SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.1.3.MF0489_3. Capítulo 1
Parte 4
Criptografía

JOSÉ PABLO HERNÁNDEZ

10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

En el ámbito de la criptografía, se denominan funciones resumen a aquellos procedimientos que, dado un mensaje de un tamaño cualquiera, producen una salida de un tamaño fijo.

Como consecuencia de esta definición, el conjunto de mensajes de entrada es siempre mayor que el de las salidas.

Por ello, parece claro que más de un mensaje de entrada ofrecerá la misma salida. A esta situación se le denomina colisión.

10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

Las aplicaciones más extendidas de las funciones resumen son el control de integridad y la creación de firmas digitales.

10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

Funciones resumen criptográficamente robustas:

- **Resistencia a la primera pre-imagen.**
- **Resistencia a la segunda pre-imagen.**
- **Resistencia a colisiones.**

10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

Concepto efecto avalancha:

Un cambio en un bit de entrada produzca un cambio en la mitad de los bits de la salida.

Con ello, la salida de la función resumen se comporta de una manera aleatoria, lo que dificulta la búsqueda de colisiones.

10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

Las funciones resumen tienen las propiedades de:

- **Difusión.**
- **Determinismo.**
- **Eficiencia, rápidas tanto en hardware como en software.**

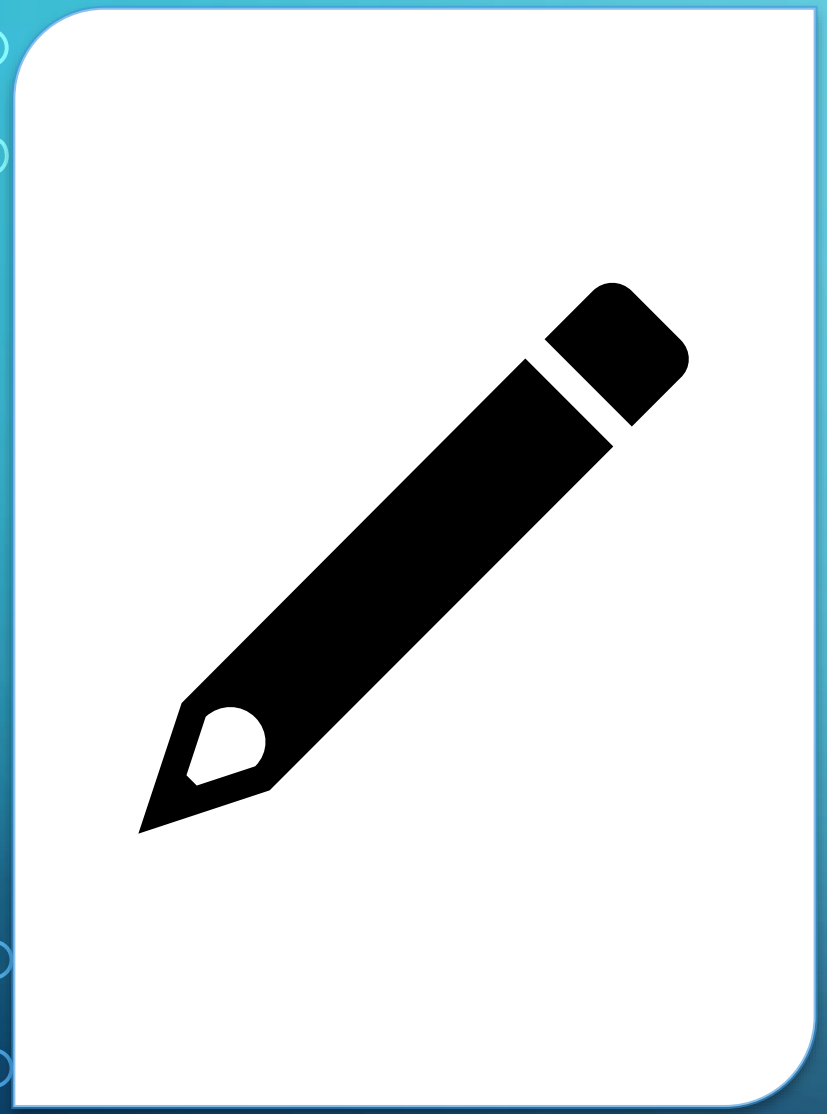
10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN

Merkle-Damgard: Utilizada para crear algunas de las funciones resumen más conocidas, como son MD5, SHA-1 o SHA-2.

