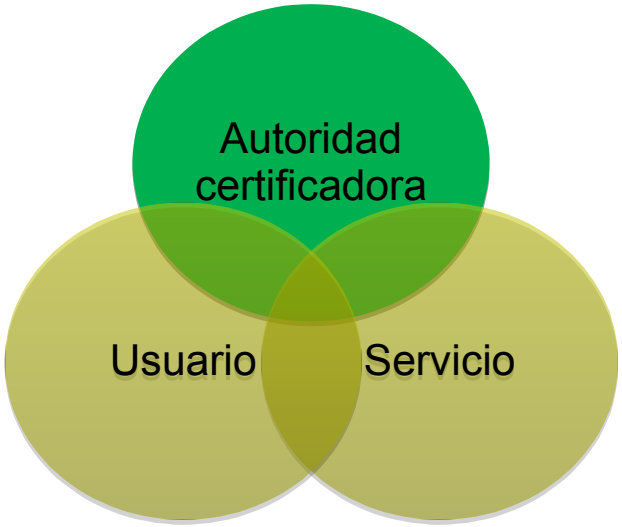
documento.txt.asc

Cifrado asimétrico: Firma electrónica

- Verificación de la firma: ¿La clave pública obtenida es realmente la clave pública deseada?
  - GPG:Usa un anillo de confianza
    - Las claves públicas son firmadas por otros usuarios
    - Debe seleccionar aquellas firmas en las que confía
    - Probar el software seahorse o kleopatra
  - PKI X.509 [RFC5280]
    - Los certificados están únicamente firmados por la Autoridad de Certificación.
    - Contienen la clave pública y otros datos extra.
    - ¿Quien firma el certificado de la Autoridad de Certificación?

Cifrado asimétrico: Certificados digitales

- Certificado digital: Archivo firmado con la clave privada de una autoridad de certificación
- Autoridad de certificación:
  - Evita la suplantación, con su firma certifica que alguien es quien dice ser.
  - Ambas partes confían en la autoridad.
  - Todos conocen la clave pública de la autoridad



Cifrado asimétrico: Certificados digitales

- Cometido de las Autoridades de certificación:
  - Generan certificados digitales firmando la clave publica y algunos otros datos incluidos en el certificado.
  - Revocan certificados digitales emitidos previamente.
  - **CRL**: Listado de revocación de certificados gestionado por la CA.
  - Forman una Jerarquía.
  - La raíz es un certificado autofirmado.
  - Cada país tiene una lista de CA.
  - Ejemplos: VeriSign, FNMT, CAcert.

Cifrado asimétrico: Certificados digitales

- Ordenamiento jurídico:
  - Ley 59/2003 firma electrónica, certificado electrónico, DNI-e, etc.
  - Elimina barreras legales de la firma electrónica
  - Potencia del desarrollo de Internet
- Conceptos regulados:
  - Firma electrónica: simple, avanzada y reconocida [PAE]
  - Certificado digital
  - Autoridad de certificación
  - DNI-e

Cifrado asimétrico: Certificados digitales

- Existen diversos formatos, X.509 estandarizado [RFC5280]
- Además de la clave pública y firma de la CA contienen muchos campos adicionales


```
-----BEGIN CERTIFICATE-----
MIIDojCCAoqgAwIBAgIQE4Y1TR0/BvLB+WUF1ZAcYjANBgkqhkiG9w0BAQUFADBr
MQswCQYDVQQGEwJVUzENMAsGA1UEChMEVklTQTEvMC0GA1UECxMmVmlzYSBJbnRl
cm5hdGlvbmFsIFNlcnZpY2UgQXNzb2NpYXRpb24xHDAaBgNVBAMTE1Zpc2EgZUNv
bW1lcmNlIFJvb3QwHhcNMDIwNjI2MDIxODM2WhcNMjIwNjI0MDAxNjEyWjBrMQsw
CQYDVQQGEwJVUzENMAsGA1UEChMEVklTQTEvMC0GA1UECxMmVmlzYSBJbnRlcm5h
dGlvbmFsIFNlcnZpY2UgQXNzb2NpYXRpb24xHDAaBgNVBAMTE1Zpc2EgZUNvbW1l
cmNlIFJvb3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvV95WHm6h
2mCxlCfLF9sHP4CFT8icttD0b0/Pmdjh28JIXDqsOTPHH2qLJj0rNfVIsZHBAk4E
lpF7sDPwsRROEW+1QK8bRaVK7362rPKgH1g/EkZgPI2h4H3PVz4zHvtH8aoVlwdV
ZqW1LS7YgFmypw23RuwhY/81q6UCzyr0TP579ZRdhE2o8mCP2w4lPJ9zcc+U30rq
299yOlzzlr3xF7zSujtFWsan9sYXiwGd/BmoKoMWuDpI/k4+oKsGGelT84ATB+0t
vz8KPFUgOSwsAGl0lUq8ILKpeeUYiZGo3BxN77t+Nwtd/jmliFKMAGzsGHxBvfaL
dXe6YJ2E5/4tAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgEGMB0GA1UdDgQWBBQVOIMPPyw/cDMezUb+B4wg4NfDtzANBgkqhkiG9w0BAQUF
AAOCAQEAX/FBfXxcCLkr4NWSR/pnXKUTwwMhmytMiUbPWU3J/qVAtmPN3XEolWcR
zCSs00Rsca4BIGsDoo8Ytyk6feUWYFN4PMCvFYP3j1IzJL1kk5fui/fbGKhtcbP3
LBfQdCVp9/5rPJS+TUtBjE7ic9DjkCJzQ83z7+pzzkWKsKZJ/0x9nXGIxHYdkFsd
7v3M9+79YKWxehZx0RbQfBI8bGmX265fOZpwLwU8GUYEmSA20GBuYQa7FkKMcPcw
++DbZqMAAb3mLNqRX6BGi01qnD093QVG/na/oAo85ADmJ7f/hC3euiInlhBx6yLt
398znM/jra6O1I7mT1GvFpLgXPYHDw==
-----END CERTIFICATE-----
```


