PLAN DE TRABAJO

LICENCIATURAS EN QUE SE IMPARTE

INFORMÁTICA 8 sem

DATOS DE LA ASIGNATURA

Nombre:	Cifrado
Clave(s):	0372)
Tipo:	Optativa
Plan de Estudios:	Plan 2012 (actualizado 2016)

FECHAS DEL SEMESTRE:

Inicio semestre:	12 de febrero de 2024
Fin del semestre:	21 de junio 2024
Plataforma educativa:	28 de febrero de 2024 Primer día para entrega de actividades en plataforma
Cierre de plataformas:	02 de junio de 2024 a las 23:00 hrs. Último día para entrega de actividades en plataforma
Periodo examen global:	15 y del 17 al 21 de junio 2024
Registro de calificaciones en actas:	
Consulta de calificaciones a partir del:	

DATOS GENERALES

Objetivo general:

El alumno obtendrá el conocimiento de las bases matemáticas sobre las que la teoría de la codificación moderna se sustenta, así también, los métodos y sistemas de codificación de la información en el contexto de la transmisión y el análisis de la información.

Contenido temático:

Tema		Teóricas	Prácticas
1	Introducción	2	0
2	Números primos	10	0
3	El anillo de los enteros módulo N	10	0
4	Criptografía de llave pública	12	0
5	Firma electrónica	4	0
6	Reciprocidad Cuadrática	10	0
7	Fracciones continuadas	8	0
8	Curvas elípticas	8	0
	Total	64	0
	Suma total de horas	64	

BIENVENIDA

Bienvenido a la materia de CIFRADO.

Espero que disfrutes de esta materia que es muy importante en el ámbito de la seguridad informática además de que la criptografía se aplica ya casi en todos los ámbitos de la informática, por lo que la utilizarás todos los días en el ejercicio de tu profesión, así como de la vida diaria.

PRESENTACIÓN DE LA ASIGNATURA

Estimados alumnos de la asignatura: CIFRADO.

Mi nombre en Germán Cervantes y seré tu asesor durante este semestre; por ello, mi labor es apoyarte en tu proceso de aprendizaje, resolviendo tus dudas y sugiriéndote cómo aprovechar los contenidos para que puedas obtener un mejor aprendizaje. No dejes de preguntar en las asesorías cuanto sea necesario y las veces que consideres pertinente. Esta materia es importante, ya que la criptografía se utiliza todos los días, desde tu teléfono celular para ver páginas web, autenticarte o en el ejercicio de tu profesión en muchas áreas de la informática para cubrir servicios de seguridad, sobre todo en temas de confidencialidad, integridad y control de acceso.
En este curso básicamente tendrás que resolver las actividades que se te presenten en cada UNIDAD; en donde encontraras instrucciones detalladas de cómo realizarlas, independiente mente de que se resuelvan las dudas conmigo.

FORMA EN QUE EL ALUMNO DEBE PREPARAR LA ASIGNATURA

Para realizar las actividades, deberás leer detalladamente las instrucciones de cada una de ellas. Una vez leídas y si tienes alguna duda, podemos aclararlo ya sea por mensajes o los días miércoles y viernes en el cubículo F-238 los miércoles y en el cubículo F-205 los viernes. Una vez aclarada cualquier duda, resolverás la actividad correspondiente y será revisada a la brevedad, para que puedas conocer si la realizaste correctamente y si puedes corregir algún detalle, en caso de que aplique.

Para la realización de tus actividades deberás cuidar tu **ortografía** y usar **fuentes oficiales** como: libros, revistas, artículos, etcétera. Recuerda hacer la cita en formato APA, ya que, si no lo haces incurrirás en plagio. https://www.revista.unam.mx/wp-content/uploads/3_Normas-APA-7-ed-2019-11-6.pdf .

Las actividades elaboradas con inteligencia artificial serán sancionadas según el criterio que establezca profesor.

ACTIVIDADES POR REALIZAR DURANTE EL SEMESTRE

Estimado alumno, para facilitar el aprendizaje de esta asignatura, en la sección de recursos de tu plataforma encontrarás un archivo llamado Videoclases, que contiene los vínculos a videos que tu profesor ha grabado para ti.