Según esta estructura, el proceso de construcción consiste en ejecutar un algoritmo con iteraciones encadenadas:

- **El mensaje M se divide en bloques, B, de una determinada longitud. El último bloque se rellena con los bits adecuados para completar la longitud de un bloque.**
- **Se aplica una función de compresión a la salida de una iteración anterior (vector de inicialización en el primer bloque) y a un nuevo bloque.**

Si la función de compresión es resistente a colisiones, la función resumen resultante también lo es.



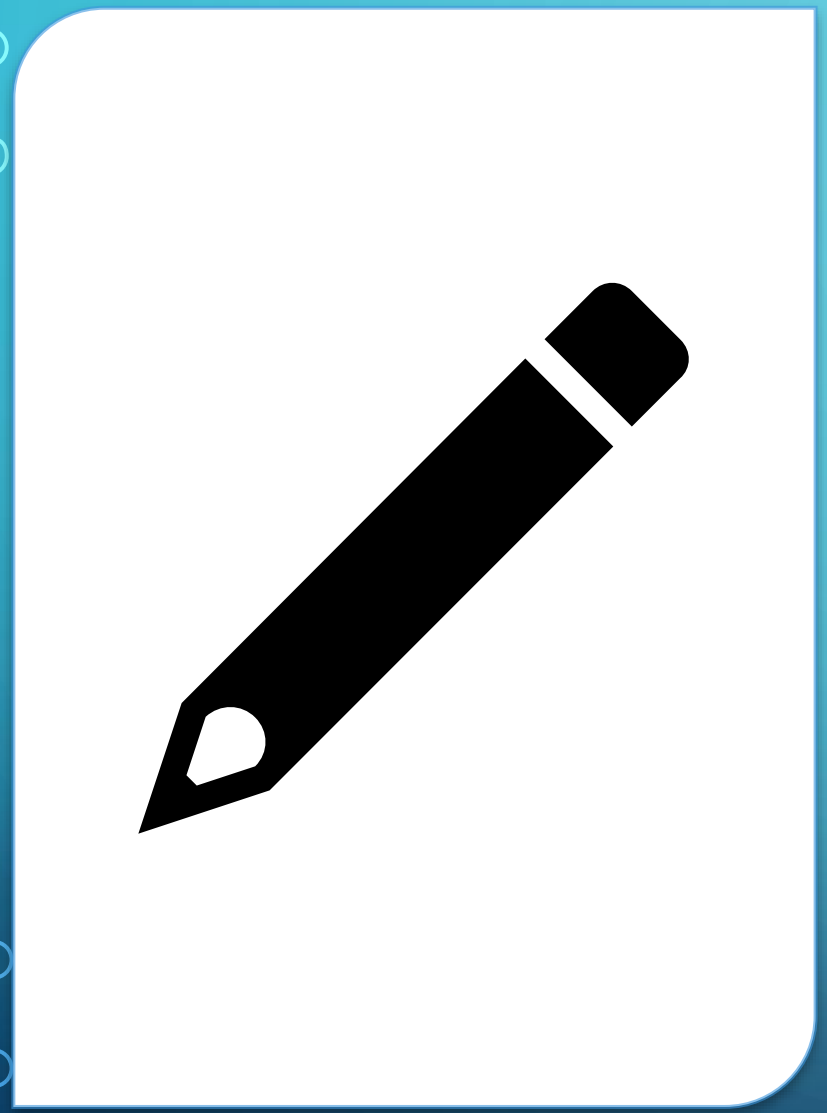
Ejemplo.

SE CONVIERTE EN UN ANALISTA DE SEGURIDAD DE UN BANCO. LE PIDEN QUE IDENTIFIQUE LA FUNCIÓN RESUMEN MÁS ADECUADA PARA COMPROBAR QUE LAS CUENTAS NO HAN CAMBIADO DESDE EL CIERRE DE LA OFICINA HASTA LA APERTURA EL DÍA SIGUIENTE. SE LE PROPONEN TRES FUNCIONES:

A. FUNCIÓN PRINUM, QUE DADO UN NÚMERO PRODUCE COMO SALIDA EL PRIMER DÍGITO DEL MISMO.

B. FUNCIÓN SUNUM, QUE DADO UN NÚMERO PRODUCE COMO SALIDA LA SUMA DE SUS DÍGITOS.

¿CUMPLEN ESTAS FUNCIONES LAS PROPIEDADES DE UNA FUNCIÓN RESUMEN CRIPTOGRÁFICAMENTE SEGURA? SI NO, ¿PUEDE CONSTRUIR UNA QUE SÍ LO SEA EMPLEANDO LAS DESCRITAS?



