C 2006.
(42)

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Planilla a completar para presentación de Cursos de Posgrado

1.- DEPARTAMENTO de COMPUTACION.....

2.- NOMBRE DEL CURSO: **Criptografía**

3.- DOCENTES:

RESPONSABLE/S: **Dr. Hugo Scolnik**
COLABORADORES:.....
AUXILIARES:.....

4.- CARRERA de DOCTORADO

5.- AÑO: 2006..... CUATRIMESTRE/S: 1° y 2° 2006

6.- PUNTAJE PROPUESTO PARA CARRERA DE DOCTORADO: 3 (tres) puntos

7.- DURACIÓN (anual, cuatrimestral, bimestral u otra): un cuatrimestre

8.- CARGA HORARIA SEMANAL:

Teóricas:..3hs.....
Problemas:.....
Laboratorio:..3 hs.....
Seminarios:.....
Teórico – Práctico:.....
Salida a Campo:.....

9.- CARGA HORARIA TOTAL: 96 hs.....

10.- FORMA DE EVALUACIÓN: 2 Parciales, Trabajos Prácticos y examen final

11.- PROGRAMA ANALÍTICO (adjuntarlo).

12.- BIBLIOGRAFÍA (indicar título del libro, autor, Editorial y año de publicación)(adjuntada)

Criptografia

11.- PROGRAMA ANALÍTICO (adjuntarlo).

Objetivo:

12.- BIBLIOGRAFÍA (indicar título del libro, autor, Editorial y año de publicación)

WDouglas R. Stinson
"Cryptography, Theory and Practice "CRC Press , 1995.

G. Simmons (editor)
"Contemporary Cryptology, The Science of Information Integrity" IEEE Press, 1992.

A.J. Menezes, P.C. van Oorschot y S.A. Vanstone
"Handbook of Applied Cryptography" CRC Press, 1997.

Bruce Schneier
"Applied Cryptography, Protocols, Algorithms and Source Code in C " J.Wiley - Second Edition, 1996.

Michael Luby
"**Pseudorandomness and Cryptographic Applications,** Vol. 1" Princeton University Press, 1996.

U.Maurer (editor)
"**Advances in Cryptology - Eurocrypt 96"** Lecture Notes in Computer Science, Springer-Verlag, 1996.

D. E. Knuth
"The Art of Computer Programming, Vol. 2, Seminumerical Algoritms" Addison Wesley Reading, 1981.

Balcazar - Diaz - Gabarro
"**Complexity Theory"**

I. Niven and H. Zuckerman
"**An Introduction to the Theory of Numbers"** J.Wiley - Fourth Edition, 1980.

E. Kranakis
"**Primality and Cryptography** " Wiley - Teubner Series in Computer Sciences 1986.

N. Koblitz
"**A Course in Number Theory and Cryptography"** Springer, 1994.

N. Koblitz
"**Algebraic Aspects of Cryptography"** Springer, 1998.

F. L. Bauer
"**Decrypted Secrets,** Methods and Maxims of Cryptology "Springer , 1997.

A. Salomaa
"**Public-Key Cryptography** " Springer. Second Edition, 1996.

E. Bach and J. Shallit
"**Algorithmic Number Theory,**Vol. 1" The MIT Press, 1996.

J. Seberry and J. Pieprzyk
"**Cryptography: An Introduction to Computer Security**"Prentice Hall , 1989.

W. Stallings
"**Network and Internetwork Security, Principles and Practice** "IEEE Press, 1995.

O. Goldreich
"**Modern Cryptography, Probabilistic Proofs and Pseudo-randomness** " Springer, 1999.

D. E. Flath
"**Introduction to Number Theory**" Wiley Interscience , 1989.

H. Cohn
"**Advanced Number Theory** "Dover, 1962.

. Diffie and ME Hellman,
"New Directions in Cryptography",
IEEE Transactions on Information Theory, IT-22 no 6 (November 1976) p. 644--654.

R. Rivest, A. Shamir, and L. Adleman,
"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",
CACM 21, pp. 120--126, Feb. 1978.

A. Shamir,
"How to Share a Secret",
CACM 22, pp. 612--613, November 1979.

PIA
DC Alejandro Ríos

FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE COMPUTACION
U. B. A.