Actividades Formativas IMEIO/ Educational Activities IMEIO

Título/Title: Introducción a la Criptografía Introduction to Public Key Cryptography	
Organizador/Organizer: Jorge Jiménez Urroz/ jorge.urroz@upm.es	
Profesores/Lecturers: Jorge Jiménez Urroz	
Horas totales/Number of hours: 20	
Lugar/Location: ETSCCyP	
Fechas/Dates: Junio 2024/ June 2024	

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, y al final se hará una breve interpretación de estos en el entorno de las curvas elípticas. Los conocimientos de curvas elípticas necesarios para este capítulo se darán también como materia del curso.

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

-2. Aritmética elemental: Complejidad de cálculo. Divisibilidad y algoritmo de Euclides. Congruencias. Teorema chino del resto. Las funciones $\mu(n)$ y $\varphi(n)$ y teoremas de ortogonalidad. Estructuras algebraicas. Reciprocidad cuadrática.

-3. Criptografía de clave pública: Protocolos criptográficos. Funciones de Hash. El criptosistema RSA. El Gamal. Pruebas de conocimiento cero.

-4. 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.

-5. El logaritmo discreto: El algoritmo de Shanks. El algoritmo de Pollard ρ. El algoritmo de Pohlig-Hellman. El cálculo del Índice.

-6. Criptografía con curvas elípticas: Fundamentos. El intercambio de claves de Diffie-Hellman. El criptosistema de Massey-Omura. El Gamal y RSA elíptico. El ataque MOV. Primalidad y Factorización. Parejas amigables de curvas elípticas.

The course will be an introduction to Public key Cryptography, with emphasis on the arithmetical problems that guarantee the security of each protocol. We will give the notions of security, and we will see the main cryptographic protocols as cryptosystems, key exchange, Hash functions, authentication, signatures or zero knowledge proofs.

We will develop the theory first refering to problems in classical problems of elementary arithmetic, as factorization (and primality tests) and discrete logarithms and at the end we will interpret briefly those problems in the context of elliptic curves. The necessary knowledge of elliptic curves for this chapter will also part of the course.

-1. Introduction: Classic cryptography with examples. Cryptanalysis. Entropy and security

-2. Elementary arithmetic: Complexity of calculation. Divisibility and Euclid's algorithm. Consistencies. Chinese remainder theorem. The functions $\mu(n)$ and $\varphi(n)$ and orthogonality theorems. Algebraic structures. Quadratic reciprocity.

-3. Public key cryptography: Cryptographic protocols. Hash functions. The RSA cryptosystem. The Gamal. Zero knowledge proofs.

-4. Primality and Factorization: Fermat Test. Solovay-Strassen. Miller-Rabin. Pollard's methods, $p-1$ and ρ. Fermat factorization. The factor base algorithm. Quadratic sieve.

-5. The discrete logarithm: Shanks' algorithm. Pollard's algorithm ρ. The Pohlig-Hellman algorithm. The calculation of the Index.

-6. Cryptography with elliptic curves: Fundamentals. The Diffie-Hellman key exchange. The Massey-Omura cryptosystem. The Gamal and elliptical RSA. The MOV attack. Primality and Factorization. Friendly pairs of elliptic curves.

¿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?

Si/Yes