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: Computación y Privacidad

3.- DOCENTES:

RESPONSABLE/S: Frédéric Prost.
COLABORADORES:
AUXILIARES:

4.- CARRERA de DOCTORADO

5.- AÑO: 2015 CUATRIMESTRE/S: SEGUNDO

6.- PUNTAJE PROPUESTO PARA CARRERA DE DOCTORADO: ½ punto.

Dr. JOSE OSCAR PANTANO
SECRETARIO DE POSGRADO
FCEN - UBA

7.- DURACIÓN (anual, cuatrimestral, bimestral u otra): **1 semana**

8.- CARGA HORARIA SEMANAL: 15 hs.

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

9.- CARGA HORARIA TOTAL:15**hs**

10.- FORMA DE EVALUACIÓN: Examen individual domiciliario.

11.- PROGRAMA ANALÍTICO:

1- Introducción:
1.1- La criptografía no es suficiente: ejemplos históricos (Enigma code-breaking, varios ataques a protocolos criptográficos, desanonimización).
1.2- Protocolo Shamir y aplicaciones.
1.3- Teoría de la información y criptografía.

2- Formalizando identidad y anonimato:
2.1- Esquemas de certificación de identidad.
2.2- Midiendo el anonimato.
2.3- Privacidad diferencial.
2.4- Algoritmo de Chaum para comunicaciones anónimas (enrutamiento de la cebolla).

Ataques a esquemas anónimos en teoría y en práctica.

3- Propiedad de no-interferencia:
3.1- Formalizando el flujo de información en programas: distintas definiciones de análisis estático de no interferencia en diferentes paradigmas (funcional, imperativo y cálculo concurrente).

4- Prueba de conocimiento nulo:
4.1- Prueba interactiva de identidad sin revelar ID.
4.2- Prueba no interactiva conocimiento nulo.
4.3- Análisis estático de protocolos de conocimiento nulo.

5- Evidencia formal para protocolos elaborados:
5.1- Voto electrónico.
5.2- Dinero electrónico.
5.3- Lista negra anónima.

12.- BIBLIOGRAFÍA:

F. Prost. Enforcing dynamic interference policy. In Proceedings of the third IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-11), 2011.
Goldwasser, S.; Micali, S.; Rackoff, C. "The Knowledge Complexity of Interactive Proof Systems". SIAM J. Comput. 18 (1): 186–208.
Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2):120–126. 1978.
Chaum, D. L. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM24 (2): 84. 1981
Weldemariam, K., et al., Formal analysis of an electronic voting system: An experience report. J. Syst. Software (2011).
Ryan Henry and Ian Goldberg. 2011. Formalizing Anonymous Blacklisting

Con 2015

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales

Referencia Expte. N° 504.989 vinc 01

Buenos Aires, - 3 AGO 2015

VISTO:

la nota presentada por el Dr. Esteban Feuerstein, Director del Departamento de Computación, mediante la cual eleva la información y el programa del curso de posgrado **Computación y privacidad,** que será dictado durante 2015 por el Dr. Frédéric Prost,

CONSIDERANDO:

lo actuado por la Comisión de Doctorado,

lo actuado por la Comisión de Postgrado,

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 1°: Autorizar el dictado del curso de posgrado **Computación y privacidad** de 15 hs. de duración.

Artículo 2°: Aprobar el programa del curso de posgrado **Computación y privacidad**, obrante a fs 2 a 4 del expediente de la referencia.

Artículo 3º: Aprobar un puntaje máximo de medio (0,5) punto para la Carrera del Doctorado.

Artículo 4°: Comuníquese a la Dirección del Departamento de Computación, a la Biblioteca de la FCEyN (con fotocopia del programa incluido) y a la Secretaría de Postgrado (sin fotocopia del programa). Cumplido Archívese.

RESOLUCION CD Nº 1855
SP/ga 27/07/2015

Dr. JOSE OLABE IPARRAGUIRRE
SECRETARIO DE POSGRADO
FCEN - UBA

Dr. LUIS M. BARALDO VICTORICA
VICEDECANO