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
Unidad 1: Introducción	Actividad 1 (colaborativa)	Presentación de alumnos en el curso	N/A	5 pts
Unidad 1: Introducción	Actividad 2 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Cano, M. J. (2013). Inseguridad de la información: una visión estratégica. Colombia: Alfaomega. Díaz, G., Alzórriz, I., Sancristóbal, E., & Castro, M. (2014). Procesos y herramientas para la seguridad de redes. España: Universidad Nacional de Educación a Distancia.	7 pts
Unidad 2: Números primos	Actividad 1 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y	

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
			aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	
Unidad 3: El anillo de los enteros módulo N	Actividad 1 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	
Unidad 4: Criptografía de llave pública	Actividad 1 Lectura, video y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente. Video: https://youtu.be/5deqv3nEMmM	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
Unidad 4: Criptografía de llave pública	Actividad 2 Caso práctico	Utiliza la herramienta Kleopatra para realizar la práctica como se indica de manera detallada en la plataforma.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	
Unidad 5: Firma electrónica	Actividad 1 Lectura, video y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente. Video: https://youtu.be/R68IVb6PWm4	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. • Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	15 pts
Unidad 6: Reciprocidad cuadrática	Actividad 1 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and	10 pts

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
			implementations using C++. España: CRC Press. • Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	
Unidad 7: Fracciones continuadas	Actividad 1 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press. • Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	10 pts
Unidad 8: Curvas elípticas	Actividad 1 Lectura y Cuestionario	Consulta el material que se presenta en la plataforma y contesta el cuestionario correspondiente.	• Azad, S., & Pathan, A. K. (2015). Practical cryptography: algorithms and implementations using C++. España: CRC Press.	10 pts

Unidad	N° Actividad (consecutivo)	Descripción	Bibliografía sugerida	Valor (enteros)
			• Fúster, A., Hernández, L., Martín, A., Montoya, F., & Muñoz, J. (2012). Criptografía, protección de datos y aplicaciones: una guía para estudiantes y profesionales. México: Alfaomega.	
			Ponderación total de las actividades	90 pts

EXÁMENES

De acuerdo con los lineamientos del modelo educativo, tienes tres períodos a lo largo del semestre para presentar tus exámenes parciales (consulta las fechas en el calendario de inscripción a parciales y globales en el Portal SUAyED), tú decides el período en el que los realizarás. Si tu asignatura es optativa, deberás consultar los períodos y número de exámenes con tu asesor.

Para esta asignatura están programados de la siguiente manera:

- **Parciales:**

  Deberás entregar las actividades de aprendizaje de las unidades implicadas en cada parcial, **antes de que inicie el periodo de aplicación**. Es importante que te inscribas en cada periodo y cumplas con los lineamientos para su presentación.

NÚMERO	UNIDADES (que lo integran)	VALOR (núm. enteros)

1ro.	1,4	10 pts

- **Global. Examen más requisito**

Valor examen	Valor requisito	Apertura de requisito en plataforma	Entrega de requisito en plataforma	Aplicación de global
80 %	20 %	11 de junio de 2024	12 al 14 de junio de 2024	15 y del 17 al 21 de junio 2024

PORCENTAJES Y ESCALA DE EVALUACIÓN Y ACREDITACIÓN

Porcentajes de evaluación:

Concepto	Porcentajes
Actividades de aprendizaje	80 %
Actividades colaborativas	10 %
Exámenes parciales	10 %
Otro	XX %
Total	**100 %**

Escala de evaluación:

Rango	Calificación
1.00 a 5.99	**5**
6.00 a 6.54	**6**
6.55 a 7.54	**7**
7.55a 8.54	**8**
8.55 a 9.54	**9**
9.55 a 10.00	**10**

FUNCIONES DEL ASESOR

Por ser una modalidad abierta, tu asesor:

1. Será tu apoyo y guía de manera presencial para la resolución de dudas y desarrollo de las actividades; así mismo, por la mensajería de la plataforma educativa para dudas concretas.
2. Calificará y retroalimentará tus actividades de aprendizaje en plataforma educativa en un lapso no mayor a diez días hábiles después de la entrega.
3. Te recomendará recursos didácticos adicionales para ampliar tu conocimiento. No es su obligación facilitarte: copias, archivos digitales o proporcionarte ligas directas de la BIDI.
4. Enviará tu calificación al finalizar el semestre de manera personalizada.

DATOS DEL ASESOR O GRUPO DE ASESORES

Nombre	Correo electrónico
Germán Ignacio Cervantes González	gcervantes@fca.unam.mx

Enseñar no es transferir conocimiento, sino crear las posibilidades para su propia producción o construcción.

Paulo Freire