DESDE 2023
https://revista.ccaitese.com

RICT Revista de Investigación Científica, Tecnológica e Innovación

ISSN: 2992-7315

Publicación Semestral RICT Vol. 2 No. 3 (2024) Páginas 6 – 11

Protocolo criptográfico de firma digital para el signado de documentos digitales con criptografía asimétrica para el intercambio seguro de información en la empresa CDS, S.C.

Cryptographic digital signature protocol for signing digital documents with asymmetric cryptography for the secure exchange of information in the company CDS, S.C.

Abraham-Jorge Jiménez-Alfaro [a], Edgar Corona-Organiche [a], Griselda Cortés-Barrera [a], Irving-Cardiel Alcocer-Guillermo [b]

[a]Ingeniería en Sistemas Computacionales, TECNM/Tecnológico de Estudios Superiores de Ecatepec, Valle de Anáhuac, 55210 Ecatepec de Morelos, Estado de México.
[b]Ingeniería en Tecnologías de Información y Comunicaciones , TECNM/Instituto Tecnológico Gustavo A. Madero, Calle 608 No. 300 y Av. 412, Col. San Juan de Aragón, 07470 Alcaldía. Gustavo A. Madero, Ciudad de México.

Resumen

La firma digital corresponde a la versión computarizada de la firma personal manuscrita o firma ológrafa. Estas se utilizan ampliamente como prueba de autoría o acuerdo de una parte, entre otros usos, siempre en referencia a un documento. Sin embargo para la empresa CDS, S.C., pueden resultar inseguras en tanto que pueden ser, con relativa facilidad, aplicadas de manera deshonesta. Por ejemplo, pueden ser tomadas desde una pieza de papel para pasarlas a otra, o los documentos podrían ser modificados luego de la aplicación de la firma. La firma digital y los protocolos criptográficos como metodología proporcionan tecnología que apoya para resolver estos problemas en documentos digitales. El artículo presenta la arquitectura de un protocolo criptográfico de firma digital para signar documentos en la empresa CDS, S.C., así como, los aplicativos de encriptado y desencriptado que tendrán los mandos de alta dirección y medios de la organización para garantizar la prueba de autoría de un documento digital.

Palabras clave: Firma Digital, Cifrado Clave Publica, Protocolo de Firma Digital

Abstract

The digital signature corresponds to the computerized version of the personal handwritten signature or holographic signature. These are widely used as proof of authorship or agreement of a party, among other uses, always in reference to a document. However, for the company CDS, S.C., they can be unsafe since they can be, with relative ease, applied dishonestly. For example, they can be taken from one piece of paper to another, or documents could be modified after the signature has been applied. Digital signature and cryptographic protocols as a methodology provide technology that supports solving these problems in digital documents. The article presents the architecture of a cryptographic digital signature protocol to sign documents in the company CDS, S.C., as well as the encryption and decryption applications that the organization's senior management and media will have to guarantee proof of authorship. of a digital document.

Keywords: Digital Signature, Public Key Encryption, Digital Signature Protocol

1. Introducción

Los protocolos son una serie de pasos que envuelven a dos o más partes, diseñados para realizar una tarea. En particular, si usan un algoritmo criptográfico se denominan protocolos criptográficos (Stallings, 2017).

Para Stallings (2019) los algoritmos criptográficos por sí solos no cumplen con la función de resolver los problemas de seguridad; deben formar parte de un protocolo criptográfico.

Por otra parte, supone también que:

- Las partes involucradas deben conocer el protocolo.

*Autor para la correspondencia: ajimenez@tese.edu.mx
Correo electrónico: ajimenez@tese.edu.mx (Abraham-Jorge Jiménez-Alfaro), ecorona@tese.edu.mx (Edgar Corona-Organiche), gcortes@tese.edu.mx (Griselda Cortés-Barrera), irving.ag@gamadero.tecnm.mx (Irving-Cardiel Alcocer-Guillermo)

Historial del manuscrito: recibido el 25/01/2024, última versión-revisada recibida el 03/04/2024, aceptado el 04/04/2024, en línea (postprint) desde el 08/04/2024, publicado el 09/04/2024. **DOI:** https://doi.org/10.2992/rict.v2i3.43

- Las partes lo aceptan y concuerdan en aplicarlo.
- El protocolo no tiene ambigüedades.
- El protocolo es completo, para toda situación se contempla una acción determinada.

