UNIVERSIDAD NACIONAL
DE
SANTIAGO DEL ESTERO

Facultad de Ciencias Exactas y Tecnologías

PLANIFICACIÓN ANUAL 2022

Asignatura: *CRIPTOGRAFÍA*
(Optativa IV)
Licenciatura en Matemática
Plan de Estudio: 2004

Dra. ROSANNA COSTAGUTA (Prof. Adjunto – Responsable)

1.- IDENTIFICACIÓN:

1.1- Nombre de la Asignatura /Obligación Curricular: **CRIPTOGRAFÍA (Optativa 1V)**

1.2- Carrera /s: ***Licenciatura en Matemática (Mención Modelos Aplicados a la Informática)***

1.3- Ubicación de la Asignatura/Obligación Curricular en el Plan de Estudios:

Octavo módulo – 4 to. Año

1.3.2- Ciclo al que pertenece la Asignatura/Obligación Curricular: ORIENTACIÓN

1.3.3- Carga horaria semanal: 8 horas. Carga horaria total: 120 horas.

1.3.5- Correlativas Anteriores:

Regularizadas: Ecuaciones Diferenciales, Cálculo Numérico, y Topología.
Aprobadas: No corresponde.

1.3.6- Correlativas Posteriores: Optativa II.

1.4- Objetivos establecidos en el Plan de Estudios para la Asignatura/Obligación Curricular:

El Plan de estudios no presenta definición de objetivos para cada una de las asignaturas/obligaciones curriculares.

1.5- Contenidos mínimos establecidos en el Plan de Estudios para la Asignatura /Obligación Curricular:
No existen contenidos mínimos definidos.

1.6- Año académico: 2022

2.- PRESENTACIÓN

2.1- Ubicación de la Asignatura como tramo de conocimiento de una disciplina / Ubicación de la Obligación Curricular como actividad o herramienta:

Esta asignatura corresponde al ciclo de Orientación de la carrera y está orientada principalmente a brindar a los alumnos fundamentos de la Criptografía, así como conocimientos sobre técnicas y metodologías propios de la disciplina que les permitan comprender los métodos de encriptado y también adquirir competencias para diseñar nuevos algoritmos de encriptamiento.

2.2- Conocimientos y habilidades previas que permiten encarar el aprendizaje de la Asignatura / Obligación Curricular:

Para el estudiante que cursa la asignatura se requieren conceptos previos adquiridos en las asignaturas Ecuaciones Diferenciales, Cálculo Numérico, y Topología. Contar con estos conocimientos previos permitirá al estudiante realizar una adecuada complementación con los que adquirirá en la cátedra, a fin de poder comprender, diseñar y desarrollar algoritmos propios de la Criptografía aplicados en la solución de problemas. Se espera además que los alumnos que ingresen a la cursada posean sentido de responsabilidad por el propio comportamiento, y cuenten con habilidades desarrolladas tanto respecto a un trabajo productivo en equipo como a un trabajo eficaz individual.

2.3- Aspectos del Perfil Profesional del Egresado a los que contribuye la asignatura:

La asignatura brinda a los estudiantes:

- Profundos conocimientos sobre técnicas propias de la Criptografía, que le servirán para el diseño de algoritmos específicos de la disciplina aplicados a la solución de problemas en otras áreas.

- Práctica en la integración de técnicas y metodologías de la Criptografía con otras provenientes de la Matemática.
- Formación en pensamiento reflexivo.
- Ejercicio de una actitud crítica frente a su propio quehacer.
- Práctica en la manifestación de una actitud creativa en la búsqueda de respuestas originales a problemas específicos mediante la aplicación de técnicas y metodologías propias de la disciplina.

3.- OBJETIVOS

- Que el alumno desarrolle las siguientes competencias básicas:
  - Representación de la Información
  - Lectura analítico-crítica
  - Resolución de Problemas

- Que el alumno desarrolle las siguientes competencias específicas:
  - Reconocer el tipo de problemas que pueden ser estudiados con técnicas de Criptografía
  - Aplicar diferentes métodos de encriptamiento de información
  - Desarrollar destrezas interpretativas, tanto visuales como analíticas
  - Comprender y valorar los avances logrados en el campo de la Criptografía y su contribución a otras ramas de conocimiento

- Que el alumno desarrolle las siguientes competencias digitales:
  - Buscar y seleccionar información relevante.
  - Comunicar sus ideas en diferentes formatos.
  - Utilizar adecuadamente distintas herramientas de la web 2.0.
  - Argumentar, negociar y consensuar posiciones en foros digitales.

