UNIVERSIDAD DEL VALLE DE GUATEMALA
CAMPUS CENTRAL
FACULTAD DE INGENIERÍA

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Iniciativa Académica de Criptografía y Cifrado de la Información

1 Identificación

Curso:	CC3078 – Criptografía y Cifrado de Información	**Créditos:**	4
Ciclo:	Segundo	**Requisitos:**	Programación y Algoritmos
Año:	2021		Estructuras de Datos y Algoritmos
			Matemática Discreta 1
Profesor:	Alan Reyes–Figueroa	**Horario:**	Martes y jueves – 19:00-20:35
Email:	agreyes	**Sala:**	Por definir

Sitio Web del Curso:

- https://pfafner.github.io/cr2021

Office Hours:

- Viernes de 19:00 a 20:00 hrs, o por solicitud del estudiante. También pueden enviar sus dudas por mediante el correo electrónico institucional.

2 Descripción

Este curso es una introducción al estudio de los métodos de criptografía, criptoanálisis y cifrado de la información, la cual consiste en procesar datos en forma ininteligible, de forma reversible, sin pérdida de información, normalmente de forma digital. Dicho de otra forma, la criptografía es el estudio de cómo alterar un mensaje para que alguien que lo intercepte no pueda léalo sin el algoritmo y la clave adecuados, mientras que los métodos de cifrado son aquellos algoritmos matemático/computacionales para llevar a cabo esta alteración. En esta materia, estudiaremos de manera introductoria los principales métodos y protocolos actuales de cifrado, así como su implementación computacional.

La primera parte el curso inicia con una revisión histórica de la criptografía, para dar paso rápidamente a los métodos usados en la criptografía actual. Se hace una revisión de conceptos y herramientas básicas sobre los que se fundamentan la mayoría de algoritmos y métodos criptográficos. Se hace un recordatorio breve de conceptos matemáticos útiles como distribuciones discretas de probabilidad, teoría de la información, entropía, y conceptos importantes de la criptografía como seguridad e integrabilidad.

Seguidamente, haremos una introducción a los métodos criptográficos simétricos. En particular, se estudian principalmente los métodos de cifrado en flujo *stream ciphers*) Se estudian ejemplos como los métodos como el cifrado XOR, los métodos *one time pad*, y los basados en generación de números pseudo-aleatorios. Luego se discuten los métodos de cifrado en bloque (*block ciphers*). Se estudian principalmente los métodos de tipo AES y DES, así como otras aplicaciones.
Seguidamente estudiamos el tema de integridad de datos. Se discuten algunas construcciones clásicas como los sistemas de autenticación de mensajes (MAC). Se introducen luego los métodos de cifrado autenticado, que garantizan tanto la confidencialidad como la integridad.

Luego se estudia el tema de métodos asimétricos. Se introduce el concepto de intercambio de llaves entre dos partes, así como las motivaciones de la criptografía de llave pública. Se hace un repaso de teoría de números computacional,

por ejemplo el algoritmos de Euclides, y resultados de aritmética modular, entre otros. Con esos conceptos, se estudian los métodos de cifrado de clave pública y sus aplicaciones. Estudiamos principalmente los protocolos de Diffie-Hellman, el sistema RSA, así como los métodos CCA.

El curso finaliza con una serie de temas avanzados y recientes como las implicaciones de la computación cuántica para la criptografía, las criptomónedas y los métodos *blockchain*.

3 Competencias a Desarrollar

Competencias genéricas

1. Piensa de forma crítica y analítica.
2. Resuelve problemas de forma estructurada y efectiva.
3. Desarrolla habilidades de investigación, desarrollo e implementación y habilidades de comunicación a través de proyectos y presentaciones ante sus colegas.

Competencias específicas

1.1 Entiende los conceptos teóricos que formalizan los principales algoritmos criptográficos y esquemas de cifrado de información y sus limitaciones.

1.2 Conoce los primitivos y algoritmos criptográficos más utilizados en la actualidad.

2.1 Aplica métodos y técnicas para la implementación correcta de métodos y algoritmos criptográficos.

2.2 Implementa las soluciones criptográficas adecuadas para el contexto mediante programas de computación escrito en un lenguaje de alto nivel.

2.3 Utiliza un enfoque global para resolver problemas. Se apoya en herramientas auxiliares para su solución, como el análisis de algoritmos, el álgebra, la probabilidad y la teoría de números.

3.1 Desarrolla todas las etapas de un proyecto aplicado donde se realiza una implementación o análisis criptofráfico.

3.2 Escribe un reporte técnico sobre la solución de un problema en criptografía. Concreta un análisis riguroso y conclusiones importantes.

3.3 Comunica de manera efectiva, en forma escrita, oral y visual, los resultados de su investigación.

4 Metodología Enseñanza Aprendizaje

El curso se desarrollará durante diecinueve semanas, con cuatro períodos semanales de cuarenta y cinco minutos para desenvolvimiento de la teoría, la resolución de ejemplos y problemas, comunicación didáctica y discusión. Se promoverá el trabajo colaborativo de los estudiantes por medio de listas de ejercicios. El curso cuenta con una sesión de laboratorio semanal para la implementación de algoritmos y la práctica de las técnicas del análisis criptográfico.

El resto del curso promoverá la revisión bibliográfica y el auto aprendizaje a través de la solución de los ejercicios y problemas adicionales, y el desarrollo de un seminario. Se espera que el alumno desarrolle su trabajo en grupo o individualmente, y que participe activamente y en forma colaborativa durante todo el curso.