Para Craig (2003) Todas estas características son fundamentales para permitir que:

- Las comunicaciones entre computadoras sean seguras, al tener queseguir un protocolo formal para el intercambio de mensajes.

- Al especificar los pasos que se deben seguir, sea posible examinar en detalle si existen puntos débiles en cuanto a la seguridad; y por otro lado, evitar realizar acciones fuera del protocolo con intenciones delictivas.

Para Stallings (2019) los problemas de seguridad de las redes pueden dividirse de forma general en cuatro áreas interrelacionadas:

1.-**El secreto**, encargado de mantener la información fuera de las manos de usuarios no autorizados.

2.-**La validación de identificación**, encargada de determinar la identidad de la persona o computadora con la que se esta hablando.

3.-**El control de integridad**, encargado de asegurar que el mensaje recibido fue el enviado por la otra parte y no un mensaje manipulado por un tercero.

4.-**El no repudio**, encargado de asegurar la "firma" de los mensajes, de igual forma que se firma en papel una petición de compra/venta entre empresas.

Las firmas manuales en los documentos se usan desde tiempos inmemoriales como prueba de autoría, o al menos de consentimiento con el contenido del documento. Para Stallings (2019) existen algunas características que las hacen tan confiables:

- **La firma es inolvidable e irrepudiable**. El firmante no puede aducir que nosabe si es su firma, o negarla.
- **La firma es auténtica**. El que recibe el documento está convencido de que elfirmante deliberadamente firmó el documento.
- **La firma no es reusable**. Es parte del documento y no se puede mover o copiar a otro.
- **La firma es inalterable**.

Se asume que una firma realizada por otro medio distinto al manual, pero quecumpla con estas características, es confiable y puede ser aceptada por las partes. Es el caso de la firma efectuada en un medio digital.

2. Materiales y Método

2.1.- Criptografía y Criptoanálisis

El criptoanálisis (Maiorano, 2009) se encarga de descifrar los mensajes, la criptografía busca métodos más seguros de cifrado, la criptografía viene del griego KRYPTOS = oculto y GRAPHE = escrito. Para Stallings (2017) se clasifica en:

- Criptografía clásica. Algoritmo secreto. Cifrados por sustitución y transposición, entre otros.
- Criptografía moderna. Algoritmo público. Cifrados en base a claves que se mantienen secretas.

Para Maiorano (2019) el cifrado y descifrado constan de una serie de etapas para que un texto normal se cifre y descifre para garantizar la seguridad de información, ver figura 1.

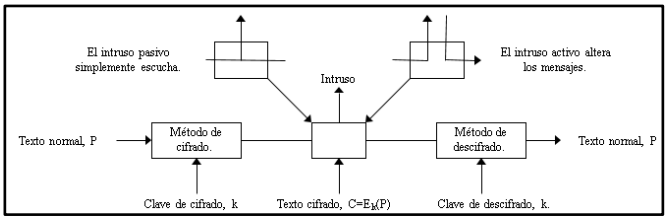

Figura 1.- La encriptación o cifrado.

- El texto normal (P) se transforma (cifra) mediante una función que tiene como parámetro una clave k.
- C = Ek(P) es el texto cifrado (C) obtenido a partir de P, usando la clave k y la función matemática Ek para codificar.
- P = Dk(C) es el descifrado de C para obtener el texto normal P.

Para el descifrado se necesita la inversa de la función matemática descrita como:
Dk(Ek(P)) = P dónde :

- E y D son sólo funciones matemáticas parametrizadas con la clave k
- Estas funciones E() y D( ) son conocidas por el criptoanalista, pero no la clave.

2.2.- Algoritmos del Protocolo Criptográfico

2.2.1.- Algoritmos Simétricos

Llamados algoritmos de una clave. Estos algoritmos

usan para cifrar y descifrar mensajes con la misma clave. En algunos casos pueden tener una clave para cada operación, pero se puede deducir una clave de la otra (Stallings, 2019).