Certificado X.509 codificado PEM

Certificados digitales

> openssl x509 -in www.microsoft.com.crt -text
Data:
Version: 3 (0x2)
Serial Number: 03:eb:7e:1d:9b:4c:4c:7b:14:5f:f6:a9:02:ce:81:f9
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
Validity
Not Before: Apr 7 00:00:00 2017 GMT
Not After : Apr 8 23:59:59 2019 GMT
Subject: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=MSCOM, CN=www.microsoft.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:b5:aa:73:e7:bd:ff:a0:6c:6a:1d:0f:0e:11:63:
86:ac:b9:8c:55:c2:7e:ec:1f:df:01:64:53:9d:33:
7f:4d:66:ee:08:24:ce:63:55:92:74:11:77:02:62:
ac:28:46:19:ae:06:f2:ba:ad:f3:d9:e0:3e:40:85:
0f:42:84:6f:82:1a:f4:92:19:e7:ef:84:34:ae:f7:
6d:b5:e3:e9:f1:7a:fb:5c:e0:4e:45:95:9b:77:cc:
9b:55:81:9e:c5:01:b5:97:9f:34:5d:f1:00:51:ac:
45:69:26:a4:8c:d4:4f:0e:c8:fb:d3:e8:e9:1d:5a:
76:c3:5c:88:2d:c8:fa:95:27:5a:c2:15:0a:cf:99:
0d:40:19:b9:6e:55:49:7c:b1:f4:6a:84:26:43:c6:
41:68:df:d8:a3:1a:c4:a1:e8:08:df:71:0c:53:36:
3a:da:f8:2b:5f:62:c9:a2:aa:ee:1f:ec:64:88:0d:
95:1e:7d:48:bd:b3:fd:f7:24:e2:5f:67:f3:73:d2:
ec:14:26:b7:e4:ba:2b:60:44:2a:42:32:0d:3f:ef:
96:64:0b:6e:79:5c:f8:c4:fe:b2:8e:16:08:cb:96:
8b:bb:83:b6:5f:96:bb:51:75:68:20:95:31:0c:e5:
fd:02:80:5a:a9:27:33:26:f7:a9:e8:b3:37:30:eb:

Exponent: 65537 (0x10001)

.....

X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:privacy.microsoft.com, DNS:c.s-microsoft.com, DNS:microsoft.com, DNS:i.s-microsoft.com, DNS:staticview.microsoft.com, DNS:www.microsoft.com, DNS:wwwqa.microsoft.com

X509v3 Authority Key Identifier:
keyid:5F:60:CF:61:90:55:DF:84:43:14:8A:60:2A:B2:F5:7A:F4:43:18:EF