Ejemplo. Solución.

LA FUNCIÓN PRINUM ES UNA FUNCIÓN RESUMEN, PUES CUMPLE LA CONDICIÓN DE QUE SU SALIDA SIEMPRE ES DEL MISMO TAMAÑO. NO OBSTANTE, NO SERÍA CRIPTOGRÁFICAMENTE SEGURA EN TANTO QUE SERÍA TRIVIAL ENCONTRAR DOS NÚMEROS (POR EJEMPLO, 1 Y 150) QUE OFRECIESEN EL MISMO RESULTADO (1 EN AMBOS CASOS). POR SU PARTE, LA FUNCIÓN SUNUM NO ES NI SIQUIERA UNA FUNCIÓN RESUMEN, PUES LA SALIDA TIENE UN TAMAÑO VARIABLE MEDIDA EN NÚMERO DE DÍGITOS. ASÍ, SI SE TOMA COMO ENTRADA EL NÚMERO 10, LA SALIDA SERÍA 1, PERO SI SE CONSIDERASE EL NÚMERO 449, LA SALIDA SERÍA 17.

SIN EMBARGO, SE PODRÍA CONSTRUIR UNA FUNCIÓN RAZONABLEMENTE ROBUSTA SI SE COMBINASEN AMBAS FUNCIONES. PARTICULARMENTE, SI LA SALIDA DE SUNUM FUESE LA ENTRADA DE PRINUM SE OBTENDRÍA UNA FUNCIÓN RESUMEN EN LA QUE ENCONTRAR COLISIONES SERÍA RAZONABLEMENTE MÁS COMPLEJO QUE EN EL CASO DE PRINUM. EN CUALQUIER CASO, DADA LA TECNOLOGÍA ACTUAL, ESTA FUNCIÓN NO SERÍA COMPUTACIONALMENTE ROBUSTA, POR LO QUE SE CONCLUYE QUE NO ES POSIBLE CONSTRUIR LA FUNCIÓN BUSCADA COMBINANDO LAS EXISTENTES.

10.1. FUNCIONES RESUMEN CON CLAVE

Existe una variante conocida como funciones resumen con clave, comúnmente conocidas como HMAC.

La salida se calcula en función del mensaje de entrada y de la clave introducida.

11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003

La Ley 59/2003, de 19 de diciembre, dota de marco legal a la utilización de la firma electrónica.

La firma electrónica, de acuerdo a la definición prevista en la Ley, es "el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".

Así, la firma electrónica es un mecanismo que permite la autenticación del emisor.

11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003

La Ley introduce el concepto de **certificado reconocido** como aquel expedido por un prestador de servicios de certificación que cumpla una serie de condiciones.

Con respecto al uso del Documento Nacional de Identidad electrónico (DNIe), el texto establece que es el documento que acredita la identidad del titular y que permite la firma de documentos.

11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003

El dispositivo de creación se define como el programa o sistema que se utiliza para aplicar los datos de creación de firma.

Para considerarse seguro, se imponen cinco condiciones:

- Que los datos necesarios para firmar pueden generarse solo una vez y que, además, se mantienen en secreto con una protección razonable.
- Que se proporciona una seguridad razonable tal que no es posible derivar los datos de creación de firma a partir de la propia firma o de los datos de verificación.
- Que la firma esté protegida frente a falsificaciones, atendiendo a la tecnología disponible.
- Que el firmante pueda prevenir adecuadamente el uso de los datos de creación de firma por parte de terceros.
- Que no se altere la información que va a ser firmada y que esta se presente al firmante con anterioridad a la operación.

