Introducción a la Criptografía

Objetivo

La criptografía se ha introducido de manera gradual e imperceptible en muchos aspectos de la vida moderna:

- Nuestros teléfonos celulares cifran sus conexiones con las radios base o con puntos de acceso Wi-Fi.
- Usamos conexiones cifradas para conectarnos con los sitios web de nuestras universidades.
- Intercambiamos mensajes cifrados extremo a extremo con aplicaciones como Whatsapp o Signal.
- Instalamos software que está firmado digitalmente.
- Firmamos digitalmente documentos.

Sin embargo, a menudo carecemos del conocimiento necesario para juzgar la efectividad de las herramientas que utilizamos, y la experiencia indica que son herramientas difíciles de usar bien y fáciles de usar mal.

El objetivo del curso es brindar una introducción práctica a la criptografía moderna y su aplicación en el contexto de las universidades argentinas. Se presentarán distintas herramientas de protección de la confidencialidad, integridad y autenticidad de la información en un esquema de tres pasos:

1. Introducción al problema
2. Solución al problema presentado
3. ¿Qué puede salir mal?

Los destinatarios de este curso son:

- Responsables de áreas de tecnología que deban tomar decisiones sobre herramientas a utilizar.
- Personal de áreas de infraestructura que deba desplegar y mantener equipos y sistemas.
- Programadores que utilicen herramientas criptográficas en sus desarrollos.

Al finalizar el curso podremos responder preguntas como:

- ¿Qué es más seguro, Whatsapp o Telegram y por qué no es Telegram?
- ¿Qué herramientas debo usar para cifrar y por qué no PGP?
- ¿Es posible tener correo electrónico seguro y por qué no?
- ¿Qué algoritmos de clave pública debo utilizar y por qué no RSA?
- ¿Qué bibliotecas criptográficas me conviene utilizar y por qué no OpenSSL?
- Tengo que redactar la política de seguridad de mi universidad ¿qué algoritmos y longitudes de clave debo especificar?

Cronograma

Semana 1

Introducción. Confidencialidad. Integridad. Criptografía simétrica y asimétrica.
Primitivas básicas:

- Cifrado de flujo
- Cifrado de bloques
- Cifrado autenticado
- Funciones de Hash
- MAC
- Cifrado asimétrico
- Firma digital

Algoritmos públicos y algoritmos privados. Principio de Kerckhoff
Aplicación en un modelo de capas de red.

Semana 2

Criptoanálisis. Tipos de ataques.
Claves. Generación de claves. Generación de valores aleatorios.
Entropía.
Seguridad de una clave.
Qué puede salir mal. Netscape. Dual_EC_DRBG.

Semana 3

Cifrados de flujo.Casos de Uso
One time pad. Seguridad incondicional y seguridad computacional.
LFSR. NLFSR. Algoritmos de cifrado de flujo.
Nonces.
Qué puede salir mal. CSS. Reutilización de IV. Wep. RC4.

Semana 4

Cifrado de bloques. Casos de uso.
Modos de operación. Mecanismos de relleno.
AES
Qué puede salir mal. Padding oracle attack. Side channel attacks.
E-fail.

Semana 5

Funciones de hash criptográficas. Casos de uso
Propiedades.
SHA-2, SHA-3.

Derivación de claves.
Protección de contraseñas.
Qué puede salir mal. Colisiones en MD5. El caso de Flame. Colisiones en SHA-1.

Semana 6

Cifrado autenticado. Casos de uso.
Autenticación. MAC. HMAC. CMAC. Poly1305
AEAD. AES-GCM. ChaCha20-Poly1305.
OCB. EAX. CCM.
Qué puede salir mal. Nonce misuse. Interacción entre confidencialidad e integridad.

Semana 7

Criptografía de clave pública. Casos de uso.
RSA.
Intercambio de claves. Diffie-Hellman.
Firma Digital. DSA.
Criptografía de curvas elípticas. ECDSA. EdDSA. X25519.
Qué puede salir mal. Ataques sobre RSA.

Semana 8

Aplicaciones y tendencias actuales
Bibliotecas modernas. NaCl, libsodium, Tink.
Signal. Age. Minisign. Signify. Magic wormhole
Criptografía post-cuántica.

Metodología

Se dictarán 8 clases sincrónicas mediante videoconferencia. En cada clase se planteará un problema específico que puede resolverse mediante criptografía (por ejemplo, confidencialidad de un mensaje), se mencionarán las soluciones existentes y se cerrará con ejemplos en los que se han aplicado soluciones erróneas. No veremos en profundidad detalles de los algoritmos, salvo en los casos en los que la ignorancia de esos detalles pueda conducir a malas decisiones.
En todas las clases se plantearán ejercicios prácticos y cuestionarios de autoevaluación sobre cada tema específico.

Bibliografía

Notas de clase, disponibles en el aula virtual.
Estándares y papers relevantes, disponibles en el aula virtual.