Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Planilla a completar para presentación de Cursos de Posgrado

1.- DEPARTAMENTO de COMPUTACIÓN

2.- NOMBRE DEL CURSO: Criptografía

3.- DOCENTES:

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

4.- CARRERA de DOCTORADO

5.- AÑO: 2012 CUATRIMESTRE/S: 1 y 2

6.- PUNTAJE PROPUESTO PARA CARRERA DE DOCTORADO: 4 puntos

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

8.- CARGA HORARIA SEMANAL:

Teóricas: .....
Problemas: .....
Laboratorio: 2.....
Seminarios: .....
Teórico – Práctico: 4.....
Salida a Campo: .....

9.- CARGA HORARIA TOTAL: 96

10.- FORMA DE EVALUACIÓN: Parciales, trabajos de laboratorio, final

11.- PROGRAMA ANALÍTICO:

El problema de la factorización de enteros. Métodos clásicos y modernos. Nuevos algoritmos desarrollados en la facultad, problemas abiertos.
Algoritmos para resolver el problema del logaritmo discreto. Nuevos resultados.

Nuevos tests de seudoprimalidad. Problemas abiertos.

12.- BIBLIOGRAFÍA:

Douglas 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.

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.

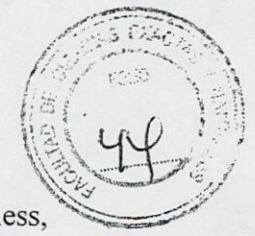
F. L. Bauer, Decrypted Secrets, Methods and Maxims of Cryptology, Springer, 1997.

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.

Artículos Clásicos

W. 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.

Dra Paula Zabala
Depto. de Computación
F.C.E.N. - U.B.A.

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Referencia Expte. Nº 487.713/2006

Buenos Aires, 04 JUN 2012

VISTO:

la nota presentada por la Dra. Paula Zabala del Departamento de Computación, mediante la cual eleva la Información y el Programa del Curso de Posgrado **CRIPTOGRAFIA**, que se dicta en el primer y segundo **de 2012** por el Dr. Hugo Scolnik

CONSIDERANDO:

lo actuado por la Comision de Doctorado de esta Facultad el 02/05/2012,

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 2º: Aprobar el Programa del curso de posgrado **CRIPTOGRAFIA** obrante a fs 42 a 44 del expediente de la referencia.

Artículo 3º: Aprobar un puntaje de cuatro (4) puntos para la Carrera del Doctorado.

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

Artículo 5º: Comuníquese a la Dirección del Departamento de Computación, a la Biblioteca de la FCEyN y a la Subsecretaría de Postgrado (con fotocopia del Programa incluido). Cumplido Archívese

Resolución CD Nº 1121
SP/med 02/05/2012

Dr. JORGE ALIAGA
DECANO

Dr. JAVIER LÓPEZ DE CASENAVE
SECRETARIO ACADEMICO