Comp. 2000
19

CARAL.DOC

UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación

2. CUATRIMESTRE: Segundo de 2000

3. ASIGNATURA: Seminario de Criptografía

4. CARRERA: Licenciatura en Ciencias de la Computación

5. CARACTER DE LA MATERIA: (Optativa)

6. NUMERO DE CODIGO DE CARRERA: 18

7. NUMERO DE CODIGO DE MATERIA: C .....

8. PUNTAJE: 3

9. PLAN DE ESTUDIOS AÑO: (1987 y 1993)

10. DURACION DE LA MATERIA: cuatrimestral

11. HORAS DE CLASE SEMANAL:

a)TEORICAS: 1 hs c)PRACTICAS: hs

b)LABORATORIO: 2 hs d)SEMINARIOS: 3 hs

12. CARGA HORARIA TOTAL: 6 90hs CUATRIMESTRALES

13. ASIGNATURAS CORRELATIVAS: ALGORITMOS Y ESTRUCTURA de DATOS I (PLAN '93)
LABORATORIO II - PROGRAMACIÓN de COMPUTADORES I (PLAN '87)

14. FORMA DE EVALUACION: (Promoción)

15. PROGRAMA Y BIBLIOGRAFIA: Adjuntas a esta hoja.

16. DOCENTES Hugo D.Scolnik

Fecha: 29 Junio 2000

Dra. PATRICIA [illegible]
DIRECTORA
DEPTO. DE COMPUTACION
F. C. E. y N. UBA

CARAL.DOC

Dr HUGO SCOLNIK

Programa de la materia Seminario de Criptografía
Hugo D.Scolnik
Segundo cuatrimestre de 2000

Objetivo: estudiar temas avanzados de Criptografía, y que no se cubren en la materia Criptología. Los mismos incluyen a algunos de los trabajos de investigación actuales, ajenos y los de nuestra Facultad.

Dirigida a: Licenciaturas en Computación y Matemática

1. Resultados sobre primalidad

Cotas clásicas para el número de primos. Los resultados de Pierre Dusart y la demostración de Milton Brown de la conjetura de Goldbach (Junio 2000).
Fórmulas de Meissel, Lehmer, Gauss, Legendre. La función de Chebyshev y la función zeta de Riemann.
Primos gemelos, cadenas de Cunningham, Mersenne, Fermat, Sophie Germain.
Tests alternativos de primalidad. Certificados de primalidad. Teorema de Lehmer-Pocklington, Teorema de Lenstra.

2. Métodos modernos de factorización.

Algoritmos de cribado. Métodos de Euler, Gauss, Legendre, Erdos-Kac, variaciones. Algoritmo de Pollard. Modificación de Brent. Métodos de fracciones continuas.Criba cuadrática. Criba cuadrática múltiple. Curvas elípticas. Método de Lenstra. El método NFS (Number Field Sieve) y GNFS (General Number Field Sieve)
Números primos y criptografía. Puntos fijos de RSA
Algunos resultados nuevos sobre residuos cuadráticos y su relación con la factorización para atacar RSA.

3. Software actual

Bibliotecas para teoría de números. Software para primalidad :Certifix 0.5, Proth, WinBiTwin 1.0

Bibliografía:

1. Hans Riesel, Prime Numbers and Computer Methods for factorization, Birkhäuser, 1994
2. Neal Koblitz, Algebraic Aspects of Cryptography, Springer-Verlag, 1997
3. Neal Koblitz, A Course in Number Theory and Cryptography, Second Edition, Springer- Verlag, 1994
4. S.C.Coutinho, The Mathematics of Ciphers – Number Theory and RSA Cryptography, A.K.Peters, 1999.

Dra. PATRICIA BORENSZTEJN
DIRECTORA
DEPTO. DE COMPUTACION
F. C. E. y N. UBA