Ciberseguridad

Bloque 4.

Blockchain como herramienta para trazabilidad y securización de flujos de información.

Ezequiel Herruzo Gómez

eze@uco.es

Bloque 4.- Blockchain como herramienta para trazabilidad y securización de flujos de información.

Tema 1.- Cifrado y hash

Tema 2.- Trazabilidad

Tema 3.- Blockchain

Cifrado y hash

- **Generalidades de la encriptación asimétrica.**
- **Algoritmos. Elgamal y Curva elíptica.**
- **Funciones hash. SHA-256.**
- **Generadores de claves.**
- **Firma electrónica y certificado digital.**
- **¿El futuro de la criptografía?**

Cifrado y hash

Generalidades encriptación asimétrica

Uso de dos claves (cifrar y descifrar) para el envío de mensajes.

- Claves privada y pública.
  - Clave privada: Base del sistema criptográfico y propiedad del generador de claves.
  - Clave pública: Distribuida entre los usuarios del sistema.
    - Existencia de numerosas claves públicas.
    - Ninguna clave pública puede ser calculada a partir de otra clave pública.

Cada pareja de claves sólo se puede generar una vez.

Una de las claves nunca podrá ser calculada a partir de su par.

Cifrado y hash

Generalidades encriptación asimétrica

Funcionamiento:

Cifrado y hash

Generalidades encriptación asimétrica

Posibilidades de cifrado:

- Encriptación mediante clave pública.

  Propiedad de confidencialidad.

- Encriptación mediante la clave privada.

  Propiedad de autenticidad.

Cifrado y hash

Generalidades encriptación asimétrica

Importancia de la complejidad de las claves en el cifrado asimétrico

Confianza en la clave pública:

- Correcta.
- No alterada.
- No conocida por usuarios externos (depende del uso).

El problema de intercambio de claves.

¿Cómo hacer llegar al usuario final su clave de forma segura?

Mecanismos: Centralizados; Distribuidos.

Cifrado y hash

Algoritmos. Elgamal y Curva elíptica

Elgamal:

Basado en el problema matemático del logaritmo discreto.

Idea: Crear mecanismo de pares de claves relacionadas, entre usuarios que no han tenido contacto entre sí.

Propiedades del algoritmo basadas en:

- Propia definición de logaritmo. Distinta complejidad operación directa e inversa.
- Establece grupo cíclico discreto, con infinitas posibles soluciones.
- Añade las particularidades de los número primos. Se facilitan ciertas operaciones y complican otras.

Cifrado y hash

Algoritmos. Elgamal

Aclarando:

Logaritmo de un número es el exponente al que hay que elevar la base para obtener dicho número.

$\log_n P = x$, quiere decir que: $P = n^x$

Diferente dificultad de ejecución de la operación directa a la inversa.

Asociar las particularidades anteriores a un grupo cíclico puede suponer tener infinitas soluciones posibles.

5 mod 8 = 5; 13 mod 8 = 5; si seguimos: 21 mod 8 = 5

teniendo una misma solución (5).

Pueden existir infinitos valores que la satisfagan.

Cifrado y hash

Algoritmos. Elgamal

Aclarando:

Habría que probar cada uno de los valores para saber si es la solución buscada.

Si hacemos mucho mayor el número divisor, el grupo cíclico se amplía y la detección de las posibles claves se complica hasta hacerla imposible.

Ej. (256 b): 898402865429232609682269648299642774036187389532602614743605419008198227990 21

Divisor número primo => Aplicación de numerosas particularidades matemáticas

Pequeño teorema de Fermat, permite la realización de operaciones clave en criptografía

Cifrado y hash

Algoritmos. Elgamal

Proceso de comunicación: Generación de clave.

Elección de un número primo ‘p’ lo suficientemente grande como para que la solución del logaritmo discreto en el grupo cíclico (mod p) sea muy compleja.

Se eligen ‘g’ y ‘a’ dentro de este grupo cíclico de modo aleatorio

(en concreto $0 < a < (p-1)$, donde ‘a’ será la clave privada del sistema generador).

Se crea ‘K’ del siguiente modo:

$$K = g^a \pmod p$$

Consiguiendo la clave pública, compuesta por los valores: (g, p, K).

Nótese que el cálculo de ‘K’ es muy sencillo si lo comparamos con el posible cálculo de la clave privada ‘a’, donde tendríamos que resolver: $a = \log_g K \pmod p$.

Cifrado y hash

Algoritmos. Elgamal

Proceso de comunicación: Difusión de clave

La clave pública es difundida entre los usuarios del sistema criptográfico.

(g, p, K)

Si un usuario que forma parte del sistema criptográfico quiere enviar el mensaje ‘m’ al propietario de la clave privada ‘a’ se realizará el proceso siguiente…

Cifrado y hash

Algoritmos. Elgamal

Proceso de comunicación: Cifrado de mensaje.

Para enviar el mensaje ‘m’ encriptado con este algoritmo, el emisor enviará la dupla (y_1, y_2), calculada:

$$y_1 = g^b \pmod p$$

$$y_2 = K^b \cdot m \pmod p$$

donde ‘b’ es un número aleatorio elegido por el emisor dentro del grupo cíclico (mod p). $(0 < b < p)$

b será la clave privada del emisor.

Cifrado y hash

Algoritmos. Elgamal

Proceso de comunicación: Desencriptado y recepción mensaje

El receptor, propietario de la clave privada 'a', tras recibir la dupla (y_1, y_2), realizará el siguiente cálculo:

$$y_1^{-a} \cdot y_2 \pmod p$$

Resolviendo la expresión anterior…

$$(g^b)^{-a} \cdot K^b \cdot m \pmod p = g^{-ab} \cdot (g^a)^b \cdot m \pmod p = m \pmod p$$

Teniendo de este modo en recepción el valor del mensaje 'm' enviado por el emisor.

(recordad pequeño teorema de Fermat)

Cifrado y hash

Algoritmos. Curva elíptica

Generalidades ECDSA: Eliptic Curve Digital Signature Algorithm

Pertenece a la familia de algoritmos DSA, de firma digital.

Introduce la criptografía de curva elíptica (ECC) en algoritmos de firma digital.

Asegura:

- La información no es revelada a terceros.
- Permite identificar y verificar la procedencia del mensaje.
- Permite conseguir la confidencialidad en el envío de mensajes.

Mucho más seguro para el mismo tamaño de claves.

- ECDSA y clave 192 bits, misma seguridad que RSA y clave 1024 bits.

Cifrado y hash

Algoritmos. Curva elíptica

Generalidades ECDSA: Eliptic Curve Digital Signature Algorithm

Proceso básico de generación de claves.

1. Selección de una curva elíptica *E*
   (de la forma $y^2 = x^3 + a \cdot x + b$)
2. Selección de un punto *P* (existente en *E*) de orden *n*.
   (n es un número natural elegido por el generador)
3. Selección de un número aleatorio *d* en el intervalo [1, *n - 1*].
4. Se calcula $Q = d \cdot P$.

d es la clave privada.

Q es la clave pública.

Cifrado y hash

Algoritmos. Elgamal y Curva elíptica

Destacar:

RSA (Rivest-Shamir-Adelman):

Uno de los algoritmos de encriptación asimétrica más antiguos. Este algoritmo genera una clave pública a partir de dos números primos de gran tamaño y un valor auxiliar. Los números primos serán la clave privada.

Habitualmente proporcionan:

Técnicas de validación de claves.

Algoritmos de firma.

Mecanismos de generación de valores pseudo-aleatorios.

Cifrado y hash

Funciones hash. SHA-256.

Asegurar el envío de información a través de las redes, debe cumplir:

- Integridad: La información debe ser correcta y no haber sido modificada por agentes no autorizados.

- Confidencialidad: La información no debe ser divulgada a entidades no autorizadas.

- Disponibilidad: Es posible acceder a la información siempre que se necesite.

(Posible conflicto entre Confidencialidad y Disponibilidad)

Cifrado y hash

Funciones hash. SHA-256.

Mecanismos que ayudan a mantener la integridad de la información:

a) La gestión de permisos que realizan los administradores de sistemas.

b) El registro de los accesos a los archivos.

c) El control de versiones en usuarios autorizados.

d) Copias de seguridad o respaldo. Permiten restauración.

e) En comunicaciones, la aplicación de funciones resumen o hash.

Realizar una comprobación entre la información de resumen del mensaje recibido y los datos de resumen generados de la información útil recibida.

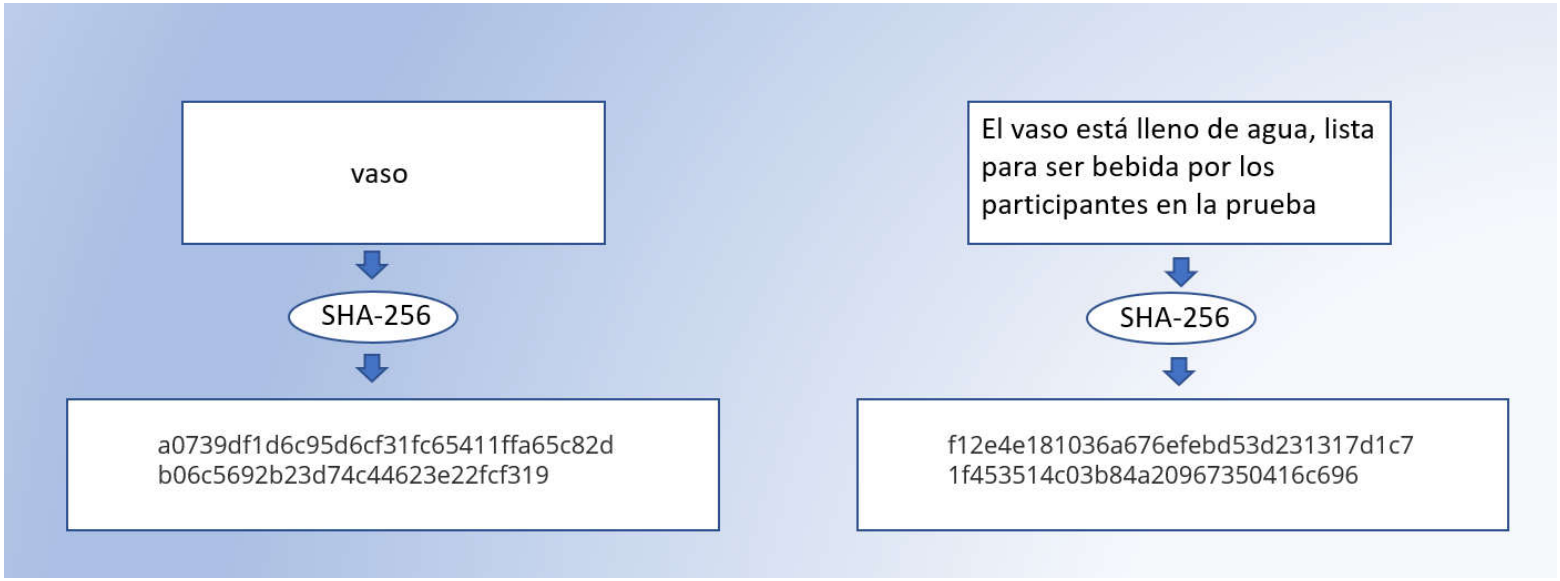
Características del hash o resumen:

- Tamaño fijo del hash.
- Unidireccionalidad. No Podemos obtener el mensaje a partir del hash.
- Unicidad. El hash es único por mensaje. Incluso cambios mínimos.

Cifrado y hash

Funciones hash. SHA-256.

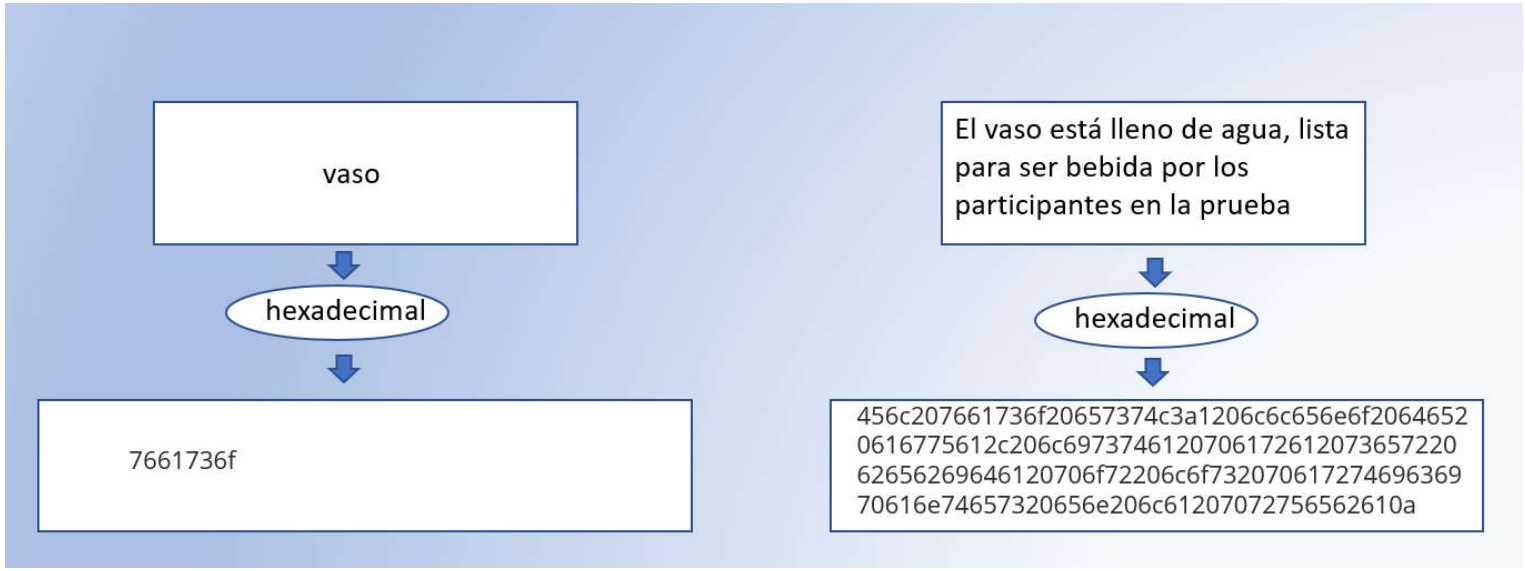
Ejemplo: Cálculo hash



Cifrado y hash

Funciones hash. SHA-256.

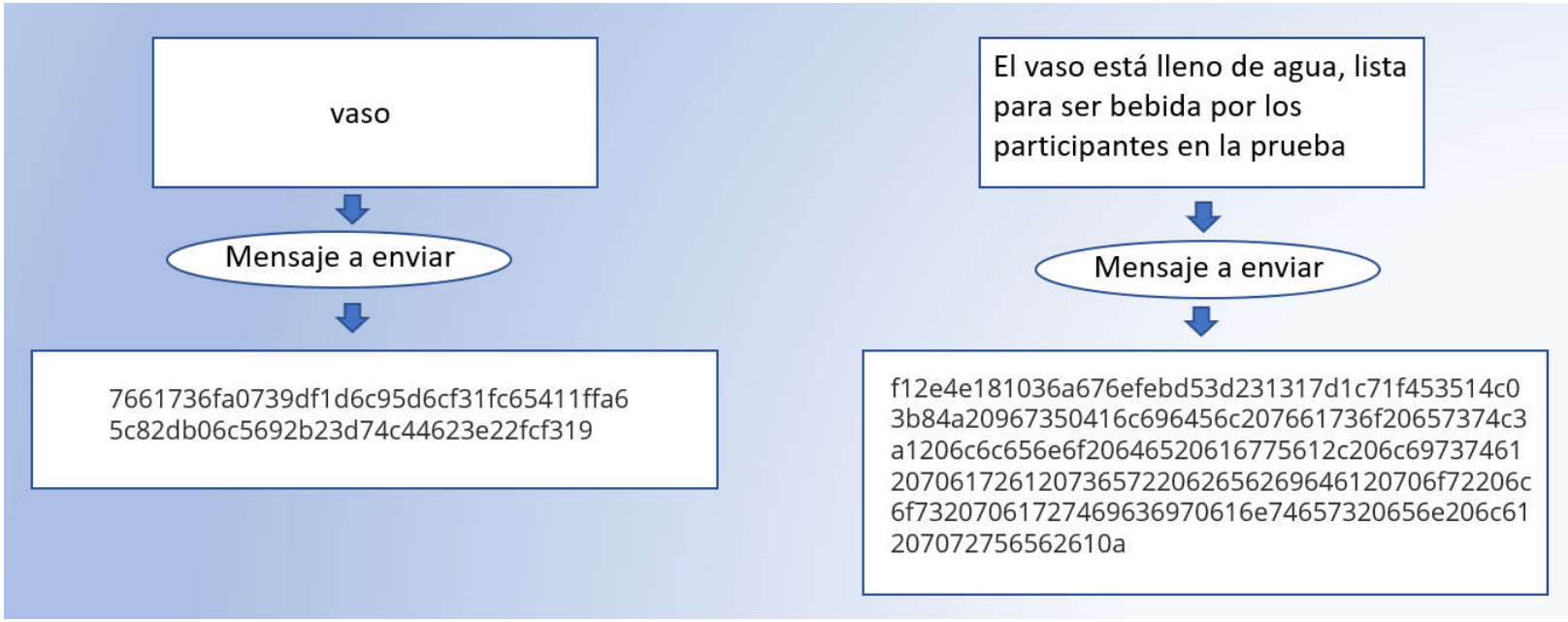
Ejemplo: Mensaje útil en hexadecimal



Cifrado y hash

Funciones hash. SHA-256.

Ejemplo: Mensaje completo a enviar



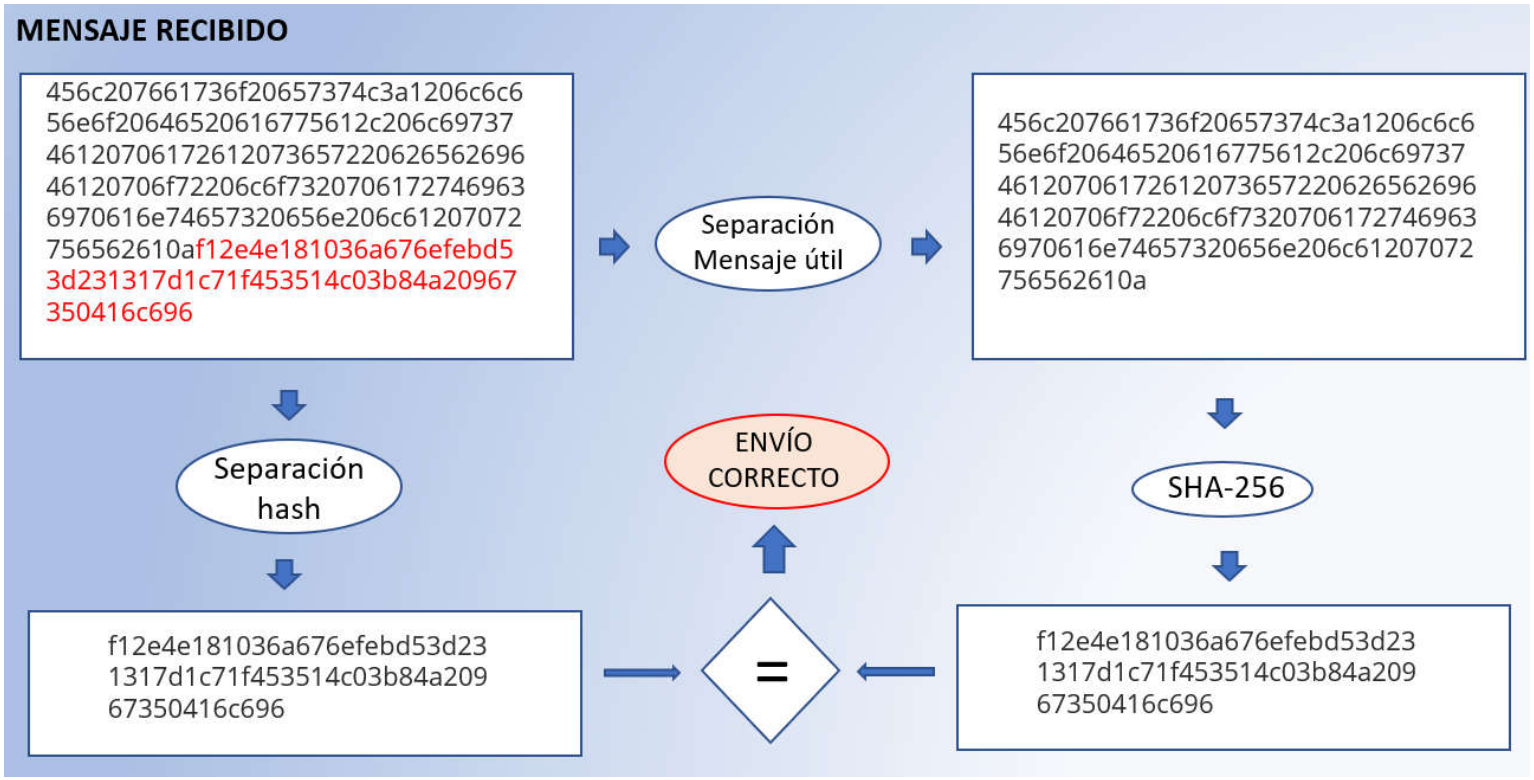
Cada carácter alfanumérico son dos valores hexadecimales.

Hash formado por 64 valores.

Cifrado y hash

Funciones hash. SHA-256.

Ejemplo: Recepción



Cifrado y hash

Funciones hash. SHA-256.

Colisiones:

Existir mensajes que den lugar al mismo hash.

Mayor robustez del algoritmo más se evitan las colisiones.

Algoritmos más utilizados:

· MD6: Message Digest Algorithm. Función hash de 256 bits de procesamiento paralelo, resumir rápidamente entradas muy largas.

Sencillez de implementación y velocidad de ejecución.

· SHA: Secure Hash Algorithm. Familia de algoritmos (SHA-1, SHA-2, SHA-3)

SHA-256 (SHA-2) muy utilizado últimamente. IBM Food Trust.

SHA-3, aporta mayor seguridad pero muy costoso computacionalmente.

Cifrado y hash

Funciones hash. SHA-256.

SHA-256. (familia SHA-2)

Muy popular.

Pasos en su ejecución:

1.- Preprocesado (formar bloque de 512 bits)

2.- Inicialización valores hash

3.- Inicialización constantes k

4.- Descomposición en bloques y envío a ejecución iterativa.

5.- Definición array auxiliar w

6.- Compresión

7.- Modificación final de valores

8.- Concatenación del hash generado

(ejercicio propuesto)

Cifrado y hash

Generadores de claves.

Recordemos:

- Clave pública, compartida sin riesgo para el funcionamiento del sistema.
- Clave privada, no distribuida y sólo pertenece a su propietario.

- Desencriptar con clave pública → autenticidad.
- Encriptar con clave pública → confidencialidad.

(Encriptando con clave pública solamente se puede desencriptar con la privada)

Cifrado y hash

Generadores de claves.

Complejidad de la generación de claves →

→ herramientas que facilitan el uso de sistemas generadores de claves.

- Mecanismos para la implementación de generadores de claves:

  I.- Incorporación de un motor generador de claves.

  II.- Utilización de herramientas externas generadoras de claves.

  III.- Incorporación de mecanismos o sistemas hardware especializados en encriptación.

Cifrado y hash

Generadores de claves.

I.- Incorporación de un motor generador de claves

Desarrollo de un sistema privado de criptografía asimétrica.

Incorporación a nuestro desarrollo: Descarga, adaptación, compilación y ejecución. (numerosas fuentes de código; ej. Github)

A partir de datos propios generar clave privada y claves públicas.

Cifrado y hash

Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

Necesario la seguridad en las comunicaciones:

Uso SSH (Secure Shell protocol), OpenPGP, GPG, etc.

Sistemas que permiten trabajar de manera segura a través de redes no seguras.

Herramienta SSH-Keygen. Comando que genera parejas de claves.

Cifrado y hash

Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

SSH.

Utilización del comando ssh-keygen.

Ejemplo: ssh-keygen -t ecdsa -b 2048 -f clave
(genera una clave de 2048 bits para el algoritmo ECDSA en el fichero ‘clave’)

La ejecución de este comando crea el fichero ‘clave’ cuyo contenido es:

```
-----BEGIN PUBLIC KEY-----
  MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0TqlveKKlc2MFvEmuXJi
  LGBsY1t4ML4uiRADGSZlnc+7Ugv3h+MCjkkwOKiOdsNo8k4KSBIG5GcQfKYOOd17
  AJvqCL6cGQbaLuqv0a64jeDm8oO8/xN/IM0oKw7rMr/2oAJOgIsfeXPkRxWWic9A
  VIS++H5Qi2r7bUFX+cqFsyUCAwEAAQ==
-----END PUBLIC KEY-----
```

Cifrado y hash

Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

Webs generadoras de claves. (travistidwell)

Uso de webs para generar claves. Encriptar y desencriptar mensajes.

Ejemplo:

Cifrado y hash

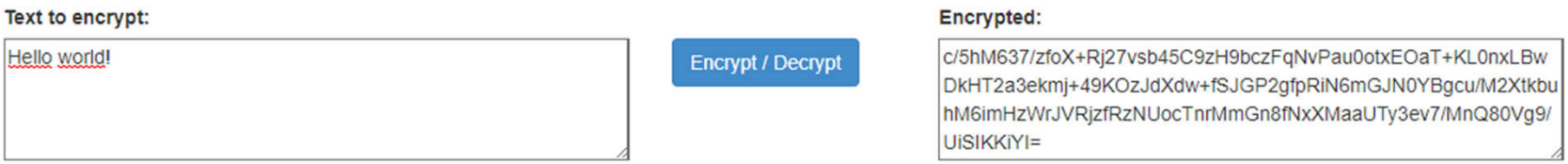
Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

Webs generadoras de claves. (travistidwell)

Ejemplo: Encriptar mensaje haciendo uso de las claves generadas.

Usarlo también para desencriptar el mensaje.



Cifrado y hash

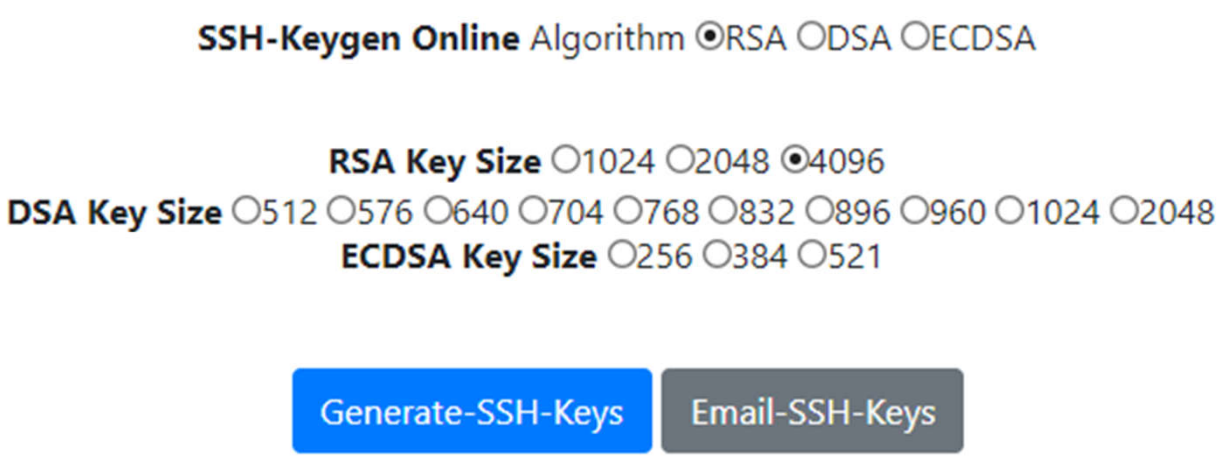
Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

Webs generadoras de claves. SSH online.

Ejemplo:

https://8gwifi.org/sshfunctions.jsp.



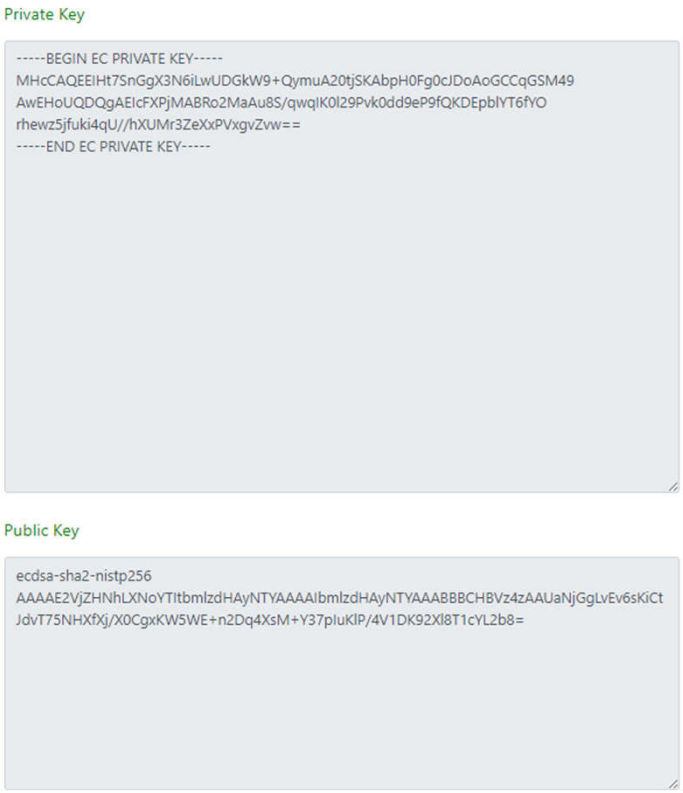
Cifrado y hash

Generadores de claves.

II.- Utilización de herramientas externas generadoras de claves

Webs generadoras de claves.
SSH online.

Ejemplo: Claves pública y privada generadas.



Cifrado y hash

Generadores de claves.

III.- Incorporación de mecanismos o sistemas hardware especializados en encriptación

Coprocesadores hardware especializados en criptografía.

Especial interés en sistemas empotrados y sistemas privados.

ATECC508. Ejemplo de chip coprocesador que implementa algoritmos de encriptación y dispone de una librería con funciones para encriptar y desencriptar.

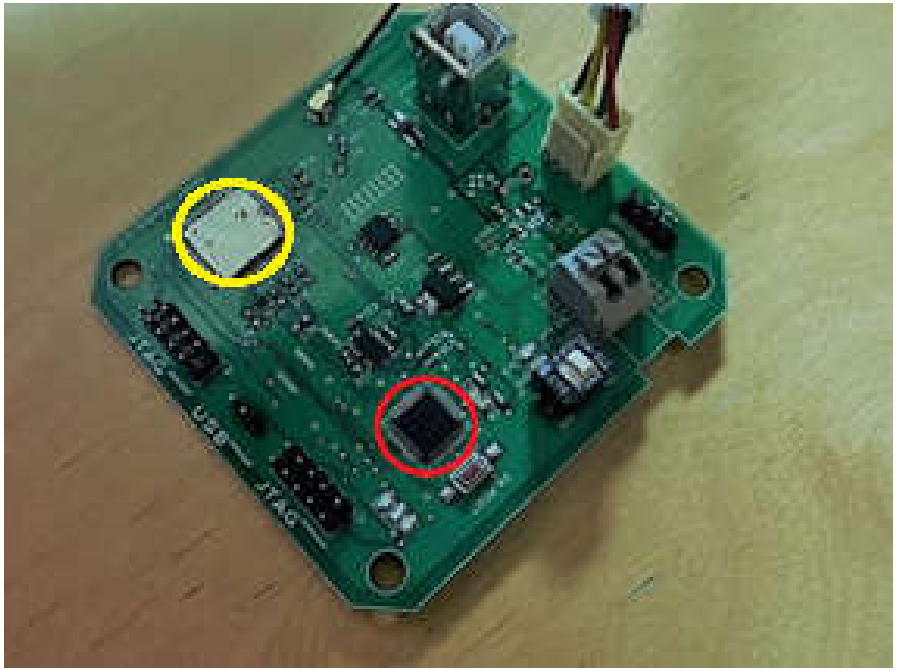
Cifrado y hash

Generadores de claves.

III.- Incorporación de mecanismos o sistemas hardware especializados en encriptación

Inserción de ATECC508 en una PCB.

Uso de librerías y Funciones específicas.



Cifrado y hash

Firma electrónica

Mecanismo de autentificación.

No incluye identificación de agentes.

Permite la verificación de mensajes.

Toda firma digital debe de ser:

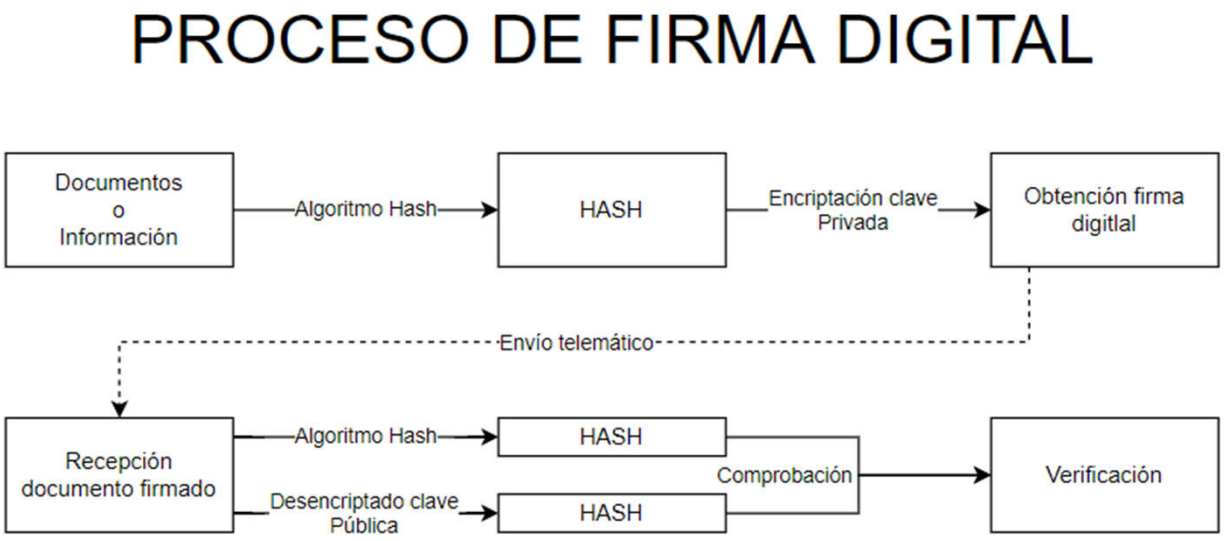
- Única.
- Verificable.
- Infalsificable.
- Viable.
- Innegable.

Cifrado y hash

Firma electrónica

Basadas en la criptografía asimétrica.

Claves pública y privada para encriptar y desencriptar la información.



Cifrado y hash

Firma electrónica

Ventajas:

- Seguridad en la información.
- Gestión de tiempo.
- Simplificación de procesos.
- Erradicación de fraudes

Aplicaciones:

- Facturas.
- Contrataciones.
- Voto electrónico.
- Mensajes con autenticidad.
- Dinero electrónico.
- Transacciones comerciales.

Cifrado y hash

Certificado digital

La asociación entre un usuario o entidad y su clave queda registrada en un certificado digital.

Autentificación digital de usuarios y dispositivos.

Cada usuario posee una clave pública que lo puede identificar.

Este certificado digital permitirá la firma de documentos.

Cifrado y hash

Certificado digital

Infraestructuras de clave pública (PKI) para asegurar su correcto funcionamiento.

PKI formadas por:

- Certificados digitales

  Elemento principal. Documento electrónico identificativo.

- Autoridad certificadora (CA)

  Autentifica la identidad de los usuarios.

  Previenen la entrada de entidades falsas. Proporcionan las claves públicas.

- Autoridad de registro (RA)

  Otorgan los certificados digitales a los usuarios. Permiso de las CA.

Cifrado y hash

Certificado digital

La infraestructura de clave pública (PKI) permite:

Identificación de usuarios en la red.

Cifrado y descifrado de mensajes.

Firma de nueva información.

Sistemas seguros de transferencia.

Cifrado y hash

Certificado digital

Tipos de certificados digitales:

- Certificado personal.
- Certificado de representante.
- Certificado de pertenencia a empresa.
- Certificado de persona jurídica.
- Certificado de atributo.

Cifrado y hash

Certificado digital

Tipos de Infraestructuras de Clave Pública:

- Infraestructuras de Clave Pública simple (SPKI)
  - Asocia cada usuario a una clave pública. Sistema centralizado
- Infraestructura de Clave Pública descentralizada – DPKI
  - Elimina las dependencias de un sistema centralizado.
  - El sistema funcionará aunque una parte se haya caído.
- Infraestructura de Clave Pública basada en Blockchain
  - Hace uso de una cadena de bloques.
  - Proporciona una seguridad muy elevada.

Cifrado y hash

¿El futuro de la criptografía?

Computadores clásicos o digitales:

Unidad mínima de información el bit (0, 1).

Unión de bits → posibilidad de codificación (8 bits = byte). ASCII

Más reducción en tamaños de integración → algunos conflictos.

Transistor. Componente básico chips computadora digital, y necesita espacio.

Cifrado y hash

¿El futuro de la criptografía?

Computación distinta a la tradicional:

Basada en aprovechar la superposición y entrelazamiento cuánticos.

Conseguir más estados por unidad de información y operaciones más eficientes.

Qubit. Unidad básica de información en la computación cuántica.

En superposición coherente el qubit puede ser 0, 1 o ambos a la vez.