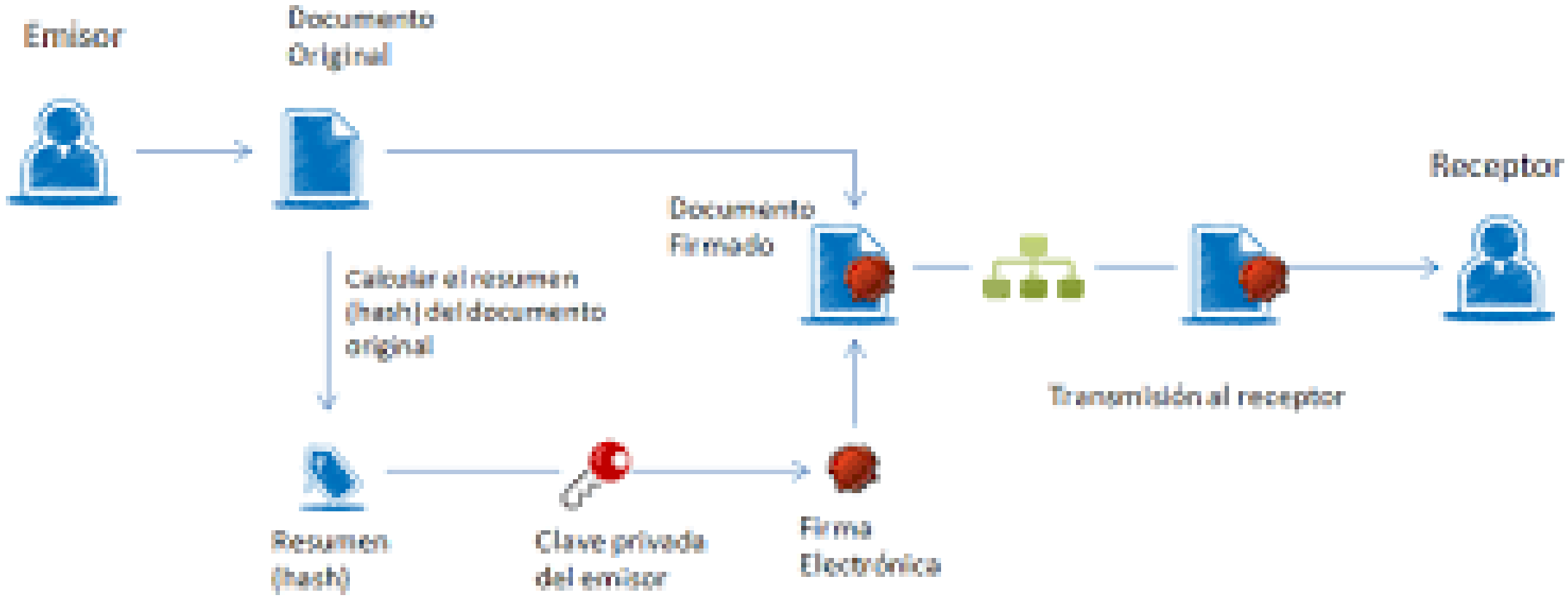
11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003

En lo referente a los **dispositivos de verificación**, estos deben asegurar que el proceso, además de realizar la verificación (y mostrar el resultado) de forma fiable, cumple los siguientes aspectos:

- Que los datos utilizados para verificar la firma sean los mostrados a la persona que efectúa la verificación.
- Que la persona que verifica la firma pueda establecer si los datos han sido modificados.
- Que se muestren los datos de identidad del firmante y que se verifique su certificado electrónico.
- Que pueda detectarse cualquier cambio que afecte a la seguridad del proceso.