X509v3 CRL Distribution Points:
Full Name:
URI:http://ss.symcb.com/ss.crl

Signature Algorithm: sha256WithRSAEncryption
46:27:13:c1:95:07:8a:60:7a:22:6f:b4:27:9e:2c:ba:8c:36:
3d:a6:f4:69:6b:88:67:7e:83:e1:e8:ba:57:73:68:1b:a2:ea:
ba:14:1a:42:5c:b2:e9:e0:65:ef:2d:10:37:35:3c:7b:d3:1f:
39:c6:3c:b2:b0:44:9f:0a:f1:bf:bc:7e:90:c1:75:c3:35:43:
7a:ae:d1:0a:a0:a1:5b:b6:7b:35:7e:8e:9f:7d:ff:2c:3d:25:
a4:67:d1:28:78:80:9e:11:47:17:ee:a8:77:17:5d:f2:55:95:
47:28:ba:bc:5e:61:6b:55:26:2e:dc:49:40:19:b6:e8:30:1d:
8d:8d:67:6d:86:73:1f:ce:ca:af:04:0c:6d:8d:93:ba:60:8a:
d7:f7:6d:40:65:a8:3b:b6:e9:ae:de:32:08:be:45:74:21:3d:
47:87:64:af:06:34:77:3b:4f:a5:54:3a:a3:52:3e:d7:95:dc:
1a:fc:76:d8:a8:aa:ea:09:e0:b2:59:ab:c6:92:4a:82:c2:f1:
d5:e6:f7:f1:8b:13:1e:ec:9b:16:3c:e1:1a:83:39:fa:a5:24:
26:10:5f:05:31:36:b2:45:e5:1b:8b:e8:36:ef:e6:a7:56:71:
f1:fc:02:cc:6f:5b:f6:be:19:ae:00:17:1e:27:fe:15:7f:d1:
dc:32:37:84

Ejemplos de aplicaciones

Aplicaciones

- Tecnologías
  - Autenticación: Almacenes de ~~contraseñas~~ hashs
  - Cifrado punto a punto
  - Infraestructuras de clave pública (PKI)
  - IPSec
  - Túneles cifrados
  - Firma electrónica
  - BlockChain
  - SSL
  - PGP / GPG
  - Etc.

Aplicaciones: Autenticación

- Ejemplo: ¿Contraseñas guardadas en Linux?
  - Necesidad de uso del salto
  - Formato: **FSALTO$HASH**
    - F = 1 → MD5
    - F = 2 → blowfish (¿función hash?)
    - F = 4 → SHA1
    - F = 5 → SHA2-256
    - F = 6 → SHA2-512
  - Resultado en base64 en el conjunto [a–z,A–Z,0–9,./,]
  - Probar comandos: md5pass, sha1pass, frente a md5sum

Fichero /etc/shadow en linux

```
ana:$4$kk$KDHqofE/HuX5QU8d64ZB7gfdcLo:15104:0:99999:7:::
july:$1$ale$XS7uv3N9fqq/qJg/wOoYn0:15236:0:99999:7:::
lucia:$6$437ZX.Mb$qK0HTP/3zXfvjbIlN30rw0vsZggBWAO3/4vR0H.----/2C.:15322:0:99999:7:::
sistema::*:16113:0:99999:7:::
```

Aplicaciones: Autenticación

- ¿Contraseñas guardadas en WordPress?
  - Usan muchos de ellos todavía MD5
  - 3 vectores de ataque
    - Fuerza bruta
    - Colisiones
    - Inyección SQL

Tabla wp_users de Wordpress

ID	user_login	user_pass	user_nicename
2	sport	PBebXfgXh3UNiYUNcVPNGi8ckSIbFnO.	Agente
3	miguel	PBm/PTz.2t3yseAE4rbnxr7pRNcWOyU.	Administrador
4	belen	PB.yEGjuZ0B9GoBjXGOigSC6xexULS2/	Comercial
5	rido	PBu7hsPqX6yods3KccHPY/6buV5UB8Q1	Gerente

Aplicaciones: Autenticación

- Wordpress usa phpass con el formato:

PRSALTOHASH

Aplicaciones: Autenticación

- Ejemplos de ataque por fuerza bruta

Nvidia GTX 1080 Hashcat Benchmarks	
SHA1	8538.1 MH/s
SHA256	2865.2 MH/s
MD5	24943.1 MH/s
SHA512	1071.1 MH/s
phppass (Wordpress/Joomla)	6917.9 kH/s

Aplicaciones: SSL/TLS

- SSL: Secure Sockets Layer.
  - Estándar de comunicaciones cifradas con servidores Web (Obsoleto 1996)
  - Es un protocolo para dar seguridad a la capa de transporte
- TLS: no es más que una nueva versión de SSL (v1.3 2018)
  - Fácil de utilizar a nivel de programación (API)
  - StartTLS: Utilizado para iniciar comunicación segura a partir de una comunicación plana de texto inicial

Aplicaciones: SSL/TLS

- Versiones:
  - TLS 1.0, 1.1, 1.2 y 1.3
    - TLS 1.0 20 años de antigüedad
    - TLS 1.1 12 años de antigüedad
  - TLS 1.0 y 1.1: vulnerables a POODLE, BEAST etc. (Buscar POODLE , sept. 2014).
  - Se recomienda eliminar el soporte 1.0/1.1 de todos las aplicaciones/sistemas
  - Google Chrome, Apple Safari, Microsoft Edge, Internet Explorer, y Mozilla Firefox lo eliminarán en 2020

Aplicaciones: Firma electrónica

- Firmado de software:
  - Apps Stores: GooglePlay, Apple
  - Debian / Ubuntu: GPG
- Administración electrónica
  - https://firmaelectronica.gob.es

Aplicaciones: Block chain

- Blockchain (HASH):
  - Base de datos: almacenamiento en bloques de datos
  - Bloques de tamaño fijo/variable según la implementación
  - Los bloques están en forma de lista enlazada
  - Se mantienen la integridad de la lista usando HASHs, tanto de los bloques como de los datos contenidos
  - Merkletree / Merkleroot: Consiste en aplicar una función HASH a los resultados HASH anteriores.

