Programa de Matemática discreta 2

1. NOMBRE DE LA UNIDAD CURRICULAR

Matemática Discreta 2.

2. CRÉDITOS

9 créditos.

3. OBJETIVOS DE LA UNIDAD CURRICULAR

El estudiante deberá:

- Comprender y manejar ciertas estructuras algebraicas como son los Grupos. Se hará especial énfasis en los grupos finitos, por su interés en la informática.
- Fortalecer la capacidad de realizar razonamientos por analogía en problemas planteados en éste y en el curso de Matemática Discreta 1.

4. METODOLOGÍA DE ENSEÑANZA

Cuso teórico practico de 3 horas semanales de clases teóricas, 3 horas semanales de clases prácticas y 4 horas semanales de dedicación domiciliaria.

5. TEMARIO

1. Anillo de enteros, Divisibilidad y Aritmética modular.
2. Grupos, Subgrupos, Grupos cíclicos, Teorema de Lagrange, Homomorfismos, Subgrupos normales, Grupos cociente, Teoremas de isomorfismos, Grupos Simétricos.
3. