

Algoritmo asimétricos y sus funciones de encriptación y desenscriptación

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.

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. Tipos de Algoritmos Asimétricos

2.1. 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 1 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!

2.2. RSA

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

2.3. DSA

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

2.4. Cifrado ElGamal

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

2.5. Cifrado Criptografía de curva elíptica

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

Figura 1: 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.

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

Cuadro 2: Una simple tabla.

2.6. Criptosistema de Merkle-Hellman

L^AT_EX 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.

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x \quad (1)$$

$$\int_0^1 dx = 1 \quad (2)$$

$$e^{i\pi} + 1 = 0 \quad (3)$$

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

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

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

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

donde U_m^ℓ es un elemento de la matriz unitaria \mathbf{U} .
Calculamos ahora su hermitiano conjugado

$$\hat{b}_m = \left(\sum_{\ell} U_m^\ell \hat{a}_\ell^\dagger \right)^\dagger \quad (6)$$

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

Ahora, para añadir una matriz:

$$\begin{array}{cc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \begin{bmatrix} a & b \\ c & d \end{bmatrix} \end{array} \quad \begin{array}{cc} \begin{vmatrix} a & b \\ c & d \end{vmatrix} & \left\| \begin{array}{cc} a & b \\ c & d \end{array} \right\| \end{array}$$

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

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.

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

Cuadro 5: Una simple tabla.

2.7. Goldwasser-Micali

Puedes añadir listas con numeración automática ...

1. Como esta,
2. y como esta.

... o con puntitos ...

- Como este,
- y como este.

2.8. Cifrado Goldwasser-Micali-Rivest

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

2.9. Cifrado extremo a extremo

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

2.10. ¿Cómo añadir 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: [?].

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

Cuadro 6: Una simple tabla.