12. ELEMENTOS FUNDAMENTALES DE LA FIRMA DIGITAL

12.1. ELEMENTOS FUNDAMENTALES. ESQUEMA BÁSICO



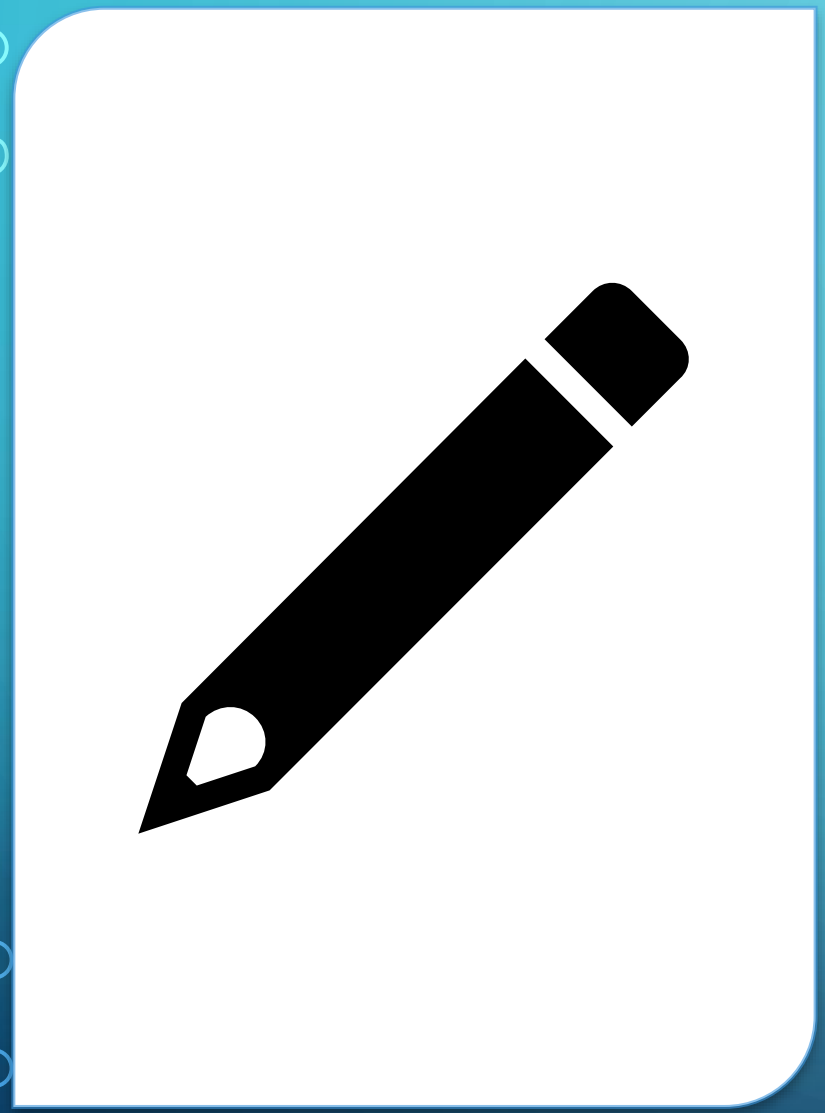
12.2. TIPOS DE FIRMA Y CRITERIOS DE USO

La Ley define tres tipos de firmas, que se construyen de manera incremental:

- Firma electrónica
- Firma electrónica avanzada
- Firma electrónica reconocida

Ejemplo.

UN CIUDADANO ESPAÑOL REALIZA UNA APUESTA A TRAVÉS DE INTERNET, CON LA MALA FORTUNA DE QUE LA PIERDE. DECIDE RECURRIR A LA JUSTICIA, ALEGANDO QUE LA FIRMA CON LA QUE SUPUESTAMENTE AUTORIZÓ LA APUESTA NO ERA VÁLIDA. DICHA FIRMA SE REALIZÓ UTILIZANDO SU CERTIFICADO X.509 EXPEDIDO POR LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE, QUE ERA VÁLIDO CUANDO LA FIRMA SE LLEVÓ A CABO. ¿CUÁLES DE LOS ELEMENTOS QUE INTERVIENEN EN LA FIRMA PODRÍAN SER PUESTOS EN DUDA POR EL CIUDADANO PARA DEMOSTRAR SU FALSEDAD?



Ejemplo. Solución.

PARA RESPONDER A LA PREGUNTA, ES NECESARIO REVISAR LOS ELEMENTOS QUE INTERVIENEN EN LA FIRMA:

EL ALGORITMO DE FIRMA: DADO QUE NO SE ESPECIFICA NADA AL RESPECTO, ES DE SUPONER QUE EL ALGORITMO UTILIZADO ES UNO DE LOS COMÚNMENTE UTILIZADOS Y CUYA ROBUSTEZ HA SIDO YA DEMOSTRADA. NO ES UN ELEMENTO QUE PUEDA SUSCITAR CONTROVERSIA.

EL MATERIAL CRIPTOGRÁFICO DEL FIRMANTE: LA FIRMA ESTÁ AVALADA POR UN CERTIFICADO VÁLIDO Y EMITIDO POR UNA AUTORIDAD CONFIABLE. NO PARECE SER UN ELEMENTO CONTROVERTIDO.