Algunos protocolos utilizan la figura de un árbitro; es una tercera parte desinteresada y confiable, que garantiza a las partes involucradas el cumplimiento de un protocolo. Es desinteresada pues no tiene intereses particulares para intervenir en el protocolo, y es confiable pues las partes toman como honestas las acciones que realiza.

El árbitro otorga mayor seguridad en algunos protocolos. Sin embargo, también genera algunos problemas:

- Demoras en la ejecución del protocolo, ya que se agrega la transmisión de datos al árbitro, al total de mensajes transmitidos entre las partes.

- Cuello de botella en el computador del árbitro.

El árbitro es otro punto factible de atacar para alguien que desee quebrar elprotocolo.
El emisor y el receptor deben acordar la clave que usarán. El emisor la usa para encriptar el mensaje plano y el receptor para desencriptarlo, ver figura 2.

El protocolo es:

1. **A y B concuerdan un algoritmo simétrico.**
2. **A y B concuerdan una clave.**
3. **A encripta el mensaje con el algoritmo y la clave seleccionados.**
4. **A envía el mensaje cifrado a B.**
5. **B desencripta el mensaje cifrado con el algoritmo y la clave seleccionados.**

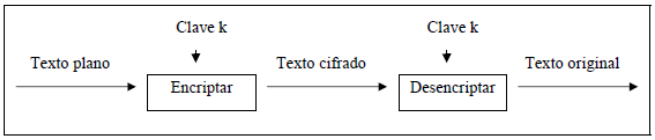

Figura 2.- Cifrado Simétrico.

2.2.2- Algoritmos de Clave Pública

Para Liu (2000) Estos algoritmos usan una clave para encriptar el mensaje claro, llamada clave pública, y otra para desencriptarlo, llamada clave privada o secreta. Esta clave no se puede deducir de la clave pública, ver figura 3.

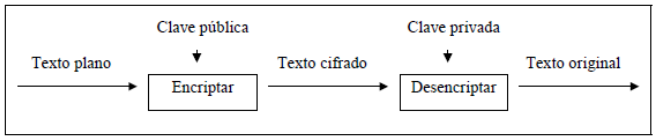

Figura 3.- Cifrado Asimétrico.

Este método se puede comparar con una casilla de correos; cualquier personapuede dejar una carta en la casilla de A, pero sólo A tiene la llave para abrirla y leer las cartas.

El protocolo es:

1. **A y B concuerdan un algoritmo de clave pública.**
2. **A recibe la clave pública de B (k_B).**
3. **A encripta el mensaje con el algoritmo seleccionado y la clave pública de B(k_B).**
4. **A envía el mensaje cifrado a B.**
5. **B desencripta el mensaje cifrado con su clave privada**.

2.3.- Algoritmo Híbrido del Protocolo de Cifrado

En algunos casos, es conveniente combinar los dos tipos de algoritmos; para encriptar mensajes largos los simétricos son más rápidos, y para distribuir las claves que usa el algoritmo asimétrico, los algoritmos de clave pública son más seguros (Stallings, 2017).

El protocolo es:

1. **A y B concuerdan un algoritmo simétrico y uno de clave pública.**
2. **B recibe la clave pública de A (k_A).**
3. **B encripta la clave que usará en el algoritmo simétrico (k_B) con k_A.**
4. **B envía a A k_B encriptada.**
5. **A desencripta con su clave privada a k_B.**
6. **A encripta el mensaje con k_B.**
7. **B desencripta el mensaje con k_B.**

Para Maiorano(2009) desde el punto de vista práctico los pasos son:

1.- Se conoce solo el texto cifrado, ver figura 4.

Figura 4.- Cifrado Asimétrico.- Texto Cifrado.

2.- Conoce un texto cifrado y el texto normal al que pertenece, ver figura 5.

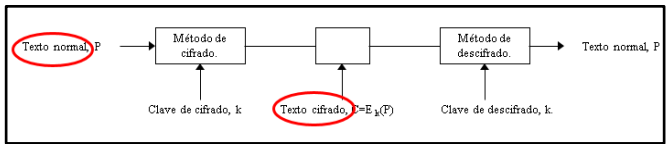

Figura 5.- Cifrado Asimétrico.- Textos.

