Criptografía Moderna

Fundamentos:

Si bien la criptografía es un campo de estudio antiguo, el surgimiento de la criptografía moderna en las últimas décadas se caracteriza por diversos e importantes rasgos que la distinguen de la criptografía clásica. Para empezar, la disponibilidad de computadoras y la gran extensión de sistemas de información en red y de la Web, ha incrementado dramáticamente tanto la necesidad de criptografía sólida como las posibilidades de lo que puede ofrecer.
Sumado a las aplicaciones clásicas en materia militar y de seguridad, han emergido diversas aplicaciones criptográficas en cuestiones financieras, legales y sociales, desde las más generalizadas como proteger las comunicaciones por internet y pagos online, hasta las más ambiciosas metas del comercio electrónico – en particular, criptomonedas, voto electrónico, firmado electrónico de contratos, Aprendizaje Automático que preserve la privacidad, etc.

Objetivos:

Los objetivos de este curso intensivo corto son dos: Primero, proveer los fundamentos científicos basicos de la disciplina, para luego abarcar una selección de áreas de investigación activas, incluyendo contraseñas intercambio de contraseñas y protocolos de derivación, cómputo grupal seguro, soporte homomórfico secreto para compatir, y fundaciones y aplicaciones de protocolos blockchain.
El curso sera dictado por expertos en el campo de investigación provenientes de prestigiosas universidades e institutos de investigación, lo que nos lleva al segundo objetivo, además de la diseminación del conocimiento, de promover la colaboración e interacciones de investigación entre los docentes y los estudiantes locales.

Programa:

1. Introducción a la criptografía moderna.
2. Diseño y análisis de protocolos de autenticación por intercambio de clave.
3. Secure Multi-Party Computation.
4. Homomorphic Secret Sharing y aplicaciones.
5. Fundamentos y aplicaciones de protocolos basados en blockchain.