Criptografía

Programa detallado

La palabra Criptografía procede de

$$\begin{array}{c} \textit{crypto} = \text{secreto} \\ \textit{grafos} = \text{escritura} \end{array}$$

Así, la *Criptografía* es la ciencia que estudia la escritura cifrada (oculta).

Se denomina:

Criptoanálisis al estudio de la ruptura de los cifrados obtenidos por la Criptografía. *Criptología* a la unión de Criptografía y Criptoanálisis.

El procedimiento de cifrar consiste en transformar un mensaje en claro en un mensaje cifrado o criptograma, a través de una función de cifrado:

$$\begin{array}{ccc} \mathcal{M} & \longrightarrow & \mathcal{C} \\ M \text{ (mensaje en claro)} & & \\ +K \text{ (clave)} & \mapsto & C \text{ (mensaje cifrado)} \end{array}$$

Se ha producido un desarrollo constante de la Criptografía a lo largo de la historia. El conjunto de técnicas criptográficas desarrolladas hasta finales de los años 70 del pasado siglo recibe el nombre de *Criptografía clásica*. Su uso era fundamentalmente militar, diplomático o relacionado con grandes empresas, y su único objetivo era garantizar la confidencialidad de los mensajes.

En la actualidad su uso es civil y masivo, y sus objetivos son múltiples: además de tener que garantizar la confidencialidad de los mensajes han aparecido otras necesidades, como veremos a lo largo de este curso.

Detallamos a continuación el contenido del curso.

- Vídeos:

1_1clasica.	Introducción a la Criptografía: Criptografía clásica.
1_2seguridad.	Introducción a la Criptografía: Seguridad criptográfica.
1_3preliminares.	Preliminares matemáticos: Conversión de mensajes. Aritmética modular.
1_4preliminares.	Preliminares matemáticos: Cifrado afín I. Divisibilidad. Números primos.
2_1preliminares.	Preliminares matemáticos: Inversos modulares. Teorema chino del resto.
2_2cifradoenflujo.	Cifrado en flujo: Características del cifrado en flujo. Generación de secuencias pseudoaleatorias.
2_3gencongruen.	Cifrado en flujo: Generadores congruenciales.
3_1registros.	Cifrado en flujo: Registros de desplazamiento.
3_2bloque.	Cifrado simétrico en bloque: Introducción. Modos de cifrado.
3_3DES.	El algoritmo DES: Descripción del algoritmo. Debilidades y ataques. Triple DES.
4_1preliminares.	Preliminares matemáticos: Anillos de polinomios. Cuerpo de Galois. Operaciones en el algoritmo AES.
4_2AES.	Cifrado simétrico en bloque: El algoritmo AES.
4_3preliminares.	Preliminares matemáticos: Primalidad. Factorización.
5_1clavepublica.	Criptografía de clave pública: Características de la Criptografía de clave pública. Complejidad computacional. Servicios de seguridad.
5_2logdisc.	Criptografía de clave pública: Logaritmo discreto. Intercambio de claves de Diffie-Hellman. Criptosistema ElGamal.
5_3RSA.	Criptografía de clave pública: Criptosistema RSA.
6_1hashintro.	Protocolos de autenticación: Funciones hash. Introducción.
6_2hashalg.	Protocolos de autenticación: Funciones hash. Algoritmos.
6_3firmas.	Protocolos de autenticación: Firmas digitales.

- Prácticas:

Práctica 0:	Funciones auxiliares.
Práctica 1:	Aritmética modular.
Práctica 2:	Cifrado afín.
Práctica 3:	Cifrado en flujo.
Práctica 4:	El algoritmo AES.
Práctica 5:	Primalidad. Factorización.
Práctica 6:	Clave pública.