3.- Dispone del sistema de cifrado. Puede escoger un texto normal y cifrarlo, ver figura 6.

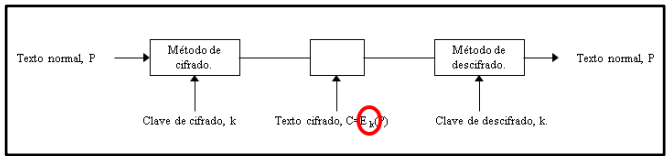

Figura 6.- Cifrado Asimétrico.- Sistema de Cifrado.

3. Resultados

Para Stallings (2019) La idea es usar el mecanismo de clave pública y clave privada para firmar documentos electrónicos. Algunos algoritmos de clave pública, como el RSA, sirven tanto para encriptar como para firmar mensajes.

RSA es el algoritmo de cifrado asimétrico más popular en la actualidad. Creado por Ron Rivest, Adi Shamir y Leonard Adleman –notar que son las iniciales de los apellidos las que forman el nombre del algoritmo– fue publicado en el año 1977.Actualmente el algoritmo es considerado seguro, en tanto sean utilizadas llaves de longitud suficientemente seguras (se siguen utilizando llaves de 1 024 bits, pero ya se recomienda al menos una longitud de 2 048). El algoritmo sirve tanto para encriptar y desencriptar, como para la generación de firmas digitales. Es, en la actualidad, ampliamente utilizado en protocolos de comercio electrónico, entre otras aplicaciones (Maiorano, 2009).

Es decir que para firmar sólo encripta mensajes (con su clave privada), y cualquiera puede desencriptarlos con la clave pública. El mensaje encriptado es la firma del mensaje, ver figura 7, ya que sólo el dueño de la clave privada pudo generarlo (Stallings, 2019).

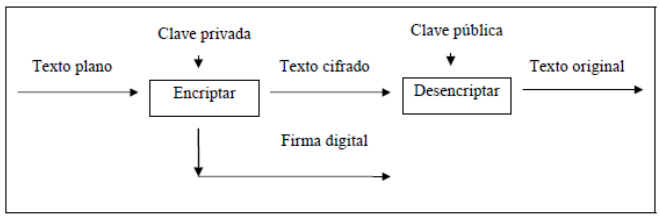

Figura 7.- Protocolo Criptográfico para le generación de firma Digital.

El protocolo es:

1. A concuerdan un algoritmo de firma digital con clave pública.

2. A firma el mensaje con su clave privada kA.

3. A envía a B el mensaje firmado.

4. B desencripta el mensaje con la clave pública de A y verifica la firma.

Se puede observar que se cumplen las características que tiene una firma manual:

- **La firma es inolvidable e irrepudiable, pues A y sólo A conoce la clave privada, y B demuestra que A lo firmó con la clave pública.**
- **La firma es auténtica. B lo verifica con la clave pública de A.**
- **La firma no es reusable, ya que es función del mensaje.**
- **La firma es inalterable, pues si cambia el mensaje, ya no concuerda con la firma.**

La firma digital:

- **Debe ser fácil de generar.**
- **Será irrevocable, no rechazable por su propietario con el acuse de recibo.**
- **Será única, sólo posible de generar por su propietario.**
- **Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.**
- **Debe depender del mensaje (por compendio) y del autor (por certificado).**

Para Maiorano (2009) y Stallings (2019) la firma Digital se genera entonces como sigue:

Supongamos los algoritmos públicos tal que:

E(D(P)) = P

D(E(P)) = P

El algoritmo de cifrado E( ), descifrado D( ) y la clave de cifrado, se hacen públicos (de ahí el nombre de criptografía de clave pública), **pero se mantiene secreta la clave de descifrado , ver figura 8. E_A es clave pública y D_B es clave secreta** (Stallings, 2019).