- Que el alumno desarrolle las siguientes competencias transversales:
  - Aplicar principios y generalizaciones ya aprendidas a la resolución de nuevos problemas y situaciones
  - Hacer inferencias razonables a partir de observaciones
  - Sintetizar e integrar informaciones e ideas
  - Pensar holísticamente (atendiendo tanto al todo como a las partes)
  - Organizar eficazmente su trabajo
  - Trabajar productivamente con otros
  - Desarrollar una actitud de apertura hacia nuevas ideas, una estima duradera por el aprendizaje, una comprensión informada de la ciencia y la tecnología, un sentido de responsabilidad por el propio comportamiento, el respeto por el otro, y un compromiso por la honestidad

4.- SELECCIÓN Y ORGANIZACIÓN DE CONTENIDOS

4.1- Programa Sintético

UNIDAD 1: Fundamentos de la Criptografía
Definiciones. Términos asociados. Reseña histórica.

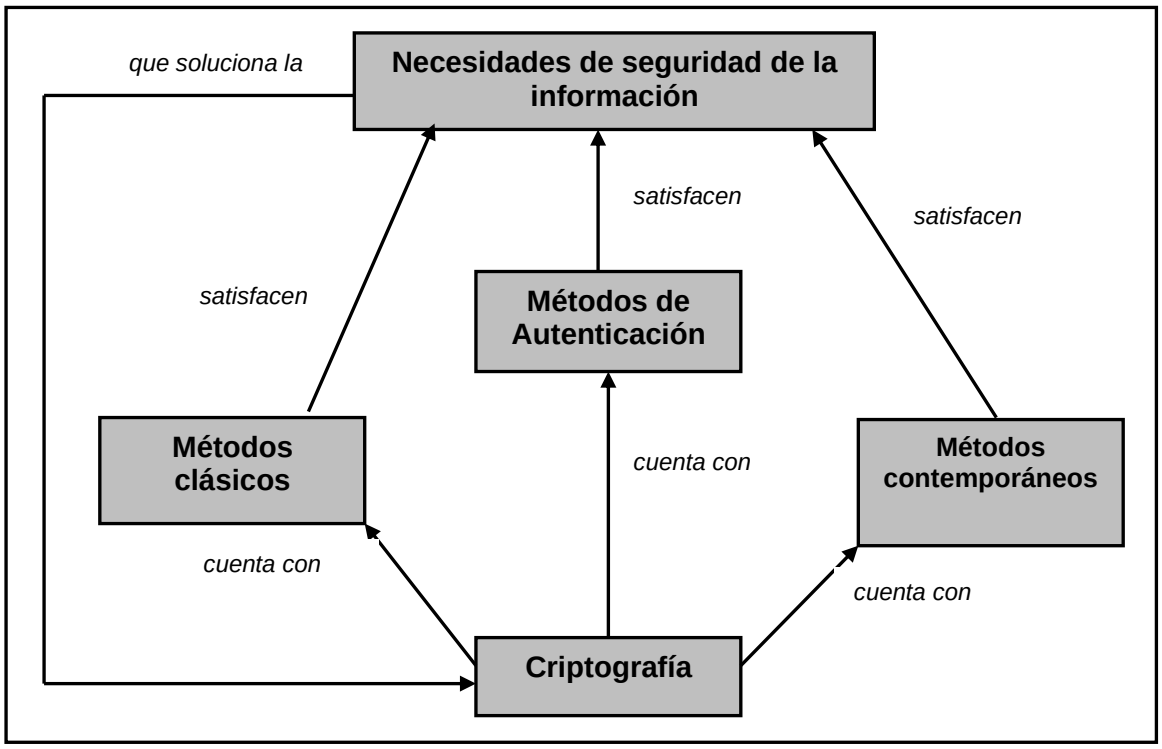
UNIDAD 2: Criptografía Clásica
Métodos clásicos de encriptación: por sustitución y por trasposición.

UNIDAD 3: Criptografía Moderna
Cifrados simétricos y asimétricos. Métodos de ataque conocidos.

UNIDAD 4: Métodos de autenticación
Autenticación de mensajes y autenticación de transmisores.

4.2- Articulación Temática de la Asignatura /Obligación Curricular:

La articulación temática se resume en el siguiente gráfico:



4.3- Integración horizontal y vertical con otras asignaturas:
Por ser asignatura del cuarto y último año de la carrera, y tal como se explicitó en la sección 1.3.5., Criptografía (Optativa IV) se integra verticalmente con las asignaturas: Ecuaciones Diferenciales, Cálculo Numérico, y Topología. La integración horizontal se da con la asignatura Optativa III, Teoría de Algoritmos y Lenguajes, por cuanto allí los estudiantes aprenden a formular problemas matemáticos y algoritmos.

4.4- Programa Analítico

UNIDAD 1: Fundamentos de la Criptografía
Criptografía: Etimología de la palabra. Definiciones. Términos asociados. Reseña histórica. Necesidad de encriptar la información. Estructura de los criptosistemas.