Ej.: 8 qubits, 256 operaciones simultáneamente.

Cifrado y hash

¿El futuro de la criptografía?

Nuevos campos de trabajo:

Soportes físicos. Arquitecturas. Comunicaciones. Algoritmia (también en criptografía)

Previsión medio plazo:

Existencia de sistemas cuánticos que operen en red con acceso a recursos que utilizamos habitualmente.

Traspaso de servicios en red a sistemas cuánticos.

Cualidades fundamentales para entender computación cuántica:

- Superposición cuántica.
- Entrelazamiento cuántico.

Cifrado y hash

¿El futuro de la criptografía?

Superposición cuántica:

qubit, en dos estados posibles al mismo tiempo, asimilados 0 y 1.

2 qubits, en 4 estados posibles: 00, 01, 10 y 11.

3 qubits, 8 estados posibles: 000, 001, 010, 011, 100, 101, 110 y 111.

Estados que podrían ser procesados de forma simultánea.

Comparando:

Computador clásico computamos n bits en un determinado momento.

Computador cuántico computamos 2^n bits simultáneamente.

Los algoritmos cuánticos que operan sobre estados de superposición procesan simultáneamente todas las posibles combinaciones qubits.

Cifrado y hash

¿El futuro de la criptografía?

Entrelazamiento cuántico:

Entrelazamiento de las partículas → sincronizar la vibración a nivel subatómico de algunas características de las partículas que se entrelazan.

Como puede ser el spin, ángulos de rotación, etc.

Objetivo: Asociar o relacionar múltiples qubits mediante el entrelazamiento de dicha característica.

Qubits entrelazados no pueden descomponerse en factores independientes para cada uno de los qubits.

Mantienen el mismo valor independientemente del lugar donde se encuentren.

Cifrado y hash

¿El futuro de la criptografía?

Entrelazamiento cuántico:

Característica especialmente interesante en sistemas criptográficos.

Junto a principio de incertidumbre → no se puede interferir o medir valores entre pares de variables físicas entrelazadas sin alterarlos.

Si se intenta conocer el valor de qubits entrelazados, dicho valor será alterado y no será posible determinarlo con exactitud.

Cifrado y hash

¿El futuro de la criptografía?

Entrelazamiento cuántico:

Aplicado a claves criptográficas compartidas entre emisor y receptor supone que dichas claves no puedan ser detectadas ya que interferencias para su detección las alteran automáticamente.

Uso de la teleportación cuántica en la distribución y asignación de claves criptográficas.

(Estudios sobre el posible hackeo de este tipo de claves)

Cifrado y hash

¿El futuro de la criptografía?

Eficiencia de la computación cuántica:

Avances desarrollo tecnológico: circuitos, almacenamiento, algoritmos.

Ventaja computacional cuadrática: problemas numéricos iterativos.

1.000.000 operaciones bits → 1.000 operaciones qubits

Ventaja computacional exponencial: algoritmos cuánticos nativos.

Computador cuántico de 30 qubits → equivalente a computador clásico 10 Teraflops

Cifrado y hash

¿El futuro de la criptografía?

Criptografía cuántica:

Es la criptografía basada en los principios de la mecánica cuántica para garantizar la autenticidad de los mensajes y la confidencialidad en la transmisión de información en un sistema criptográfico.

Para su estudio, dos puntos clave:

I.- Capacidad de cómputo

II.- Invulnerabilidad sistemas criptográficos cuánticos.

Cifrado y hash

¿El futuro de la criptografía?

I.- Capacidad de cómputo en sistemas cuánticos.

Antecedente: Sistemas criptográficos actuales basados en la dificultad de encontrar las claves por la complejidad y necesidades de computación.

Si la complejidad se reduce cuadrática o exponencialmente los sistemas se vuelven vulnerables.

Temor: Incorporación de computadores cuánticos a las redes (internet) que conviertan en vulnerables los sistemas de trabajo habitual.

Cifrado y hash

¿El futuro de la criptografía?

I.- Capacidad de cómputo en sistemas cuánticos.

Criptografía postcuántica (PQC). Surge en respuesta al problema anterior.

Son sistemas criptográficos resistentes a la computación cuántica

Sistemas actuales (simétricos y asimétricos) pueden ser superados por computadores cuánticos con determinados algoritmos (**Shor**).

Enfoques en la criptografía postcuántica:

- Funciones polinomiales multivariables.
- Criptografía de retículos.
- Criptografía basada en isogenia (heredera de ECC)

Cifrado y hash

¿El futuro de la criptografía?

II.- Invulnerabilidad sistemas criptográficos cuánticos.

Hay que tener en cuenta el principio de entrelazamiento cuántico.

Sistemas criptográficos cuánticos:

- Fotones entrelazados
- Principio de incertidumbre de Heisenberg

(cualquier medida realizada en un sistema cuántico provoca una perturbación en dicho sistema modificando el estado de la información y alertando de una intrusión)

Además del aviso deintrusion, no se tiene acceso a la información ya que ésta ha quedado perturbada, los valores modificados y cualquier medición será incompleta.

Cifrado y hash

¿El futuro de la criptografía?

II.- Invulnerabilidad sistemas criptográficos cuánticos.

Actualmente propuestas que trabajan con el envío de fotones polarizados entre emisor y receptor mediante fibra óptica y filtros sincronizados en los extremos.

Mecanismos de sincronización de filtros.

Interferencias en comunicación → Se altera la polarización y se detecta.

Trabajos actuales sobre interferir esta comunicación sin ser detectados.

Cifrado y hash