UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

A+T Actualidad Tecnológica

Análisis y comparación del algoritmo de cifrado DSA

Analysis and comparison of DSA encryption algorithm

Oscar Gonzalo Roa-Afanador [1], Juliana Polo-Moreno [2], Yeison David Prieto [3]

Para citar este artículo: O. G. Roa-Afanador, J. Polo-Moreno, Y. D. Prieto, " Análisis y comparación del algoritmo de cifrado DSA ", Revista Vínculos, vol 19, no. 1, p-p 46-50, 2022.
https://doi.org/10.14483/2322939X.17664

Recibido: 19-11-2021 / Aprobado: 24-03-2022

Resumen: En el presente artículo se realiza un análisis sobre el algoritmo de cifrado DSA, en el que se hace un repaso sobre la historia y su funcionamiento, además se realiza un análisis sobre sus aplicaciones, comparativas con otros métodos de cifrado y recomendaciones.

Palabras clave: RSA, DSA, Firmas digitales, Clave privada, Clave pública, Criptografía, Cifrado, Firmas digitales, Criptosistemas de clave pública, Privacidad, Autenticación.

Abstract: In this article, an analysis of the DSA encryption algorithm will be conducted, encompassing a historical overview and operational examination. Furthermore, the document will delve into its applications, conduct comparisons with alternative encryption methods, and provide recommendations.

Keywords: RSA, DSA, Digital Signatures, Private Key, Public Key, Cryptography, Cipher, Digital signatures, Public-key Cryptosystems, Privacy, Authentication.

1 Tecnólogo en sistematización de datos, Universidad Distrital, Colombia - Bogotá. ogroaa@correo.udistrital.edu.co
2 Tecnóloga en sistematización de datos, Universidad Distrital, Colombia - Bogotá. jpolom@correo.udistrital.edu.co
3 Tecnólogo en sistematización de datos, Universidad Distrital, Colombia - Bogotá. ydprietof@correo.udistrital.edu.co

1. Introducción

Hoy en día podemos evidenciar la cantidad de riesgos que implica el envío de información a través de medios digitales, uno de estos riesgos y de los más comunes es la suplantación de identidad. A lo largo de la historia hemos conocido cómo este algoritmo se ha estado usando desde los principios de la civilización como una de las tácticas para conocer, revelar información o enviar mensajes erróneos que generan una ventaja en uno o más grupos de personas.

Por este motivo se vuelve importante el concepto clave de firma digital, el cual consiste en un conjunto electrónico de datos que acompaña o está asociado a un documento o mensaje electrónico cuya funcionalidad es la de identificar de forma inequívoca al remitente, asegurando la integridad del documento o mensaje enviado a fin de confirmar que este no ha sido manipulado o modificado antes de ser obtenido por el receptor.

Existen algoritmos que permiten no solo la firma de un documento o mensaje digital, sino que también facilitan el proceso de cifrado del mensaje a transmitir.

En este documento se pretende hacer un análisis detallado del algoritmo de cifrado DSA, describiendo su funcionamiento, rendimiento y aplicaciones, adicionalmente realizaremos una observación de las comparaciones realizadas por otros autores de este con otros algoritmos para determinar cuál de estos funciona mejor de acuerdo con el requerimiento o situación en el que se requiera.

2. Algoritmo de cifrado DSA

DSA es un estándar del Gobierno Federal de los Estados Unidos o FIPS para firmas digitales. Fue un algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en el Estándar de Firma Digital (DSS), especificado en el FIPS 186. DSA se hizo público el 30 de agosto de 1991, este algoritmo como su nombre lo indica sirve para firmar y no para cifrar información. [1]

En otras palabras, el algoritmo de cifrado DSA es un algoritmo asimétrico de clave pública con el que podemos verificar la autenticidad de un mensaje dada una clave pública y la firma del mensaje. [2-3]

2.1 Algoritmo de firma digital DSA

La primera parte del algoritmo DSA es generar la clave pública y generar la clave privada, que se describe de la siguiente manera:

- Elegir un número primo q, tal que $p - 1\, mod\, p = 0$. p se denomina módulo primo.
- Elegir un número primo q, que se llama divisor principal.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 46-50. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

- Calcular un número entero g tal que $1 < g < p, g^q \ mod \ p \ = 1$ y $g = h^{\ ((p-1)/q)} mod \ p$. q también se llama módulo de orden multiplicativo g de p.
- Elegir un número entero x tal que $0 < x < q$.
- Calcular y como $g^x mod \ p$.
- Agrupar la clave pública como $\{p, q, g, y\}$.
- Agrupar la clave privada como $\{p, q, g, x\}$.

La segunda parte del algoritmo DSA es la generación y verificación de la firma, que se describe como:

- Generar el resumen del mensaje, usando un algoritmo como SHA1, se conoce como h.
- Generar un número aleatorio k, tal que $0 < k < q$.
- Calcular un número r como $(g^k \ mod \ p) \ mod \ q$. Si $r = 0$, seleccionar una k diferente.
- Calcular un número i, tal que $k * i \ mod \ q \ = 1$. i se llama inverso multiplicativo modular de $k \ mod \ q$.
- Calcular $s \ = \ i * (h + r * x) \ mod \ q$. Si $s = 0$ seleccionar una k diferente.
- Agrupar la firma digital $\{r, s\}$.

Tercera parte del algoritmo DSA, se verifica la firma de un mensaje:

- Generar el resumen del mensaje (h), usando el mismo algoritmo hash.
- Calcular w, de modo que $s * w \ mod \ q \ = 1$. w se denomina inverso modular de $s \ mod \ q$
- Calcular $u1 = \ h * w \ mod \ q$.
- Calcular $u2$= r*w mod q.
- Calcular $v \ = \ (((g^{u1}) * (y^{u2}) \ mod \ p) \ mod \ q$.
- Si $v \ == \ r$, la firma digital es válida.

