Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad-Iztapalapa

Planeación
Criptografía de clave pública
Trimestre 22-P

Clave	Grupo	Periodo
2131131	CI01	del 11 de julio de 2022 al 23 de septiembre de 2022

Inicio del curso: 11 de julio 2022
Horario:
Lunes, Martes y Jueves de 12:00 a 14:00 horas
http://mat.izt.uam.mx/mat/index.php/horarios-licmat

Profesora: Yuriko Pitones Amaro Correo: ypitones@xanum.uam.mx yuriko.pitones@cimat.mx	Ayudante:

OBJETIVO DEL CURSO: Comprender la importancia de cifrar mensajes, comprender los modelos criptográficos clásicos, aplicar modelos criptográficos, analizar las normas internacionales sobre criptografía.

El temario oficial y bibliografía del curso de **Criptografía de clave pública** se pueden encontrar en la página oficial del Departamento de Matemáticas: http://mat.izt.uam.mx/mat/documentos/coordinaciones/LICMAT/2131131.pdf

Temas

1. Introducción (3 semanas)
1.1. Aplicaciones actuales de la Criptografía.
1.2. Sustitución simple y poli-alfabética.
1.3. Técnicas de cripto-análisis.
1.4. Modelos de cifrado de Playfair y de Hill.
1.5. Secreto perfecto.

2. Cifrados de llave privada (3 semanas)
2.1. El criptosistema DES.
2.2. El criptosistema AES.
2.3. Aplicaciones.

3. Cifrados en flujo (3 semanas)

3.1. Descripción de los cifrados en flujo.
3.2. Generadores de números pseudoaleatorios.
3.3. Registros lineales con retroalimentación.

4. Normas de seguridad para redes de comunicación.

Bibliografía

1. Cortés Dávalos, A., et. al. Elementos de Criptografía Clásica. Serie Matemática Aplicada y Enseñanza. SMM, 2005, ISBN 968-5733-05-8.
2. Delfs, H., Knebl, H., Introduction to Cryptography: Principles and Applications. Springer, 2002.
3. Koblitz, N., A Course in Number Theory and Cryptography. Springer-Verlag, 1994.
4. Menezes, A. (Editor), Applications of finite fields., Kluwer Academic Press, 1993.
5. Menezes, A., van Oosrcot, P. C., Vanstone, S. A., Handbook of Applied Cryptography. CRC Press, 1996.
6. Paar, C., Pelzl, J., Understanding Cryptography, Spinger-Verlag, 2010.
7. Robling, D. E., Cryptography and Data Security, Addison-Wesley, 1983.
8. Schneier, B., Applied Cryptography, JohnWilley & Sons, 1996.
9. Stinson, D. R., Cryptography: Theory and Practice, CRC Press, 2006.

Evaluación

La evaluación del curso se realizará en tres parciales, en cada uno se contemplarán los siguientes elementos:

- Un examen parcial: las fechas e instrucciones se darán a conocer conforme avance el curso.
- Tareas y actividades: se asignará una o dos tareas/actividades semanalmente, comprenderá problemas y ejercicios relativos a los temas que se abordarán en las clases. Se entregan individualmente.

La calificación final se obtendrá con el promedio de las calificaciones de cada uno de los elementos anteriores obtenidas en los tres parciales, de acuerdo a los siguientes porcentajes:

	Porcentajes
Exámenes parciales (promedio de los tres)	70%
Tareas / Actividades (promedio de los tres)	30%

Escala de calificaciones:

La escala de calificaciones será de 0 a 100 y la equivalencia en letra es la siguiente:
NA: 0-60 S: 61- 75 B: 76 -85 MB: 86-100

Examen global y reposiciones

El examen global se realizará entre el 26 y 30 de septiembre 2022.
El/ la estudiante debe considerar lo siguiente:

División de Ciencias Básicas e Ingeniería
E-mail: ypitones@xanum.uam.mx
yuriko.pitones@cimat.mx

1. Para aprobar el curso, el/la estudiante debe obtener una calificación aprobatoria en cada uno de los tres exámenes parciales, o bien, si el/la estudiante no aprobó al menos dos de los tres exámenes, debe presentar el examen global. En este caso, la calificación del examen global representara el 100% de la calificación del curso.
2. Cualquier estudiante puede presentar el examen global, si es así, renuncia a la calificación obtenida durante el curso; y el resultado del examen global será el 100% de la calificación final.

Observaciones

Los avisos y especificaciones de las fechas de exámenes se comunicarán con anticipación en la clase o por correo electrónico.

Comentarios adicionales, enviar correo electrónico.

División de Ciencias Básicas e Ingeniería
E-mail: ypitones@xanum.uam.mx
yuriko.pitones@cimat.mx