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: 2007..... CUATRIMESTRE/S: 2° 2007

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).

Es una materia optativa que presenta aplicaciones computacionales importantes, de gran aplicabilidad y con uso de teoría no trivial
Esta materia ha sido la primera en el país dedicada a la Criptografía, e incluye firmas digitales, protocolos de seguridad, métodos de autenticación remota, etc.

El objetivo es formar a los alumnos en todo lo referente a la Criptografía y sus aplicaciones.

1)Introducción. Algunos sistemas criptográficos simples (corrimiento, substitución, afín, Vigénere, Hill, permutación, de flujo) y su criptoanálisis.

2)La teoría de Shannon. Secreto perfecto. Entropía. Propiedades.

3)Métodos simétricos. El Data Encryption Standard (DES). Modos de operación. Controversias. Idea del criptoanálisis diferencial. Otros métodos.

4)Teoría de funciones de hashing. Firmas, hashings libres de colisiones, timestamping.

5)Criptografía de clave pública. El concepto de firma digital. El método de intercambio de claves de Diffie- Hellman.
Teoría de números. El algoritmo de Euclides y su extensión. El teorema del resto chino. El método RSA. Tests de pseudoprimalidad. Implementaciones. Ataques. Métodos de factorización modernos. Otros métodos de clave pública (El Gamal, curvas elípticas).

6)Esquemas de firmas (El Gamal, Digital Signature Standard). Esquemas de identificación. Códigos de autenticación. Certificados digitales.

7)Generación de números pseudoaleatorios.

8) Pruebas de conocimiento cero.

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.

Subcomisión de Doctorado
Alejandro Ríos

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Referencia Expte. Nº 487.713/2006

Buenos Aires, 10 SET 2007

VISTO:

la nota presentada por el Dr. Alejandro Ríos, representante de la Subcomision de Doctorado en la Comision de Doctorado de esta Facultad por el Departamento de Computación, mediante la cual eleva la Información y el Programa del Curso de Posgrado **CRIPTOGRAFIA**, que será dictado durante el **segundo cuatrimestre de 2007** por el Dr. Hugo Scolnik

CONSIDERANDO:

lo actuado por la Comision de Doctorado de esta Facultad

lo actuado por la Comisión de Enseñanza, Programas, Planes de Estudio y Posgrado

lo actuado por este Cuerpo en la sesión realizada en el día de la fecha,

en uso de las atribuciones que le confiere el Artículo 113º del Estatuto Universitario,

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS Y NATURALES
R E S U E L V E:

Artículo 1º: Autorizar el Dictado del Curso de Posgrado **CRIPTOGRAFIA**, de 96 hs. de duración.

Artículo 2°: Aprobar el Programa del Curso de Posgrado **CRIPTOGRAFIA.**

Artículo 3º: Aprobar un puntaje de tres (3) puntos para la Carrera del Doctorado.

Artículo 4°: Aprobar un arancel de 20 Mód ulos. Disponer que los montos recaudados serán utilizados conforme a lo dispuesto por Resolución CD Nº 072/03.

Artículo 5°: Comuníquese a la Direccion del Departamento de Computación, a la Biblioteca de la FCEyN y a la Subsecretaría de Postgrado (con fotocopia del Programa incluido)

Resolución CD Nº 1982

Dra. MATILDE RUSTICUCCI
SECRETARIA ACADEMICA ADJUNTA

Dr. JORGE ALIAGA
DECANO