EL SISTEMA SOBRE EL QUE SE REALIZA LA FIRMA: EN ESTE CASO, LA FIRMA SE REALIZA EN UN ORDENADOR CONVENCIONAL. ESTO NO RESPONDE A UN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA, POR LO QUE EL CIUDADANO PODRÍA INTENTAR DEMOSTRAR QUE EL ORDENADOR ESTABA COMPROMETIDO Y QUE, POR EJEMPLO, PROCESÓ LA FIRMA SOBRE UN MENSAJE DISTINTO A AQUEL QUE ÉL ESTABA DISPUESTO A FIRMAR.

ADEMÁS DE LO ANTERIOR, PARA UTILIZAR LA CLAVE PRIVADA HABITUALMENTE SE NECESITA UNA CONTRASEÑA. ESTO HACE AÚN MÁS DIFÍCIL PONER EN DUDA QUE EL AFECTADO REALIZASE LA FIRMA.

13. CRITERIOS PARA LA UTILIZACIÓN DE TÉCNICAS DE CIFRADO DE FLUJO Y DE BLOQUE

Los cifradores de flujo son adecuados cuando los datos que van a cifrarse son continuos y no se conoce su tamaño, como por ejemplo, en el flujo de una red.

Los cifradores de bloque son apropiados cuando la cantidad de datos a cifrar se conocen previamente, como por ejemplo en un fichero, siendo posible determinar la cantidad de bloques a procesar.

14. PROTOCOLOS DE INTERCAMBIO DE CLAVES

Los protocolos de intercambio de claves requieren, con frecuencia, el uso de claves maestras, utilizadas y válidas por un largo periodo de tiempo, y de claves de sesión, empleadas temporalmente entre dos entidades.

Estos tipos de protocolos se pueden clasificar según el tipo de claves intercambiadas, secretas o públicas. Asimismo, los intercambios de claves privadas se pueden realizar mediante criptografía simétrica o asimétrica.

14.1. INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOGRAFÍA SIMÉTRICA

Dadas dos entidades, A y B, la distribución de una clave se podría realizar de los siguientes modos:

- A genera la clave y se la entrega físicamente a B.
- Una tercera parte puede elegir la clave y entregarla físicamente a A y B.
- Si A y B se han comunicado previamente, pueden utilizar la clave anterior para cifrar la actual.
- Si A y B tienen un enlace seguro con una tercera parte C, C puede generar y reenviar la clave a A y B.

14.1. INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOGRAFÍA SIMÉTRICA

Controlando el uso de las claves

El concepto de jerarquía de claves, junto con los procesos automáticos de distribución, simplifica la gestión de dichas claves.

Vectores de control: conjunto de campos que especifican el uso y las restricciones de la clave.

14.2. INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOGRAFÍA ASIMÉTRICA

Dadas dos entidades, A y B, que desean establecer una clave secreta común, uno de los protocolos más simples consiste en los siguientes pasos.

1. A genera un par de claves público-privada y transmite a B su clave pública y su identificador.
2. B genera una clave secreta (K_s), la cifra con la clave pública de A y se la envía.
3. A utiliza su clave privada para descifrar el mensaje recibido y obtener la clave secreta enviada por B, es decir, K_s.

14.2. INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOGRAFÍA ASIMÉTRICA

1.A envía a B los datos $N_1 + ID_A$, cifrados con la clave pública de B, a modo de identificación de la transacción.
2.B obtiene esos datos y envía $N_2 + N_1$ a A, cifrado con su clave pública. Puesto que sólo B podría haber descifrado el mensaje enviado en 1, la presencia de N_1 en este mensaje asegura a A que la entidad con la que se está comunicando es B.
3.A obtiene $N_2 + N_1$ y envía a B N_2 (con lo que demuestra a B que es realmente A) y una clave de sesión (K_s) firmada.
4.B obtiene K_s. La firma garantiza que sólo A ha podido mandarlo y, al cifrarlo con la clave pública de B, se asegura de que sólo B puede recibirlo.

