EDUCACIÓN IT

Criptografía y Blockchain

Programa de Estudio

Criptografía y Blockchain

Comprende hasta qué punto utilizamos día a día algoritmos criptográficos. Domina las técnicas de cifrado de datos y conviértete en un experto en Blockchain.

Contenido del curso

El curso comienza con la historia de la Criptografía desde sus comienzos, analizando tanto la técnica por transposición como la de sustitución. Se aprenderán algoritmos que dieron comienzo a la criptografía y se verán las debilidades que tienen las mismas y cómo, por medio del Criptoanálisis, pueden romperse algunos algoritmos rápidamente. Una vez comprendido cómo se cifraba hasta mediados del siglo pasado, veremos cómo se cifra en la actualidad.
Se introducirá al alumno en la Criptografía Simétrica analizando sus virtudes y sus debilidades; comprendiendo, a partir de la práctica el funcionamiento de la misma. Luego se abordará la Criptografía Asimétrica, con sus pros y contras.

Tratando tanto algoritmos útiles para cifrar como algoritmos que permitirán la generación de claves en entornos que no son seguros. Seguidamente se trabajará con los algoritmos de HASH, tratando también los distintos ataques existentes sobre los mismos. También se interiorizará al alumno en el uso del concepto de cifrado al vuelo y en la práctica de la Esteganografía, sus usos y costumbres. Habiendo adquirido los conocimientos anteriores se verá cómo es el funcionamiento de una Infraestructura de Clave Pública y sus uso más comunes. Para finalizar viendo cómo a partir de la criptografía surge el concepto de Blockchain y su uso para muchas criptomonedas.

::PRÁCTICAS EN CLASE ::
A lo largo del curso realizaremos distintas prácticas basadas en casos reales. Desde laboratorios, aplicando criptografía clásica, en donde el alumno deberá no sólo descifrar textos brindados por el instructor, a partir de una clave dada, sino también romperlos utilizando criptoanálisis. Pasada la parte manual, y habiendo comprendido las bases de la Criptografía, se comenzará con el uso de herramientas, como es el caso de OpenSSL, tanto para el uso de Criptografía Simétrica como así también para la Asimétrica. También se hará uso de la herramienta Gpg4win En el caso de las prácticas de HASH se utilizarán herramientas tanto por línea de comandos como por GUI. Con respecto al cifrado al vuelo, se utilizará en clase la herramienta VeraCrypt y para el caso de Esteganografía, se utilizarán herramientas que harán muy sencillo el uso de esta técnica. Se implementará una PKI para el uso de certificados digitales confiables en entornos web. Y se navegará la Blockchain por dentro con herramientas

específicas.

Requisitos

Conocimientos previos:
Tener conocimientos de seguridad informática o haber realizado el curso de Introducción a la seguridad Informática

Modalidad de cursado

Puedes tomar este curso en modalidad presencial o modalidad online - en vivo

¿Qué aprenderás?

- Fundamentos de la Criptografía clásica
- Cómo aplicar algoritmos criptográficos
- Principios de Kerckhoff
- Criptografía simétrica y asimétrica
- Trabajando con OpenSSL y GnuPG
- Cómo se usan los algoritmos de HASH
- Funciones de Rainbow Tables
- Infraestructura de Clave Pública
- Cómo usar la Esteganografía
- Funcionamiento de una PKI y sus buenas prácticas
- Blockchain y su arquitectura
- Criptomonedas y minería

Plan de Estudios

1. Criptografía Clásica

Conceptos generales
Transposición
Sustitución
Historia
Criptoanálisis
Principios de Kerckhoff

2. Criptografía Simétrica y Asimétrica

Criptografía Simétrica
Conceptos
Tipos de Criptografía Simétrica
Bloque
Flujo
Problemáticas
OpenSSL
Criptografía Asimétrica
Conceptos
Usos de la Criptografía Asimétrica
Cifradores
Generadores de claves
Curvas Elípticas
Firma electrónica vs Firma digital
OpenSSL
GnuPG

3. HASH y otras aplicaciones Criptográficas

HASH
Conceptos
Colisiones
Ataque de cumpleaños
Rainbow tables

HMAC
Cifrado al Vuelo
Conceptos
Usos comunes
VeraCrypt
Esteganografía
Conceptos
Aplicación

4. Infraestructura de Clave Pública

Conceptos
Arquitectura
Implementación
Usos
Problemáticas
Blockchain

5. ¿Qué es la Blockchain?

Criptomonedas
Árbol de Merkle
Redes P2P
Consenso
Prueba de trabajo
Minería
Otras Aplicaciones

EDUCACIÓN IT

Centro de Capacitación y Desarrollo Profesional

Lavalle 648 Piso 8, Microcentro, CABA
TEL_PRINCIPAL
info@educacionit.com