UNIDAD 2: Criptografía Clásica
Método clásicos de encriptación: conceptos básicos, encriptado y desencriptado, métodos de ataque conocidos. Por sustitución monoalfabética: César, César generalizado, ordenado por clave. Por sustitución polialfabética: código Vigenere y polialfabético periódico. Por trasposición simple y ordenado por clave.

UNIDAD 3: Criptografía Moderna
Criptosistemas contemporáneos: Cifrados simétricos y asimétricos. Condiciones de los criptosistemas asimétricos. Rivest-Shamir-Adleman (RSA): algoritmo implementado, seguridad del método, encubrimiento de los mensajes. Diffie-Hellman (D-H): algoritmo implementado.

Merkle-Hellman (M-H): problema knapsack, algoritmo de encriptado y desencriptado, seguridad del método. Métodos de ataque conocidos.

UNIDAD 4: Métodos de Autenticación
Autenticación de mensajes & autenticación de transmisores: conceptos y diferencias. Esquemas de Ong-Schnorr-Shamir y Rivest-Shamir-Adleman. Prueba de mínimo conocimiento o de conocimiento cero.

4.5- Programa y cronograma de clases
El desarrollo del programa se realizará mediante clases teórico-prácticas. A continuación, se muestra el cronograma tentativo según las unidades didácticas.

UNIDAD	CARGA HORARIA	FECHAS
1 - Fundamentos de la Criptografía	16	2 semanas (agosto)
2 – Criptografía Clásica	16	2 semanas (septiembre)
3 – Criptografía Moderna	48	7 semanas (septiembre y octubre)
4 – Métodos de Autenticación	24	3 semanas (noviembre)
TOTAL	**104**	---

Los trabajos prácticos previstos se muestran en la siguiente tabla:

TRABAJO PRACTICOS	UNIDAD
TP1 - Fundamentos de la Criptografía	1
TP2 – Criptografía Clásica	2
TP3 – Criptografía Moderna	3
TP4 – Métodos de Autenticación	4

5- BIBLIOGRAFÍA BASICA

- **Top Secret Data Encryption Techniques.** Gilbert Held. Sams Publishing
- **Cryptography: An Introduction To Computer Security.** Jennifer Seberry. Prentice-Hall
- **Criptografía. Técnicas de desarrollo para profesionales**. Ariel Maiorano. Alfaomega.
- **Understanding Cryptography. A Textbook for Students and Practitioners.** Christof Paar y Jan Pelzl. Springer, USA, 2010 (Digital).
- **Cryptography and data security**. Dorothy Elizabeth Robling Denning. Addison-Wesley, USA, 1982 (Digital).
- **Criptografía y Seguridad en Computadores.** Manuel J. Lucena López (Digital)

BIBLIOGRAFÍA COMPLEMENTARIA

- **Cryptography Made Simple.** Nigel P. Smart Springer, USA, 2016 (Digital).

6.- ESTRATEGIAS METODOLÓGICAS

6.1- Aspectos pedagógicos y didácticos:
En esta propuesta el aula se entiende como un espacio de diálogo y construcción, en el que se trabaja interactuando permanentemente. La comunicación se concreta con una estructura multipolar-bidireccional, donde tanto los estudiantes como el docente se consideran fuente de información. En base a ello se han seleccionado las siguientes técnicas metodológicas para poner en juego durante el desarrollo de los contenidos programáticos:

a) Discusión dirigida
b) Resolución de casos
c) Trabajo en grupo

d) Exposiciones abiertas
e) Uso de recursos educativos abiertos

La técnica metodológica por excelencia será el trabajo grupal que permite promover la construcción compartida del conocimiento y lograr así, no sólo la apropiación activa del mismo por parte de los miembros del grupo, sino también la indispensable socialización del estudiante, ya que toda su vida deberá transcurrir en contacto y en cooperación con sus semejantes.
Para mejorar la apropiación de conocimientos por parte de los estudiantes, se habilitarán oportunamente, en el aula virtual de la asignatura, recursos educativos abiertos (REA) desarrollados con eXe-learning sobre diferentes temas del contenido programático. Estos REA no sólo contendrán desarrollo teórico sino también ejemplos, material de actualidad vinculado, algunos ejercicios y tareas de autocomprobación.
En particular, considerando las actividades prácticas, los estudiantes resolverán 4 Trabajos prácticos cuyas temáticas están enunciadas en la tabla incluida en la sección 4.5.
Todas las actividades dispondrán de los recursos necesarios dentro del aula virtual de la asignatura para asegurar su cursado tanto de manera presencial como virtual (si fuera necesario).

