Introducción a la criptografía

Guía de asignatura

Última actualización: julio de 2022

1. Información general

Nombre de la asignatura	Introducción a la criptografía
Código	11310059
Tipo de asignatura	Obligatoria
Número de créditos	2
Tipo de crédito	1A+1B
Horas de trabajo semanal con acompañamiento directo del profesor	64
Horas semanales de trabajo independiente del estudiante	32
Prerrequisitos	Álgebra Lineal y Programación de computadores
Correquisitos	Ninguno
Horario	
Líder de área	Daniel Díaz Correo: danielo.diaz@urosario.edu.co
Salón	

2. Información del profesor y monitor

Nombre del profesor	**Mateo Sanabria Ardila**
Perfil profesional	Matemático de la escuela colombiana de ingeniería. M.Sc. en ingeniería de sistemas de la Universidad de los Andes. Con experiencia en verificación formal sobre sistemas distribuidos, matemática computacional y criptografía.
Correo electrónico institucional	Mateo.sanabria@urosario.edu.co
Lugar y horario de atención	**A definir con los estudiantes**

3. Resumen y propósitos del curso

Desde el comienzo de la escritura, los seres humanos hemos tratado de comunicarnos secretamente. Antes de la era moderna la criptografía se usaba básicamente para permitir que dos personas se pudieran comunicar a través de un canal de información inseguro, de tal manera que, si una tercera persona tenía acceso al mensaje enviado, esta no fuera capaz de entenderlo. Así, la persona que enviaba el mensaje, lo modificaba siguiendo un determinado protocolo (lo cual llamaremos: cifrar usando un determinado criptosistema). El resultado era un nuevo mensaje llamado ``mensaje cifrado''. Este mensaje cifrado era enviado al destinatario deseado a través del canal que podía ser inseguro. Finalmente, el destinatario conocía una clave secreta que le permitía invertir el protocolo de cifrado para así poder obtener el mensaje original.

Actualmente, la criptografía es la piedra angular de la seguridad informática y es utilizada para muchos propósitos además de permitir una comunicación secreta a través de un canal inseguro. Por ejemplo: mantener secreta la información guardada en una base de datos, asegurar anonimato, asegurar la autenticidad, las firmas digitales, etc.

El objetivo del curso es conocer algunos de los criptosistemas utilizados en la antigüedad, aprender los fundamentos matemáticos y los conceptos básicos para poder entender la criptografía moderna. Comprender la criptografía simétrica y asimétrica, conocer los criptosistemas clásicos (como AES y RSA), las firmas electrónicas, las funciones de hash, algunos métodos de autentificación entre otros.

4. Conceptos fundamentales

1. Introducción a la Matemática Discreta
2. Criptosistemas de la antigüedad (Cesar, Vigenère, etc.)
3. Criptografía simétrica (DES- AES)
4. Más bases matemáticas: logaritmo discreto, función de Euler, test de primalidad.
5. Criptografía a clave pública: RSA
6. Firmas electrónicas (El Gamal).
7. Funciones de HASH
8. MAC
9. Protocolo de establecimiento de clave (Diffie y Hellman).
10. Sistema para compartir el secreto de Shamir.

5. Resultados de aprendizaje esperados (RAE)

1. Aprender los fundamentos matemáticos necesarios.
2. Comprender la criptografía simétrica y sus principales criptositemas (DES, AES).
3. Comprender la criptografía asimétrica y sus principal criptositema: RSA, El Gamal.
4. Entender algunas primitivas criptográficas: firmas digitales, funciones de hash.

6. Modalidad del curso

Presencial: Martes y Jueves (7AM-9AM)

7. Estrategias de aprendizaje

En cada sesión se dará una parte teórica y se dividirá a los alumnos en grupos para hacer ejercicios y transferir el conocimiento. Tendrán también que estudiar un tema por grupos.

8. Actividades de evaluación

- Exámenes parciales (Hay 3 parciales de 15 % cada uno)
- Quices y Tareas (25 %)
- Proyecto (30%)

9. Programación de actividades

Fecha	Tema	Descripción de la actividad	Trabajo independiente del estudiante	Recursos que apoyan la actividad
Sesión 1 Martes 26/07	Introducción al curso. Matemáticas discretas, aritmética modular, Algoritmo de Euclides			
Sesión 2 Jueves 28/07	aritmética modular, Algoritmo de Euclides Criptosistemas de la antigüedad por transposición + criptoanálisis			
Sesión 3 Martes 2/08	Criptosistemas de la antigüedad por transposición + criptoanálisis			

Sesión 4 Jueves 4/08	Criptografía simétrica (DES- AES)			
Sesión 5 Martes 9/08	Criptografía simétrica (DES- AES)			
Sesión 6 Jueves 11/08	Operaciones de Bloques/ Stream Ciphers, Provably secure symmetric cipher		Taller 1	
Sesión 7 Martes 16/08	Dudas, solución del Taller 1, ejercicios en clase en grupos.			
Sesión 8 Jueves 28/08	Teorema del residuo Chino, Función Phi de Euler			
Sesión 9 Martes 23/08	Teorema del residuo Chino, Función Phi de Euler		Entregar el Taller 1	
Sesión 10 Jueves 25/08	Comienzo de PKC- preparando el RSA			
Sesión 11 Martes 20/08	Parcial 1			
Sesión 12 Jueves 1/09	Corrección Parcial 1 /Problemas para definir el RSA			
Sesión 13 Martes 5/09	Generación de números primos y seguridad del RSA		Taller en clase RSA	
Sesión 14 Jueves 8/09	Discusión de RSA			
Sesión 15 Martes 13/09	Discret log y El Gamal PKC		+ taller	
Sesión 16	El Gamal / Funciones de Hash		Taller de El Gamal	