3. Algoritmo Rivest Shamir and Adleman (RSA)

RSA es un algoritmo criptográfico de clave pública que está basado en la premisa de la dificultad de factorizar números enteros grandes. Un usuario del algoritmo RSA crea y publica el producto de dos números primos extensos, junto con un valor auxiliar, como su clave pública [4]. Los factores primos deben mantenerse en secreto. Cualquier persona puede usar la llave pública para encriptar un mensaje, pero con los métodos actuales, si la clave pública es lo suficientemente larga, únicamente alguien que conozca los factores primos puede decodificar el mensaje de forma factible [5-7].

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 46-50. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

4. Algoritmo Elliptic Curve Cryptography (ECC)

El algoritmo de criptografía de curva elíptica es relativamente nuevo en la familia de algoritmos de clave pública que puede proporcionar longitudes de clave más cortas y según el entorno y la aplicación en la que se utilice, un rendimiento mejorado sobre el sistema basado en la factorización de enteros y logaritmos discretos [8]. Este algoritmo se basa en una estructura matemática en la que se pueden definir ciertas operaciones. Estas operaciones proporcionan una función unidireccional que se puede utilizar para producir sistemas criptográficos eficientes [9-10]. La seguridad y las ventajas de usar sistemas criptográficos basados en curvas elípticas en lugar de la factorización de enteros y los métodos basados en logaritmos discretos es que proporcionan niveles de seguridad similares utilizando longitudes de clave más pequeñas

5. Conclusiones

El uso de algoritmos de cifrado se ha vuelto cada vez más recurrente, y este ha tenido mayor impacto especialmente en esta época de pandemia, para ciertos sectores económicos o para ciertos procesos donde se requiere una verificación de identidad del remitente, o se requiere mantener un alto nivel de confidencialidad de la información, para lo cual resulta esencial la implementación de un método de cifrado.

Para realizar la elección del método o del algoritmo de cifrado se debe realizar un análisis de la necesidad y determinar qué algoritmos cuentan con la solución específica para estos requerimientos, por ejemplo, si se requiere cifrar la información de un mensaje, sabemos de antemano que el algoritmo DSA no nos va a funcionar, puesto que su funcionalidad va orientada a la firma de documentos o mensajes; en cambio es algoritmo RSA puede llegar a adaptarse mejor a nuestra necesidad.

Ahora, en cuanto a optimización de recursos, sabemos que el algoritmo DSA requiere de bastante tiempo para realizar los cálculos correspondientes para realizar sus operaciones, por lo que podríamos llegar a considerar el algoritmo (ECC) o inclusive variaciones del algoritmo DSA que estén basados en curvas elípticas como por ejemplo el algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm) que es el que actualmente utiliza Bitcoin para garantizar que los fondos solo puedan ser utilizados por sus legítimos propietarios.

Referencias

[1] N. Jirwan, A. Singh, S. Vijay. "Review and analysis of cryptography techniques," *International Journal of Scientific &*

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 46-50. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Engineering Research, vol. 4, no 3, pp. 1-6. 2013

[2] MA Al-Absi, A Abdullaev, AA Al-Absi, M Sain, HJ Lee. "Cryptography Survey of DSS and DSA," Advances in Materials and Manufacturing Engineering: Proceedings of ICAMME 2019. Springer Singapore, pp. 661-669, 2020.

[3] T. Nitha, J. Meenu Elizabath. "Montgomery multiplier for faster cryptosystems," *Procedia Technology*, vol. 25, pp. 392-398, 2016

[4] JJ Ruíz-Lagunas, JC Olivares-Rojas, A Antolino-Hernández, A Núñez-Vieyra, A., Alvarado-Zamora, L. N., & Ferreira-Medina. "Caracterización de Algoritmos de Cifrado para la Comunicación Segura en Dispositivos Móviles Characterization of Encoding Algorithms for Secure Communication in Mobile Devices," 8vo CONGRESO INTERNACIONAL DE INGENIERÍA ELECTROMECÁNICA Y DE SISTEMAS (CIIES 2016) https://www.researchgate.net/profile/Juan_Carlos_Olivares_Rojas3/publication/322701191_Characterization_of_Encoding_Algorithms_for_Secure_Communication_in_Mobile_Devices/links/5a6a185a4585154d15466ae7/Characterization-of-Encoding-Algorithms-for-Secure-Communication-in-Mobile-Devices.pdf

[5] AS Alkalbani, T Mantoro, AOM Tap. "Comparison between RSA hardware and software implementation for WSNs security schemes," Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010. IEEE. pp. E84-E89, 2010.

[6] K. Kaur, E. Seema. "Hybrid algorithm with DSA, RSA and MD5 encryption algorithm for wireless devices," *International Journal of Engineering Research and Applications*, vol. 2, no 5, pp. 914-917, 2012.

[7] K. Sivaraman. "A comparison study of rsa and dsa algorithm in movile cloud computing," *International Journal of Pure and Applied Mathematics*, vol. 116, no 8, pp. 247-253, 2017

[8] A. H. Alajbegović, B. Bc, P.D.H. Jamak, B.H. Zenica, P.D.D. Zečić. "Digital Signature Algorithm (DSA)," 10th International Research/Expert Conference, Trends in the Development of Machinery and Associated Technology TMT. pp.11-15, 2006.

[9] S. Nagaraj, G Raju, V Srinadth. "Data encryption and authetication using public key approach," *Procedia Computer Science*, 48, pp. 126-132, 2015.

[10] P. MacKenzie, MK Reiter. "Two-party generation of DSA signatures," Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 137-154, 2001.