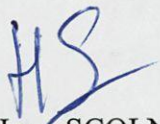
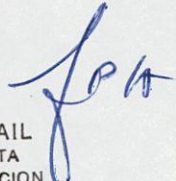


UNIVERSIDAD DE BUENOS AIRES  
FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación
  2. CUATRIMESTRE: 1ero. del 2000
  3. ASIGNATURA: **Criptología**
  4. CARRERA: Licenciatura en Ciencias de la Computación
  5. CARÁCTER DE LA MATERIA: optativa
  6. NUMERO DE CODIGO DE CARRERA: 18
  7. NUMERO DE CODIGO DE MATERIA: C038
  8. PUNTAJE: 3
  9. PLAN DE ESTUDIOS AÑO: 1993 y 1987
  10. DURACION DE LA MATERIA: Cuatrimestral
  11. HORAS DE CLASE SEMANAL:
    - a) TEORICAS/PRACTICA: 7hs
    - b) LABORATORIO:
    - c) PROBLEMAS:
    - d) SEMINARIOS: -----
  12. CARGA HORARIA TOTAL: 7hs
  13. ASIGNATURAS CORRELATIVAS: Algebra – Programación de Computadores II-  
Laboratorio II (Plan 87)      Algebra-Algoritmos y estructura de Datos I (Plan 93)
  14. FORMA DE EVALUACION: parciales y final
  15. PROGRAMA Y BIBLIOGRAFIA: Adjuntas a esta hoja
- FECHA: mayo del 2000

  
Dr. Hugo SCOLNIK  
Firma y Aclaración  
del Profesor

Firma del Director  
y Sello Aclaratorio

  
Dra. MARTA MEJAIL  
DIRECTORA ADJUNTA  
DEPTO. DE COMPUTACION  
F. C. E. y N. UBA

# Criptología

- .1. Criptografía clasica.
  - . Cifrados de corrimiento, substitucion, afin, Vigenere, Hill y de flujo.
- .2. Criptoanálisis.
  - . Criptoanálisis de los metodos afin, de substitucion y de Vigenere.
- .3. La teoria de Shannon.
  - . Teoria de la informacion. Teoria de la complejidad.
  - . Secreto perfecto. Entropia. Codificacion de Huffman y Entropia.
  - . Propiedades.
- .4. Algoritmos simetricos.
  - . Funciones univocas. Funciones de hashing.
  - . DES (Data Encryption Standard). Descripcion. Controversias.
  - . Criptoanálisis diferencial.
  - . Otros algoritmos de bloques. Criptografía de flujo.
- .5. Criptografía de clave publica.
  - . El problema de la distribucion de claves. Elementos de teoria de numeros. El algoritmo de Diffie-Hellman.
  - . Generacion probabilistica de numeros primos. Los metodos de Solovoy-Strassen y Rabin-Miller. Nuevos resultados sobre el error.
  - . El algoritmo RSA (Rivest-Adleman-Shamir). Ataques. Metodos de factorizacion.
  - . Implementacion computacional. Demostraciones de software.
- .6. Otros metodos de clave publica.
  - . El problema del logaritmo discreto. El algoritmo de ElGamal.
  - . Cuerpos finitos y curvas elipticas. Cuerpos de Galois.
  - . El problema de la mochila.
- .7. Firmas digitales y funciones de hashing.
  - . El algoritmo DSA (Digital Signature Algorithm).
  - . Las funciones MD4, MD5, y SHA. Time stamps. Implementaciones.
  - . Autoridades certificantes. Esquemas operativos.

.8. Temas complementarios.

- . Generacion de numeros aleatorios. Tests. Criptografia probabilistica.
- . Time attacks.
- . Pruebas de conocimiento cero.
- . Politica de exportacion de Estados Unidos. Seguridad en Internet.

.Bibliografia:

- .Douglas Stinson," Cryptography, Theory and Practice", CRC Press Inc., Florida, USA, 1995.
- .Bruce Schneier," Applied Cryptography", Second Edition, J.Wiley, 1996.

-----  
.Nota: se utilizaran diversos articulos de revistas segun las posibilidades y perfiles de los alumnos.  
-----

- . Teoricas: 3 horas semanales.
- . Practicas: 3 horas semanales.

Hugo D.Scolnik

  
Dra. MARTA MEJAIL  
DIRECTORA ADJUNTA  
DEPTO. DE COMPUTACION  
F. C. E. y N. UBA

Mitra Sitansu "Principles of Relational Databases" Prentice-Hall International editions [1991]

Muggleton S. "Learning of positive data"  
Proceedings of the 6<sup>th</sup> International workshop on Inductive Logic programming [1996]

Muggleton S. & De Raedt L. "Inductive Logic Programming: Theory and Methods"  
Journal of Logic Programming 19 [1994]

Muggleton S. "Inverse entailment and Progol"  
New generation Computing 13 [1995]

Muggleton S. & Feng C. "Efficient Induction of Logic Programming"  
Inductive Logic Programming Academic Press - London [1992]

Nienhuys-Cheng Shan-Hwei & de Wolf Ronald "A complete method for program specialization based on unfolding"  
Proceedings of the 12<sup>th</sup> European Conference on Artificial Intelligence (ECAI-96) [1996]

Nienhuys-Cheng Shan-Hwei & de Wolf Ronald "Foundations of Inductive Logic Programming"  
Springer [1997]

Nilsson Nils "Problem-solving Methods in Artificial Intelligence"  
McGRAW-HILL [1971]

Ullman Jeffrey "Principles of Database and Knowledge-base Systems" Vol I, II  
Computer Science Press [1995]

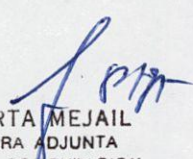
Parsaye Kamran et Al "Intelligence Databases"  
Wiley Professional Computing [1989]

Poggi Eduardo "Curso de Machine Learning"  
Departamento de Computación UBA [1988]

Quinlan J.R. "Induction of Decision trees"  
Morgan Kaufmann Publishers "Reading in Machine Learning" [1990]

Quinlan J.R. "Programs of Machine Learning"  
Morgan Kaufmann Publishers [1993]

Tamaki H. & Sato T. "Unfold/Fold transformation of logic programs"  
Proceedings of the 2nd International Logic Programming Conference. Uppsala [1984].

  
Dra. MARTA MEJAIL  
DIRECTORA ADJUNTA  
DEPT. DE COMPUTACION  
F. C. E. y N. UBA