Fundamentos de Criptografía y Seguridad Informática

6 ECTS

3 horas Teoría + 2 horas Prácticas

Francisco de Borja Rodríguez Ortiz

Escuela Politécnica Superior (EPS)

Universidad Autónoma de Madrid (UAM)

¿POR QUÉ CRIPTOGRAFÍA?

- Hoy en día se quiere formar a profesionales que puedan evaluar en un Departamento de Sistemas de Información la seguridad y protección de datos del mismo.
- Por lo tanto, las empresas actuales demandan más perfiles profesionales de informáticos con conocimiento y fundamentos en seguridad de la información.
- La herramienta fundamental para llevar a buen término ese objetivo es la criptografía y el criptoanálisis.
- En este curso se pretenden transmitir los fundamentos básicos de la criptografía y seguridad de la información.
- Se pretende dar al alumno una base profunda de la fortaleza y la debilidad de los diversos métodos de cifrado que existen.

¿POR QUÉ CRIPTOGRAFÍA?

- Los alumnos necesitarán discernir con certeza aquellos conceptos que subyacen a los algoritmos de cifrado que les permitan valorar el grado de fiabilidad y eficiencia para una aplicación cualquiera.
- El objetivo final del curso no consiste en que se hayan memorizado los métodos más punteros de cifrado y de *hashing*, sino que cuando se les ponga en sus manos un algoritmo de cifrado cualquiera sepan determinar con la ayuda de los conceptos aprendidos:
  - cómo es de seguro,
  - cuál es su eficiencia,
  - en qué circunstancias puede ser utilizado,
  - e incluso modificarlo para adaptarlo a un problema concreto.

¿POR QUÉ CRIPTOGRAFÍA?

- El curso contiene los temas fundamentales siguientes:
  - Introducción.
  - Métodos clásicos de cifrado.
  - Cifrado perfecto y distancia de unicidad.
  - Cifrado simétricos por bloques: DES y AES.
  - Criptografía de clave pública: RSA.
  - MAC y Hash.
- + 3 prácticas (estás son aplicación directa de la teoría).
- Para mas detalle se puede consultar: http://www.uam.es/ss/Satellite/EscuelaPolitecnica/es/estudios/Page/sinContenido/repositorio-de-guias-docentes.htm
- O hablar con Francisco de Borja Rodríguez Ortiz B-328.