

## **Introducción a la Criptografía Moderna.**

Dr. Fernando Virdia. Profesor Visitante. DC-FCEN-UBA. Doctor en Ciencias de la Computación con la colaboración del Dr. Ricardo Oscar Rodríguez (Profesor regular Asociado dedicación Exclusiva.)

### **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 basales 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  $\rightarrow$  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 at [https://nigelsmart.github.io/Crypto\\_Book/](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 Edición, CBC Press, (2020)

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

1. 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>