Algoritmo asimétricos y sus funciones de encriptación y desencriptación

Michael Daniel Murillo López
Corporación Universitaria Minuto de Dios -UNIMINUTO
mmurillolo1@unimiuto.edu.co
Bogotá DC - Colombia

Resumen

Los algoritmos asimétricos son técnicas inteligentes que se usan para la protección de datos y son parte fundamental al momento de definir una seguridad de un sistema. Su uso ha permitido un gran niveles de seguridad donde es necesario garantizando privacidad e incluso anonimato. En los algoritmos asimétricos se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

1. Introducción

Es un algoritmo que modifica los datos de un documento con el objeto de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad.

2. Que son las llaves publicas y privadas en los algoritmos asimétricos

Primero tienes que cargar el archivo de imagen desde su computadora usando el enlace de carga del menú del proyecto. Luego usando el comando 'includegraphics' podrás incluirlo en el documento. Con el entorno de figura y el comando de título podrás agregar un número y un título a la figura. Mira el código de la Figura 2 en esta sección para ver un ejemplo.

3. Tipos de Algoritmos Asimétricos

3.1. Diffie-Hellman

Primero tienes que cargar el archivo de imagen desde su computadora usando el enlace de carga del menú del proyecto. Luego usando el comando 'includegraphics' podrás incluirlo en el documento. Con el entorno de figura y el comando de título podrás agregar un número y un título a la figura. Mira el código de la Figura 2 en esta sección para ver un ejemplo.

Puedes añadir comentarios en el ícono + del menú de arriba.

Para responder a un comentario, simplemente da click en Reply en Rich Text.

También pueden añadirse comentarios en el margen del pdf compilado con el comando todo , como se muestra en el ejemplo de la derecha. También puedes añadirlos dentro del texto:

Este es un comentario dentro del texto.

¡Comment en el margen!

Figura 1: Esta imagen se añadió en el menú Project.

Figura 2: Esta imagen se añadió en el menú Project.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 1: Una simple tabla.

3.2. RSA

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

3.3. DSA

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

3.4. Cifrado ElGamal

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

3.5. Cifrado Criptografía de curva elíptica

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

3.6. Criptosistema de Merkle-Hellman

LaTeX es buenísimo para escribir ecuaciones. Para escribir variables o ecuaciones dentro del texto lo podemos poner entre signos de pesos y luego podemos seguir escribiendo, esto funciona si queremos escribir un símbolo como ∇, π, β, Ω, $\aleph$, etc.

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x \tag{1}$$

$$\int_0^1 dx = 1 \tag{2}$$

$$e^{i\pi} + 1 = 0 \tag{3}$$

Si queremos citar al gran Maxwell, lo podemos hacer como en la ecuación 4:

$$\nabla \times \mathbf{E} + \frac{\partial \mathbf{B}}{\partial t} = 0 \tag{4}$$

A continuación se añade un ejemplo de un desarrollo: Con este preámbulo llevamos a cabo la siguiente transformación de los operadores $\hat{a}_\ell$

$$\hat{b}_m^\dagger = \sum_\ell U_m^\ell \hat{a}_\ell^\dagger \tag{5}$$

donde U_m^ℓ es un elemento de la matriz unitaria $\mathbf{U}$.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 2: Una simple tabla.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 3: Una simple tabla.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 4: Una simple tabla.

Calculamos ahora su hermitiano conjugado

$$\begin{aligned}\hat{b}_m &= \left(\sum_\ell U_m^\ell \hat{a}_\ell^\dagger\right)^\dagger && (6)\\ &= \sum_\ell \left(U_m^\ell \hat{a}_\ell^\dagger\right)^\dagger \\ &= \sum_\ell \left(U_m^\ell\right)^* \hat{a}_\ell \\ &= \sum_\ell \left(U^{-1}\right)_\ell^m \hat{a}_\ell, && (7)\end{aligned}$$

Ahora, para añadir una matriz:

$$\begin{matrix} a & b \\ c & d \end{matrix} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} \quad \begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$$

$$\vec{A}\cdot(\vec{B}\times\vec{C}) = \begin{vmatrix} A_x & A_y & A_z \\ B_x & B_y & B_z \\ C_x & C_y & C_z \end{vmatrix} \qquad (8)$$

3.7. Goldwasser-Micali

Puedes añadir listas con numeración automática ...

1. Como esta,
2. y como esta.

... o con puntitos ...

- Como este,
- y como este.

3.8. Cifrado Goldwasser-Micali-Rivest

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

3.9. Cifrado extremo a extremo

Usa los comandos table y tabular para iniciar una tabla simple — mira la tabla 6, como ejemplo.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 5: Una simple tabla.

l para left	c para centro	r para derecha
Ejemplo	Centrado	Alineado a la
Izquierda	13	Derecha

Cuadro 6: Una simple tabla.

3.10. ¿Cómo añado una lista de Citas y Referencias?

Puedes subir un archivo `.bib` que contenga todas tus referencias en estilo BibTeX (puedes buscar la bibliografía de un libro en google añadiendo 'bibtex' al final), creado con JabRef. Luego podrás hacer citas así: [**?**].