5 Contenido

1. Introducción. Revisión histórica de la criptografía antigua. Métodos modernos. Revisión de conceptos matemáticos: probabilidad y distribuciones discretas. Teoría de la información, entropía. Operaciones a nivel de bits. Definiciones y conceptos teóricos en criptografía: seguridad, secreticidad, integrabilidad. Principio de Kerckhoff. Ejemplos de métodos criptográficos y aplicaciones.

2. Sistemas criptográficos simétricos. Cifrados de flujo o *stream ciphers*. Métodos de cifrado XOR, métodos *one-time pad*. Ataques por fuerza bruta. Cotas para el ataque. Ataques por canal lateral. Cifrados de bloque o *block ciphers*. Redes de Feistel. Ejemplos. Sistemas DES y tripe DES. Sistemas AES.

3. Sistemas criptográficos asimétricos. Cifrado asimétrico. Funciones unidireccionales. Repaso de conceptos matemáticos: primos, aritmética modular, resultados importantes. El problema de la factoración en primos. Raíces primitivas. Logaritmo discreto. Métodos de llave pública. Intercambio Diffie-Hellman. Ataques. Método El Gamal. EL sistema RSA. Ejemplos y aplicaciones.

4. Funciones hash y funciones hash criptográficas. Implementaciones. Ejemplos. Propiedades unidireccionales y propiedades de colisión. Aplicaciones: cadenas hash, contraseñas de un solo úso. Esquemas *S-key*. Árbol hash. Criptomonedas.

5. Autenticación de mensajes. Códigos de autenticación de mensajes (MAC) que se basa en claves simétricas. Diferencia MAC y funciones hash. Algoritmo de autenticación de datos (DAA) y MAC basado en cifrado (CMAC). Métodos de cifrado autenticado.

6. Firmas digitales para autenticación. Manejo de claves, jerarquía y descentralización. Estándar de firma digital (DSS).

7. Otros tópicos: criptografía de curvas elípticas, otros métodos criptográficos avanzados. Blockchain. Criptografía y computación cuántica.

6 Bibliografía

Textos:

- D. Boneh, V. Shoup (2020). *A Graduate Course in Applied Cryptography*.
- N. Smart (2016). *Cryptography Made Simple*. Springer.

Referencias adicionales:

- W. Easttom (2021). *Modern Cryptography*. Springer.
- J. Katz, Y. Lindell (2021). *Introduction to Modern Cryptography*. CRC Press.
- B. Schneier (1996). *Applied Cryptography*. 2nd Edition. Wiley.
- N. Ferguson, B. Schneier, T. Kohno (2010). *Cryptography Engineering*. Wiley.
- S. J. Nielson, C. K. Monson (202?). *Practical Cryptography in Python*. Apress.
- C. Paar, J. Pelzl (2010). *Understanding Cryptography*. Springer.
- J. Hoffstein, J. Pipher, J. H. Silverman (2008). *An Introduction to Mathematical Cryptography*. Springer.
- D. Wong (2021). *Real-World Cryptography*. Manning.
- J.-P. Aumasson (2018). *Serious Cryptography*. No Satarch Press.

7 Actividades de evaluación

Actividad	Cantidad aproximada	Porcentaje
Laboratorios	10 a 15	80%
Proyectos	1	20%

8 Cronograma

Semana	Tópico	Fecha	Actividades
1	Introducción y motivación al curso.	05-09 julio	
2	Criptografía antigua. Cifrados de sustitución. Limitantes. Ejemplos: cifrado César, cifrado Vigènere, Enigma.	12-16 julio	
3	Revisión de conceptos matemáticos: probabilidad discreta, teoría de la información. Conceptos básicos.	19-23 julio	
4	*Stream ciphers*: Métodos de cifrado XOR, métodos *one-time pad*. Ataques por fuerza bruta	26-30 julio	
5	*Stream ciphers*: Métodos por generación de números pseudo-aleatorios. Ataques por canal lateral.	02-06 agosto	
6	*Block ciphers*: redes de Feistel.	09-13 agosto	
7	*Block ciphers*: Sistemas DES y tripe DES. Sistemas AES.	16-20 agosto	
8	Integridad de mensajes. Código de autenticación MAC. Algoritmo de autenticación de datos DAA y CMAC.	23-27 agosto	
9	Revisión de aritmética modular. Congruencias. El teorema Chino del residuo. Teoremas de Euler y Lagrange.	30 agosto-03 sept	
10	Raíces primitivas. El logaritmo discreto. Métodos de factoración y testes de primalidad.	06-10 septiembre	
	Semana de asueto	13-17 septiembre	
11	Intercambio de clave pública: el método de intercambio de Diffie-Hellman.	20-24 septiembre	
12	Intercambio de clave pública: el método RSA.	27 sept - 01 octubre	
13	Otros métodos de intercambio de clave pública. Método de ElGamal.	04-08 octubre	
14	Firmas digitales. Manejo de claves y jerarquía. El estándar de firma digital DSS.	11-15 octubre	
15		18-22 octubre	
16	Funciones Hash y funciones hash criptográficas. Ejemplo. Propiedades unidireccionales y de colisión.	25-29 octubre	
17	Funciones Hash: Aplicaciones. Cadenas hash, contraseñas de un solo uso. Esquemas *S-key*. Árbol hash. Criptomonedas.	01-05 noviembre	
18	Tópicos adicionales: Criptofrafía de curvas elípticas. Otros métodos criptográficos avanzados.	08-12 noviembre	Seminarios
19	Tópicos adicionales: Esquemas *Blockchain*. Implicaciones de la computación cuántica a la criptografía.	15-19 noviembre	Seminarios
20	Presentación de proyectos.	22-26 noviembre	Proyecto