6.2- Actividades de los Alumnos y de los Docentes:
La asignatura cuenta en su plantel docente solo con una Profesora Adjunta, que en general se desempeñará como facilitador del aprendizaje, observador del proceso de aprendizaje individual y grupal, propiciador de la comunicación y la colaboración, asesor individual y grupal, proporcionador de las técnicas de búsqueda de información y de los recursos que sean necesarios para que los estudiantes puedan desarrollar las actividades previstas. Específicamente sus funciones serán:

1) Desarrollar las clases teóricas.
2) Preparar material didáctico.
3) Atender consultas de los estudiantes.
4) Elaborar recursos educativos abiertos
5) Coordinar el desarrollo de los contenidos
6) Preparar enunciados de los trabajos prácticos y asistir a los estudiantes en sus resoluciones.
7) Preparar las evaluaciones y el material didáctico.
8) Elaborar un plan de evaluación.
9) Evaluar permanentemente.

Por otra parte, se espera que los estudiantes desarrollen las siguientes actividades:

1) Participar activamente en el desarrollo de las actividades teóricas y prácticas
2) Resolver responsablemente los ejercicios contenidos en los trabajos prácticos
3) Desarrollar responsablemente las actividades que se soliciten en aula virtual
4) Recorran los recursos educativos abiertos
5) Buscar y analizar material
6) Sintetizar
7) Elaborar respuestas con rigor científico
8) Trabajar en grupo
9) Estudiar independientemente

6.3- Mecanismos para la integración de docentes
Considerando la integración vertical y horizontal de esta asignatura con otras de la carrera, y a fin de facilitar la interrelación entre los docentes responsables de mismas, se prevé realizar al finalizar el cuatrimestre una reunión que permita evaluar lo ejecutado y acordar acciones de ajuste.

6.4- Recursos Didácticos
Los recursos didácticos necesarios para el desenvolvimiento de la asignatura son los siguientes:

- Bibliografía actualizada tanto para facilitar a los estudiantes la apropiación de contenidos teóricos y prácticos.
- Aula virtual en Moodle.
- Tiza, pizarrón, PC, cañón y software PowerPoint para presentar los diferentes temas de la teoría y práctica.
- Biblioteca de SECyT para posibilitar a los estudiantes el acceso a publicaciones de trabajos actuales dentro de la disciplina.

7- EVALUACIÓN

7.1- Evaluación Formativa

La evaluación formativa es de carácter continuo y está dirigida fundamentalmente a evaluar el proceso de enseñanza-aprendizaje seguido por los estudiantes. Dado lo expuesto, tal evaluación se llevará a cabo durante todo el desarrollo de la asignatura.

7.2- Evaluaciones Parciales

Evaluación	Contenidos	Tipo	Fecha Probable	Horas	Instrumento
PARCIAL 1	Temas incluidos en Unidades 1 y 2	Individual, escrita, prueba de desempeño, de contenido teórico-práctico	Primera semana de octubre	4	Cuestionario especialmente diseñado
Recuperatorio PARCIAL 1	Temas incluidos en Unidades 1 y 2	Individual, escrita, prueba de desempeño, de contenido teórico-práctico	Tercera semana de octubre	4	Cuestionario especialmente diseñado
PARCIAL 2	Temas incluidos en Unidad 3 y 4	Individual, escrita, prueba de desempeño, de contenido teórico-práctico	Segunda semana de noviembre	4	Resolución documentada de problemas
Recuperatorio PARCIAL 2	Temas incluidos en Unidad 3 y 4	Individual, escrita, prueba de desempeño, de contenido teórico-práctico	Tercera semana de noviembre	4	Resolución documentada de problemas
TOTAL	---	---	----	**16**	---

7.3.3- Criterios de Evaluación

Los criterios de evaluación a los que se someterá la documentación presentada son los siguientes:

a) Interpretación de enunciado a resolver (Adecuada)
b) Selección de las técnicas acordes con el problema a resolver (Adecuada).
c) Aplicación de las técnicas seleccionadas (Correcta).
d) Lógica aplicada para llegar a la solución (Simple y Correcta).
e) Presentación (la documentación entregada deberá ser clara, libre de errores de ortografía, ordenada, concisa y acotada a lo que se le solicita).

7.3.4- Escala de Valoración

La escala de valoración a emplear en todos los casos será cuantitativa del 1 al 10.

7.4- Evaluación Sumativa

7.4.1- Condiciones para lograr regularizar la Asignatura.

- Registrar un mínimo de 70 % de asistencia a las clases de la asignatura
- Aprobar parciales o sus correspondientes recuperatorios con un mínimo de 6 puntos.

7.5- Examen Final

La evaluación final será escrita u oral sobre los temas incluidos en la programación analítica.

7.6- Examen Libre

Los estudiantes libres deberán cumplir las siguientes etapas, cada una de ellas eliminatoria.

1 era. etapa) Aprobar una evaluación escrita de tipo práctica.
2 da. etapa) Aprobar una evaluación oral de tipo teórica.

……..

Dra. Rosanna Costaguta
Prof. Responsable de Cátedra
Agosto 2022