14.3. INTERCAMBIO DE CLAVES SECRETAS MEDIANTE CRIPTOSISTEMAS HÍBRIDOS

Un posible esquema se describe a continuación:

El Centro de Distribución de Claves (CDC) distribuye claves maestras a cada usuario aplicando criptografía de clave pública y, posteriormente, distribuye claves de sesión cifrándolas con la maestra, es decir, aplicando criptografía de clave secreta.

De este modo, se consigue una distribución eficiente de las claves de sesión, siendo posible que un único CDC pueda distribuir las claves entre un gran conjunto de usuarios.

14.4. INTERCAMBIO DE CLAVES PÚBLICAS

Anuncio público

Dado que en la criptografía de clave pública todas las entidades disponibles de una clase que las demás pueden conocer, cualquier entidad puede mandar su clave pública a otra entidad o difundirla a un conjunto de entidades.

14.4. INTERCAMBIO DE CLAVES PÚBLICAS

Directorio público

Es posible aumentar la seguridad haciendo uso de un directorio público en el que se encontrasen todas las claves públicas de las entidades participantes en intercambios de mensajes. Para ello, una autoridad será la encargada de mantener el repositorio.

14.4. INTERCAMBIO DE CLAVES PÚBLICAS

Autoridad de clave pública

A envía un mensaje a la autoridad para conseguir la clave pública de B, incluyendo en dicho mensaje una marca de tiempo (T1).

La autoridad envía la clave de B firmada, y devuelve firmada tanto la solicitud como la marca de tiempo recibida. Posteriormente, A verifica la firma. Posteriormente A envía a B un nonce y su identificador cifrado con la clave pública de dicha entidad.

Los pasos 1-2 son repetidos por B para conseguir la clave pública de A.

B obtiene el nonce enviado por A. Después, B crea otro nonce, lo concatena con el recibido por A, lo cifra con la clave pública de A y se lo envía a dicha entidad.

A obtiene el nonce creado por B y se lo devuelve cifrado con su clave pública.

14.4. INTERCAMBIO DE CLAVES PÚBLICAS

Certificados de clave pública

Como mejora del protocolo anterior se propone la utilización de certificados que permitan a los participantes intercambiar sus claves sin la necesidad de participación de ninguna autoridad.

Un certificado, como ya se ha comentado anteriormente, es un documento que vincula a una entidad con un par de claves (en el certificado sólo se almacena la pública).

Por tanto, dado que las claves están vinculadas a un único usuario, este puede publicar su certificado sin miedo a ser suplantado.

Ejemplo.

UN PROFESOR DESEA MANDAR A SUS ALUMNOS, UN TOTAL DE 300, LA CORRECCIÓN DEL EXAMEN DE BIOMEDICINA POR CORREO ELECTRÓNICO. QUIERE GARANTIZAR LA CONFIDENCIALIDAD Y AUTENTICIDAD DE LA INFORMACIÓN. SUPONIENDO QUE TANTO EL PROFESOR COMO LOS ALUMNOS DISPONEN DE CERTIFICADOS X.509, INDIQUE QUÉ TIPO DE CRIPTOGRAFÍA HA DE UTILIZARSE Y CUÁLES SON LOS PASOS QUE HA DE REALIZAR EL PROFESOR PARA ENVIAR LOS EXÁMENES A CADA UNO DE LOS ALUMNOS.