Jueves 15/09				
Sesión 17 Martes 20/09	Funciones de Hash			
Sesión 18 Jueves 22/09	Solución del taller y dudas			
Sesión 19 Martes 27/09	Parcial 2			
Sesión 20 Jueves 29/09	MAC Definición de proyectos			
Sesión 21 Martes 04/10	Taller MAC			
Sesión 22 Jueves 06/10	Firmas digitales			
Sesión 23 Martes 11/10	Protocolo de establecimiento de clave (Diffie y Hellman).			
Sesión 24 Jueves 12/10	Taller en clase Diffie y Hellman			
Lunes 18/10 Festivo	Semana Rosarista			
Miércoles 20/10	Semana Rosarista			
Sesión 24 Martes 25/10	Secret Sharing			
Sesión 25 Jueves 27/10	Taller en clase Secret Sharing			
Sesión 26 Martes 1/11	Taller en clase: integración de conceptos			

Sesión 27 Jueves 3/11	Taller en clase: integración de conceptos			
Sesión 28 Martes 8/11	Parcial 3			
Sesión 29 Jueves 10/11	**Sustentación de proyectos**			
Semana de finales	**Sustentación de proyectos**			

10. Factores de éxito para este curso

A continuación se sugieren una serie de acciones que pueden contribuir, de manera significativa, con el logro de metas y consecuentemente propiciar una experiencia exitosa en este curso:

1. Planificar y organizar el tiempo de trabajo individual que le dedicará al curso

2. Organizar el sitio y los materiales de estudios

3. Tener un grupo de estudio, procurar el apoyo de compañeros

4. Cultivar la disciplina y la constancia, trabajar semanalmente, no permitir que se acumulen temas ni trabajos

5. Realizar constantemente una autoevaluación, determinar si las acciones realizadas son productivas o si por el contrario se debe cambiar de estrategias

6. Asistir a las horas de consulta del profesor, participar en clase, no quedarse nunca con la duda

7. Propiciar espacios para el descanso y la higiene mental, procurar tener buenos hábitos de sueño

8. Tener presente en todo momento valores como la honestidad y la sinceridad, al final no se trata solo de aprobar un examen, se trata de aprender y adquirir conocimientos. El fraude es un autoengaño

11. Bibliografía y recursos

Stinson, Douglas Robert. Cryptography : theory and practice. 3rd edition.

12. Bibliografía y recursos complementarios

13. Acuerdos para el desarrollo del curso

No está permitido comer o usar dispositivos móviles dentro de clase. No se realizará aproximación de notas al final del semestre. Las notas solo serán cambiadas con base en reclamos OPORTUNOS dentro de los límites de tiempo determinados por el Reglamento Académico. Si por motivos de fuerza mayor el estudiante falta a algún parcial o quiz, deberá seguir el procedimiento regular determinado por el Reglamento Académico para presentar supletorios. No habrá acuerdos informales al respecto. No se eximirá a ningún estudiante de ningún examen.

PROCESOS DISCIPLINARIOS-FRAUDE EN EVALUACIONES
Teniendo en cuenta el reglamento formativo-preventivo y disciplinario de la Universidad del Rosario, y la certeza de que las acciones fraudulentas van en contra de los procesos de enseñanza y aprendizaje, cualquier acto corrupto vinculado a esta asignatura será notificado a la secretaría académica correspondiente de manera que se inicie el debido proceso disciplinario. Se recomienda a los estudiantes leer dicho reglamento para conocer las razones, procedimientos y consecuencias que este tipo de acciones pueden ocasionar, así como sus derechos y deberes asociados a este tipo de procedimientos.

La asignatura no tiene ningún tipo de Bono.

14. Respeto y no discriminación

Si tiene alguna discapacidad, sea este visible o no, y requiere algún tipo de apoyo para estar en igualdad de condiciones con los(as) demás estudiantes, por favor informar a su profesor(a) para que puedan realizarse ajustes razonables al curso a la mayor brevedad posible. De igual forma, si no cuenta con los recursos tecnológicos requeridos para el desarrollo del curso, por favor informe de manera oportuna a Margot Salas y a la Secretaría Académica, de manera que se pueda atender a tiempo su requerimiento.

Recuerde que es deber de todas las personas respetar los derechos de quienes hacen parte de la comunidad Rosarista. Cualquier situación de acoso, acoso sexual, discriminación o matoneo, sea presencial o virtual, es inaceptable. Quien se sienta en alguna de estas situaciones puede denunciar su ocurrencia contactando al equipo de la Coordinación de Psicología y Calidad de Vida de la Decanatura del Medio Universitario (Teléfono o WhatsApp 322 2485756).

Universidad del Rosario