NOMBRE DE LA INSTITUCIÓN	Universidad de Sonora
DIVISIÓN ACADÉMICA	División Ciencias Exactas y Naturales
DEPARTAMENTO QUE IMPARTE LA MATERIA	Departamento de Matemáticas
LICENCIATURAS USUARIAS	Ciencias de la Computación
NOMBRE DE LA MATERIA **CLAVE**	**Teoría de Códigos** **9474**
EJE FORMATIVO	Especializante
REQUISITOS	Introducción al álgebra moderna
CARÁCTER	Optativo
VALOR EN CRÉDITOS	8 (3 teoría/2 taller)

Introducción

En la sociedad actual, inmersa en la "supercarretera de la información", cada vez es más necesario garantizar la seguridad de los datos del cliente; esto es especialmente válido si se trata de un desarrollador de software, una de las facetas del científico de la computación. La Teoría de Códigos y la Criptografía son áreas de trabajo que permiten resguardar la información que se almacena o se transmite a través de dispositivos electrónicos. Por esto, es importante difundir el desarrollo y motivar la investigación en estas áreas.

Objetivo General del Curso

Familiarizar al estudiante con los mecanismos de codificación de la información digital resaltando la naturaleza matemática de los mismos.

Objetivos Específicos del Curso

- Combinar en la teoría de códigos, teorías matemáticas elegantes con construcciones de un impacto práctico importante.
- Revisar construcciones de códigos para corrección de errores, códigos secretos y aquellos que se utilizan en la comprensión de datos.

Contenido

1. **Prerrequisitos**.
   - 1.1. Álgebra.
   - 1.2. Polinomios de Krawtchouk.
   - 1.3. Teoría combinatoria.
   - 1.4. Teoría de probabilidad.

2. **Introducción a la teoría de códigos.**
   - 2.1. Códigos correctores de errores.
   - 2.2. El problema fundamental de la teoría de código.
   - 2.3. Introducción a los códigos lineales.

3. **Comunicación confiable a través de canales no confiables.**
   - 3.1. Canales binarios simétricos.
   - 3.2. Tasa de información.
   - 3.3. Un ejemplo de aumento de confiabilidad.
   - 3.4. Distancia de Hamming.
   - 3.5. Detección de errores.
   - 3.6. Corrección de errores.
   - 3.7. Capacidad de los canales.
   - 3.8. Teorema fundamental de Shannon.

4. **Códigos lineales.**
   - 4.1. Códigos de bloques.
   - 4.2. Códigos lineales.
   - 4.3. Códigos de Hamming.
   - 4.4. Decodificación por lógica de la mayoría.
   - 4.5. Numeradores de peso.
   - 4.6. Comentarios.

5. Algunos códigos buenos.

5.1. Código de Aduanarte y generalizaciones.
5.2. El código binario de Golay.
5.3. El código ternario de Golay.
5.4. Construcción de códigos a partir de otros códigos.
5.5. Código de Reed-Muller.
5.6. Comentarios.

6. **Criptografía**.

6.1. Un escucha con ruido.
6.2. Encriptado de llaves secretas.
6.3. Encriptado de llaves públicas.
6.4. Encriptado basado en números primos grandes.
6.5. Encriptado basado en problemas de empacado.
6.6. Estándar para el encriptado de datos.

Estrategias Didácticas
En general, promover la participación activa de los estudiantes poniendo especial atención al desarrollo de habilidades.

Estrategias de Evaluación
Para la evaluación de los estudiantes, el profesor tomará en cuenta:

- Resultados de los exámenes parciales aplicados (se sugiere que sean al menos tres),
- Tareas, trabajos de investigación, presentaciones.
- Participación individual y colectiva en las actividades cotidianas.

Los porcentajes serán acordados al inicio del semestre.

Bibliografía:

- R. Hill A First Course in Coding Theory. Oxford, Applied Mathematics and Computing Science Series. 1990.
- J. Adámek Fundations of Coding Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory. John Wiley & Sons. Inc. Wiley-Interscience Publication, 1991.
- S. Roman. Coding and Information Theory Springer-Verlag, 1992.
- J.H. Van Lint. Coding Theory Springer-Verlag, 1982.
- J.H. Van Lint. Introduction to Coding theory and Algebraic Geometry Springer-Verlag, 1989

Perfil Académico Deseable del Maestro

Se recomienda que el profesor tenga las siguientes características:

- Experiencia en el ejercicio de una profesión relacionada con las Ciencias de la Computación.
- Posea conocimientos acerca de las áreas de especialización de las Ciencias de la Computación.
- Incorpore el empleo de recursos computaciones en las actividades cotidianas del curso.