No folio
COMP_2008
(9)

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: 2008..... CUATRIMESTRE/S: 1º 2008

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

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

8.- CARGA HORARIA SEMANAL:

Teóricas:.....
Problemas:.....
Laboratorio:.....
Seminarios:.....
Teórico – Práctico: 6hs.....
Salida a Campo:.....

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

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

11.- PROGRAMA ANALÍTICO (adjuntarlo).

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

Criptografía

11.- PROGRAMA ANALÍTICO (adjuntarlo).

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.

Bibliografía:

No fue adjuntada por el docente.

Dr. Alejandro N. Ríos
Departamento de Computación
FCEyN UBA

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Referencia Expte. Nº 487.713/2006

Buenos Aires, 21 JUL 2008

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 **primer cuatrimestre de 2008** por el Dr. Hugo Scolnik

CONSIDERANDO:

lo actuado por la Comision de Doctorado de esta Facultad el 02/07/08

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.**

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

Artículo 4º: 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 5º: 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). Cumplido Archivese

Resolución CD Nº —1607—
SP/med 03/07/2008

Dra. NORA CEBALLOS
SECRETARIA ACADEMICA

Dr. JORGE ALIAGA
DECANO