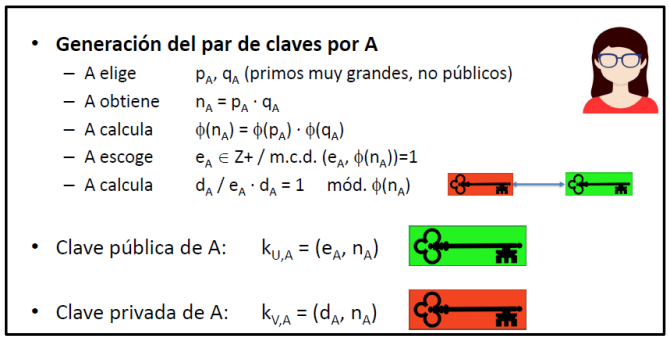

Figura 8.- Etapas del Protocolo Criptográfico para la generación de firma Digital.

Basándose en la figura 8, el algoritmo del **Protocolo Criptográfico** se basa en factorizar números grandes:

1. Seleccionar dos números primos grandes, p y q (generalmente mayores que 10^{100} → 1024 bits).
2. Calcular:
   i. ***n = p * q***
   ii. ***z = (p-1) * (q-1) la* función multiplicativa de Euler.**
3. Seleccionar un número d primo relativo con z (sin ningún factor común).
4. Encontrar e tal que ***((e * d) modulo z) = 1.***
5. **Los datos que serán públicos son el par *(e,n)* y privados *(d,n).***

La figura 9 presenta la captura del texto que firmara el documento de acuerdo al algoritmo del **Protocolo Criptográfico: Gerente Hugo Jimenez 737 ID 05**.

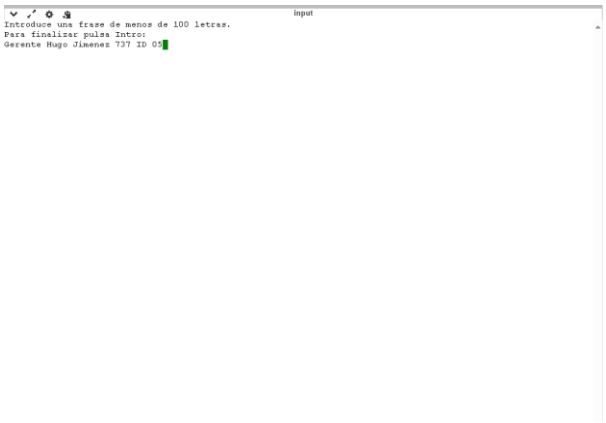

Figura 9.- Texto a firmar en las Etapas del Protocolo Criptográfico para generar el cifrado de firma Digital.

La figura 10 presenta el cifrado y generación de la firma digital de acuerdo con el algoritmo del protocolo criptográfico: **D-A-24-A-1C-28-A-35-F-2A-E-1E-35-13-12-1A-A-1C-A-34-35-3D-39-3D-35-11-7-35-36-3B.**

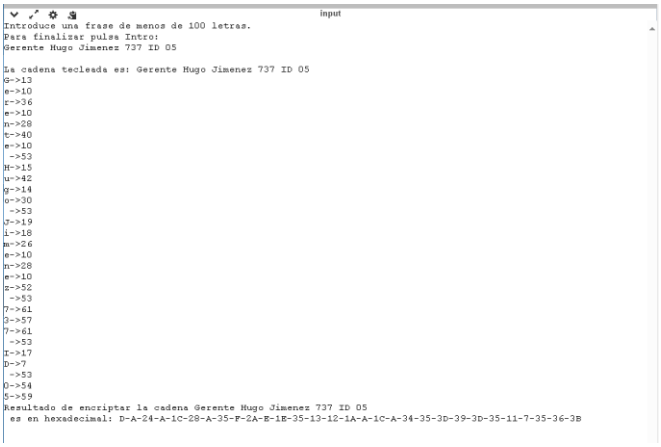

Figura10.- Ejecución de las Etapas del Protocolo Criptográfico para generar el cifrado de firma Digital.

Si el criptoanalista pudiera factorizar *n* (conocido públicamente), podría encontrar *p* y *q*, y a partir de éstos, *z*. Equipado con el conocimiento de *z* y de *e*, que es pública, puede encontrar *d* usando el algoritmo extendido de Euclides:

d = ((Y*z) +1)/e para Y=1,2,3,... hasta encontrar un d entero.

