C. 1996
(8)

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
FOLIO
31

CARAL.DOC

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación
2. CUATRIMESTRE: Segundo de 1996
3. ASIGNATURA: CRIPTOGRAFIA
4. CARRERA: Licenciatura en Ciencias de la Computación
5. CARACTER DE LA MATERIA: OPTATIVA PLAN '87 Y '93
6. NUMERO DE CODIGO DE CARRERA: 18
7. NUMERO DE CODIGO DE MATERIA: C618
8. PUNTAJE: PLAN '87 (1P) PLAN '93 (1P)
9. PLAN DE ESTUDIOS AÑO: 1987 Y 1993
10. DURACION DE LA MATERIA: SEMANAL
11. HORAS DE CLASE SEMANAL:

    a) TEORICAS 3 HS. c) PROBLEMAS HS
    b) LABORATORIO HS d) SEMINARIOS

12. CARGA HORARIA TOTAL: 3HS
13. ASIGNATURAS CORRELATIVAS: NINGUNO EN ESPECIAL. BASICOS DE MATEMATICA Y ARITMETICA. ALGORITMOS.
14. FORMA DE EVALUACION: Practicos y Final
15. PROGRAMA Y BIBLIOGRAFIA: Adjuntas a esta hoja

FECHA: 15/09/96

Firma del Profesor

Firma del Director

Dr Jordi Duch y Roson

N1 "CRIPTOGRAFÍA"

Horario: 19 a 22 hs.

PROFESOR: Dr. Jordi Quer i Bosor

Es Doctor en Ciencias Matemáticas de la Universidad Autónoma de Barcelona. Es profesor titular de dicha Universidad en la Facultad de Informática de Barcelona, donde dicta Criptografía, Teoría de la Información y la Codificación.

PROGRAMA:

Este curso pretende introducir las ideas básicas de la criptografía y mostrar sus aplicaciones. Por su contenido y objetivos esta indicado para estudiantes y titulados univeristarios de informática, telecomunicaciones y matemáticas.

INTRODUCCION.

Criptología clásica y criptología moderna. Criptología, Criptografía y Criptoanálisis.Seguridad en informática y comunicaciones: Autenticación, Control de Acceso, Confidencialidad,Integridad, No Repudio. Técnicas básicas de criptografíaTransformaciones de cifrado-descifrado,apéndices y firmas digitales. Criptología de clave privada y de clave pública.

Criptografía clásica.

Substitución mono y polialfabética. Transposición. Cifrados de Cesar, de Vigenere, de Vernam. Máquinas de rotores: Enigma.Teoría de la seguridad perfecta de Shanon. Distancia de unicidad.

Técnicas modernas de clave privada.

Cifrado en bloque y cifrado en flujo.Modos de operación para sistemas de cifrado en bloque: ECB, CBC, CFB, OFB.El Data Encryption Standard: Descripción, Historia, Estandarización, Criptoanálisis.Otros sistemas de cifrado en bloque:Skipjack, IDEA, ...Generadores pseudoaleatorios para cifrado en flujo.

Aritmética computaciones.

Operaciones aritméticas en multi-precisión. Algoritmo de Euclídes. Congruencias. Teorema chino del resto. Aritmética modular. Exponenciación modular.Residuos cuadraticos. Cálculo de raíces cuadradas. Símbolos de Legendre y Jacobi. Ley de Reciprocidad Cuadrática.

Números primos. Criterios de primalidad probabilísticos. Teorema del número primo y consecuencias.Generación aleatoria de números primos.El problema computacional de la factorización de números enteros.Estado actual y perspectivas.

Funciones unidireccionales.
Conceptos de función unidireccional y de puerta trampa.
Relación con la Teoría de la Complejidad.
Función potencia $y=x^r$. Puerta trampa.
Extracción de raíces. Función $y=x^2$. Puerta trampa.
Función exponencial discreta.
El problema del logaritmo discreto.
Variantes sobre cuerpos finitos.
El problema de la mochila.

Sistemas de clave pública.
Criptosistema RSA (Rivest, Shamir, Adleman).
Variante de Rabin-Williams.
Criptosistema de ElGamal. Cifrado y Firma.
Variante de Schnorr.
Sistema de Diffie y Hellman para distribución de claves.
Criptosistema Knapsack. Criptoanálisis de Shamir.

Técnicas criptográficas.
Transformaciones de cifrado y descifrado.
Sistemas mixtos de clave privada y clave pública.
Funciones Hash Criptográficas. Secure Hash Standard.
Firmas digitales. Digital Signature Standard.
Generación y distribución de claves.
Certificados de Claves Públicas.
Autoridades Certificadoras.
Esquemas de identificación.

Criptografía en el mundo real.
Principales campos de aplicación.
Implementaciones. Perspectivas de futuro.
Estandarización. Organismos Implicados.
Patentes.
Implicaciones ético-sociales. Control estatal. La situación en USA:
Proyecto Capstone y chip Clipper.Leyes de exportación (USA).

PREREQUISITOS: No tiene prerrequisitos especiales aunque se suponen la madurez matemática que se adquiere en los primeros cursos de cualquier carrera universitaria técnica y algunos conocimientos de aritmética elemental. Asimismo es conveniente una cierta familiaridad con el análisis de algoritmos.

Este curso se dictará en español.

Bibliografía: No se especifica