Actividades Formativas IMEIO/ Educational Activities IMEIO

Título/Title: Criptografía
Organizador/Organizer: Jorge Jiménez Urroz, jorge.urroz@upm.es
Profesores/Lecturers: Jorge Jiménez Urroz
Horas totales/Number of hours: 12
Lugar/Location: Escuela de Caminos
Fechas/Dates: Diciembre 2024

Resumen/Summary:

Resumen/Summary: El curso será una introducción a la Criptografía de Clave Pública, con énfasis en los problemas de aritmética que garantizan la seguridad de cada protocolo. Se darán las nociones de seguridad, y se verán los principales protocoles como criptosistemas, intercambio de claves, funciones de Hash, autenticación, firmas, o pruebas de conocimiento cero.

Se desarrollará la teoría primero con referencia a problemas de aritmética elemental clásicos, como la factorización (y tests de primalidad) y el logaritmo discreto.

-1. Introducción: Criptografía clásica con ejemplos. Criptoanálisis. Entropía y seguridad

-2. Criptografía de clave pública: Protocolos criptográficos. Funciones de Hash. El criptosistema RSA. El Gamal. Pruebas de conocimiento cero.

-3. Primalidad y Factorización: Test de Fermat. Solovay-Strassen. Miller-Rabin. Los métodos de Pollard, $p-1$ y ρ. Factorización de Fermat. El algoritmo base de factores. Criba cuadrática.

-4. El logaritmo discreto: El algoritmo de Shanks. El algoritmo de Pollard ρ. El algoritmo de Pohlig-Hellman. El cálculo del Índice.

En cada uno de los epígrafes anteriores, se harán ejemplos con Python. Al principio del curso haremos una brevísima introducción al lenguaje.

Aunque no será imprescindible, se recomienda traer vuestro ordenador a clase e instalar Python, para poder hacer los ejercicios en casa.

¿Aceptarías que el curso se pudiera emitir por videoconferencia restringido a algunos alumnos del doctorado que no pudieran asistir presencialmente? Would you accept that the course could be given by videoconference restricted to some doctoral students who could not attend in person?

No