1821 Universidad de Buenos Aires

Resolución Consejo Directivo

Número: RESCD-2024-98-E-UBA-DCT#FCEN

CIUDAD DE BUENOS AIRES
Martes 27 de Febrero de 2024

Referencia: EX-2023-06529998- -UBA-DMESA#FCEN - POSTGRADO - SESIÓN 14/02/2024

VISTO:

La nota presentada por la Dirección del Departamento de Computación, mediante la cual eleva la información del curso de posgrado Introducción a la Criptografía Moderna para el año 2024,

CONSIDERANDO:

lo actuado por la Comisión de Doctorado,

lo actuado por este Cuerpo en la sesión realizada en el día de la fecha 14 DE FEBRERO DE 2024

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: Aprobar el nuevo curso de posgrado Introducción a la Criptografía Moderna de 32 horas de duración, que será dictado por el Dr. Fernando Virdia con la colaboración del Dr. Ricardo Oscar Rodríguez.

ARTÍCULO 2°: Aprobar el programa del curso de posgrado Introducción a la Criptografía Moderna que como anexo forma parte de la presente Resolución, para su dictado en el primer bimestre de 2024.

ARTÍCULO 3°: Aprobar un puntaje máximo de un y medio (1,5) puntos para la Carrera del Doctorado.

ARTÍCULO 4°: Establecer un arancel de CATEGORÍA 2, estableciendo que dicho arancel estará sujeto a los descuentos y exenciones estipulados mediante la Resolución CD N.º 1072/19. Disponer que los fondos recaudados ingresen en la cuenta presupuestaria habilitada para tal fin, y sean utilizados de acuerdo a la Resolución 072/03

ARTÍCULO 5°: Disponer que, de no mediar modificaciones en el programa, la carga horaria y el arancel, el presente Curso de Posgrado tendrá una vigencia de cinco (5) años a partir de la fecha de la presente Resolución.

ARTÍCULO 6º: Comuníquese a todos los Departamentos Docentes, a la Dirección de Estudiantes y Graduados, a la Biblioteca de la FCEyN y a la Secretaría de Posgrado con copia del programa incluida. Cumplido, pase COMPUTACION#FCEN y resérvese.

ANEXO

PROGRAMA

● Proporcionar a los estudiantes una visión de la funcionalidad criptográfica necesaria para lograr comunicaciones cifradas básicas de uno a uno a través de Internet.

● Mostrar el modelado de amenazas criptográficas y las formas sutiles en que el diseño criptográfico puede fallar.

● Demostrar cómo tratar formalmente las primitivas criptográficas para demostrar garantías de seguridad a través de teoremas.

Temario:

El temario está dividido en 12 componentes, que llevarán los estudiantes de no tener bases en criptografía, a conocer los componentes basilares requeridos para comunicaciones confidenciales por internet. Idealmente, cada tema requiere unas 2 horas de clase, totalizando unas 24 horas. Seis horas extra pueden ser utilizadas en caso algún tema requiera más tiempo del previsto.

Criptografía simétrica (o “de clave secreta”)

1. Repaso sobre probabilidad, introducción de: la noción de secreto perfecto, el cifrado de un solo uso (One-Time Pad), teorema de Shannon.

2. Juegos de seguridad, definición de generador de números pseudoaleatorios (PRG), noción formal de seguridad de PRG, definición de cifrado de flujo y de seguridad semántica, construcción de cifrado de flujo semánticamente seguro similar a OTP usando un PRG.

3. Definición de cifrado de bloque, noción de seguridad IND-CPA, demostración de seguridad del modo de uso CTR.

4. Funciones hash, códigos de autenticación de mensajes (MAC), noción seguridad

MAC, HMAC con esbozo de prueba.

5. Maleabilidad de cifradores de flujo similares a OTP, noción de seguridad AE. Cifrario Encrypt-then MAC (EtM), demostración de que EtM proporciona un esquema AE-seguro, discusión de la noción de seguridad IND-CCA y su equivalencia con la seguridad AE.

Criptografía asimétrica (o “de clave pública”)

6. Distribución de claves secretas: el artículo "New Directions" y la criptografía de clave pública; hipótesis de complejidad computacional CDH.

7. Definición de mecanismo de encapsulado de claves (KEM), definición de seguridad semántica KEM, hipótesis DDH, KEM de ElGamal, demostración que Elgamal es seguro IND-CPA basado en DDH.

8. Ataques de cifrado elegido en KEMs, noción de seguridad KEM IND-CCA.

9. Oráculos aleatorios y transformación KEM CPA -> KEM CCA con demostración (si el

tiempo lo permite, puede ser la prueba más difícil hasta ahora y requiere el Modelo de Oráculo Aleatorio; podría también tratarse solo de manera intuitiva).

10. Ataques máquina-en-el-medio (MITM) y la necesidad de autenticación de claves públicas, firmas digitales, infraestructura de claves públicas (PKI).

11. Noción de seguridad de inalterabilidad (“existential unforgeability”, UF-CMA), funciones de puerta trasera, función RSA.

12. Firmas de dominio completo de hash (“Full-Domain Hash”, FDH), argumento intuitivo sobre la seguridad de firmas FDH, (y demostración si el tiempo lo permite).

Reflexiones finales: ¿hemos terminado? Realmente, no. Por ejemplo, para construir canales privados uno a uno prácticos, hay muchos problemas respecto al identificar contactos. ¡Este es un problema de investigación abierto!

BIBLIOGRAFÍA

El material del curso es estándar, y se puede encontrar tratado en varios libros de texto. Los recomendados (y usados para preparar las clases) serán:

1. Dan Boneh and Victor Shoup, "A Graduate Course in Applied Cryptography", auto editado y de libre acceso en https://toc.cryptobook.us (2023)

2. Nigel Smart, “Cryptography, an Introduction”, Third Edition, auto editado y de libre acceso en https://nigelsmart.github.io/Crypto_Book/ (2016)

3. Mike Rosulek, "The Joy of Cryptography", auto editado y de libre acceso en https://joyofcryptography.com (2021)

4. Jonathan Katz and Yehuda Lindell, “Introduction to Modern Cryptography”, Tercera Edicion, CBC Press, (2020)

5. Un artículo científico que va a ser también tratado (y que se puede recuperar de manera gratuita):

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on information theory, 22(6), 644-654.

Copia disponible en https://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

Digitally signed by MARTI Marcelo Adrian
Date: 2024.02.27 12:13:19 ART
Location: Ciudad Autónoma de Buenos Aires

Marcelo Marti
Secretario
Secretaría de Posgrado
Facultad de Ciencias Exactas y Naturales

Digitally signed by DURAN Guillermo Alfredo
Date: 2024.02.27 12:30:12 ART
Location: Ciudad Autónoma de Buenos Aires

Guillermo Alfredo Duran
Decano
Decanato
Facultad de Ciencias Exactas y Naturales

Digitally signed by GDE UBA
Date: 2024.02.27 12:30:17 -03:00