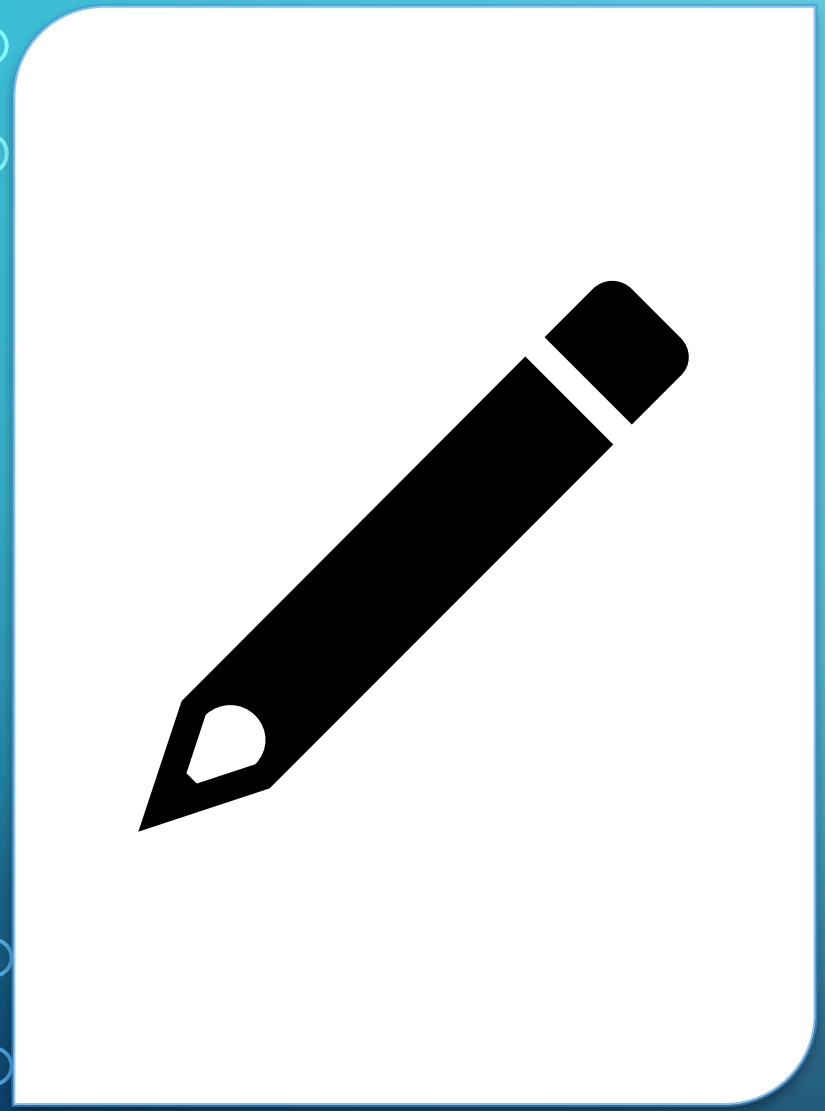
Ejemplo. Solución.

DADO EL ALTO NÚMERO DE ALUMNOS Y LA EXISTENCIA DE CERTIFICADOS, LO MÁS ADECUADO ES HACER USO DE UN CIFRADO ASIMÉTRICO.

LOS PASOS A REALIZAR POR EL PROFESOR SON LOS SIGUIENTES:

OBTENER LAS CLAVES PÚBLICAS DE TODOS LOS ALUMNOS, BIEN PORQUE ESTOS SE LAS ENTREGUEN O PORQUE ESTÉN EN ALGÚN REPOSITORIO AL QUE EL PROFESOR TIENE ACCESO.
PARA CADA EXAMEN DE UN ALUMNO X, EL PROFESOR ESCOGERÁ EL CERTIFICADO DEL ALUMNO X Y HACIENDO USO DE LA CLAVE PÚBLICA INCLUIDA EN EL MISMO, CIFRARÁ EL EXAMEN. DE ESTE MODO, SE GARANTIZA LA CONFIDENCIALIDAD.
ADEMÁS, PARA QUE EL ALUMNO TENGA CERTEZA DE QUE EL EXAMEN PROVIENE DEL PROFESOR Y GARANTIZAR LA AUTENTICIDAD DEL MISMO, ESTE LO FIRMARÁ (ANTES O DESPUÉS DE CIFRARLO, ESO DEPENDE DE SU ELECCIÓN). PARA REALIZAR LA FIRMA, EL PROFESOR LO CIFRA CON SU CLAVE PRIVADA. NÓTESE QUE, COMO NO SE HA DE SATISFACER LA PROPIEDAD DE INTEGRIDAD, LA APLICACIÓN DE UNA FUNCIÓN RESUMEN EN LA FIRMA NO ES NECESARIA (AUNQUE LO HABITUAL SEA APLICAR LA FIRMA SOBRE EL RESULTADO DE APLICAR UNA FUNCIÓN RESUMEN SOBRE EL MENSAJE A ENVIAR).
FINALMENTE, EL PROFESOR ENVÍA EL EXAMEN CIFRADO Y FIRMADO AL ALUMNO, ADJUNTANDO SU CERTIFICADO (O LO DEJA A DISPOSICIÓN DE LOS ALUMNOS).

Ejercicios



4.1.100.1.MF0489_3_EJERCICIOSCAPITULO_1.DOCX