Aplicaciones: Block chain

- Blockchain ≠ Contabilidad distribuida
- Blockchain = 90% marketing + 10% tecnología
- Tecnologías usadas en contabilidad distribuida
  - Blockchain
  - Red P2P
  - Cifrado Asimétrico
  - Funciones HASH
  - Algoritmo de Consenso: prueba de trabajo, prueba de participación
- Vulnerable a ataques del 51%

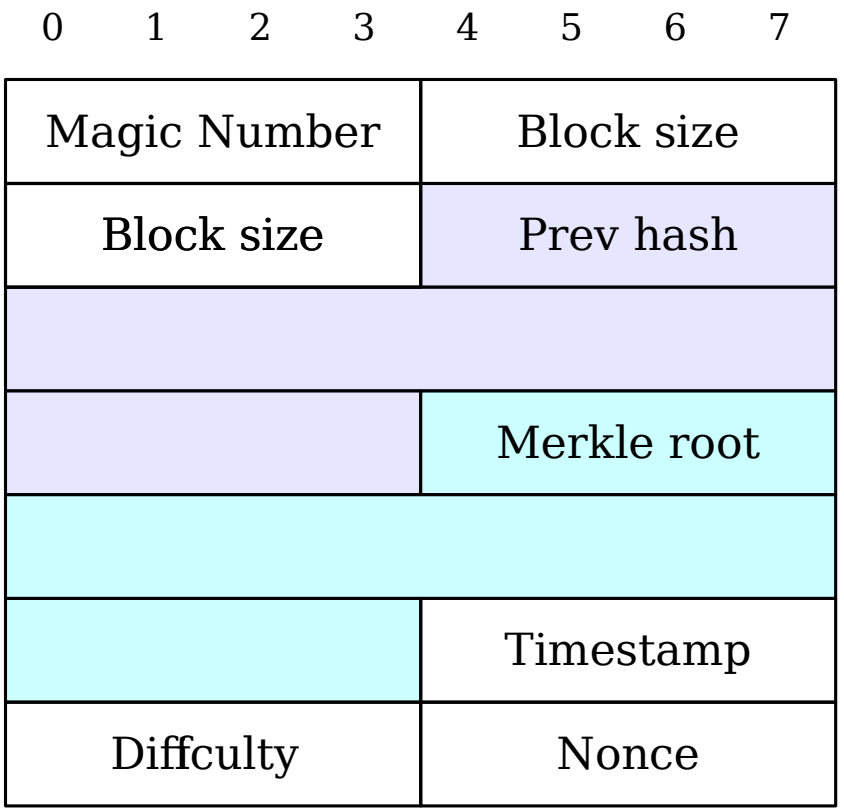
Aplicaciones: Bitcoin

- Transacciones:
  - Todas son públicas
  - Se firman con ECDSA
  - Buscar exploradores de cadenas [Blockchair]
  - ¿Dónde está la privacidad?
- Minería:
  - Búsqueda de HASH con ciertas propiedades (menor de un valor)
  - Las propiedades del HASH cambian cuando se ajusta la dificultad (actualmente 10 minutos por cierre de bloque)
  - Quien cierra un bloque puede crear una transacción con la recompensa hacia su cartera.
  - Tamaño de bloque limitado a 2M hasta que se activó SegWit
  - 2018: Picos de 68,9318566 EH/s, 68,94 trillones de hashes por segundo en la red.

Aplicaciones: Bitcoin

- Formato de bloque

F.Size	Description	Data type
4	magic	int32_t
4	size	int32_t
4	version	int32_t
32	prev_block	char[32]
32	merkle_root	char[32]
4	timestamp	uint32_t
4	bits	uint32_t
4	nonce	uint32_t
1	txn_count	var_int



Aplicaciones: Bitcoin

- Generación:
  - Se generan al cerrar un bloque
  - Limite de ~21 millones
  - Moneda deflaccionaria
- Doble HASH + MerkleRoot: SHA-256
- Reducción programada de la recompensa:
  - Cada 210.000 bloques
  - 2012 de 50 a 25
  - 2016 de 25 a 12.5