Máster Universitario en Software y Sistemas

Fundamentos de criptografía

- **PROFESOR:** Dario Fiore
- **ORGANISMO DE PROCEDENCIA:** Instituto IMDEA-Software
- **CORREO ELECTRÓNICO:** dario.fiore@imdea.org

- **PROFESOR:** Antonio Faonio
- **ORGANISMO DE PROCEDENCIA:** Instituto IMDEA-Software
- **CORREO ELECTRÓNICO:** antonio.faonio@imdea.org

Resumen de Contenido

La criptografía es una herramienta fundamental para proteger la información y la comunicación en los sistemas informáticos. Este curso es una introducción a la criptografía, adecuada para estudiantes interesados en matemáticas e informática. El curso se centrará principalmente en las definiciones y construcciones de varias primitivas criptográficas, incluidos los generadores pseudoaleatorios, las funciones pseudoaleatorias, los esquemas de cifrado, las firmas digitales y los códigos de autenticación de mensajes. Los estudiantes aprenderán a razonar acerca de la seguridad de las construcciones criptográficas y cómo usar adecuadamente estas construcciones en aplicaciones del mundo real.

Programa

1. Introducción general al problema de la comunicación secreta. Seguridad perfecta; cifrado one-time pad y resultado de imposibilidad de Shannon. Introducción a la seguridad computacional
2. Cifrado y motivación para funciones básicas: funciones/permutaciones unidireccionales, permutaciones de trapdoor
3. Teoría de números y realizaciones de (trapdoor) funciones unidireccionales
4. Encriptación de clave pública de juguete; de la encriptación determinista a la probabilística. Bits Hardcore y el teorema de Goldreich-Levin
5. Generadores pseudoaleatorios
6. Cifrado de clave pública: definición de seguridad y construcciones semánticas
7. Cifrado de clave secreta y cifrado de flujo
8. Funciones pseudoaleatorias: definiciones y realizaciones
9. Códigos de autenticación de mensaje
10. Firmas digitales
11. Funciones hash resistentes a colisiones
12. Más temas

Método de Evaluación

Hojas de ejercicios periódicos

Prerrequisitos

No se requiere conocimiento previo de criptografía, así como tampoco se requieren prerrequisitos matemáticos formales. Sin embargo, se espera una madurez matemática (por ejemplo, pruebas de lectura y escritura).

Créditos

2 ECTS

Bibliografía

- Jonathan Katz and Yehuda Lindell: Introduction to Cryptography (http://www.cs.umd.edu/~jkatz/imc.html)

Días de Impartición y Horario

- 21 de febrero, 17:00-19:00
- 26 de febrero, 17:00-19:00
- 07 de marzo, 17:00-19:00
- 14 de marzo, 17:00-19:00
- 04 de abril, 17:00-19:00
- 11 de abril, 17:00-19:00
- 18 de abril, 17:00-19:00
- 25 de abril, 17:00-19:00
- 09 de mayo, 17:00-19:00
- 16 de mayo, 17:00-19:00
- 23 de mayo, 17:00-19:00
- 30 de mayo, 17:00-19:00

Sitio web:

http://www.dariofiore.it/teaching/foundations-of-cryptography-spring-2018/

Aula

H-1003

Idioma

Inglés.

Cupo:

50

Inscripción a este seminario:

Para inscribirse a este seminario, por favor, *rellena estos campos* (solo son válidos correos de la UPM):

- Apellidos: *
- Nombre: *
- Correo electrónico: *

Inscribirme al seminario