La figura 11 presenta el descifrado de firma digital de acuerdo al algoritmo del protocolo criptográfico: **Gerente Hugo Jimenez 737 ID 05**.

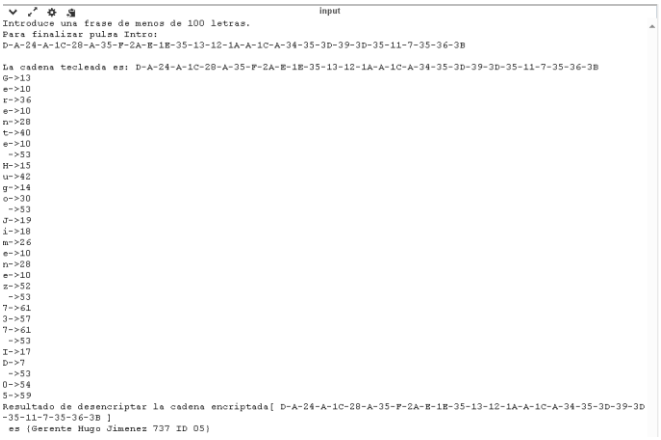

Figura11.- Ejecución de las Etapas del Protocolo Criptográfico para generar el descifrado de firma Digital.

4. Discusión

Para Maiorano (2009) la firma digital corresponde a la versión Computarizada de la firma personal manuscrita o firma ológrafa; esto es, se usará para probar la autoría de, o el acuerdo a, la información contenida en un documento electrónico. Existen diferentes protocolos para implementar esta funcionalidad criptográfica. La implementación más utilizada involucra la utilización de funciones hash junto con el protocolo de cifrado con criptografía asimétrica. Básicamente, la parte autora o firmante del documento firmará el hash resultante (Stalling, 2019).

Esto es: La parte "A" producirá el hash del documento, lo encriptará con su llave privada y enviará esto, junto con el documento, a la parte "B". "B" computará por su cuenta el hash sobre el documento. Luego, mediante la llave pública de "A", desencriptará el hash que "A" ha computado. Entonces, "B" podrá comparar ambos hashes y verificar la firma.

5. Conclusiones

El protocolo criptográfico de firma digital al emplear la encriptación y las firmas en el documento lograr mayor seguridad; el protocolo criptográfico permite segurar el signado de documentos en forma segura al establecer un protocolo entre las partes involucradas considerando las siguientes fases:

1. **A y B concuerdan un algoritmo de firma digital (con las claves pública f_A y laprivada F_A) y otro de clave pública (con las claves pública k_B y privada K_B).**
2. **A firma el mensaje con su clave privada (F_A).**
3. **A encripta el mensaje y la firma con la clave pública de B (k_B) y se los envía B.**
4. **B desencripta el mensaje y la firma con su clave privada (K_B).**
5. **B genera el hash a partir del mensaje desencriptado.**
6. **B desencripta la firma recibida con la clave pública de A (f_A), y lo comparacon el hash generado anteriormente. Si son iguales, la firma es válida.**

6. Agradecimientos

A la empresa CD, S.C., por el apoyo técnico y documental, así como, al área de Recursos Humanos por el acceso a las claves con las que signan cada uno de los miembros de la organización. A Cada uno de los integrantes de artículo por el aporte computacional y matemático para realizar los aplicativos.

7. Referencias

Craig H.(2003). Networking Personal Computers, whit TCP/IP. O'Relly Associates, Inc.Sebastopol, CA 95472.

Liu C.(2000). Managing Internet Information Services. O'Relly Associates, Inc.Sebastopol, CA 95472

Maiorano, A. (2009). Criptografía: técnicas de desarrollo para profesionales. México: Alfaomega.

Stallings, W. (2017). Fundamentos de Seguridad en Redes: Aplicaciones y Estandáres. México: Pearson, Prentice Hall.

Stallings, W. (2019). Criptografía y Seguridad de Red: Principios y Práctica. México: Pearson, Prentice-Hall.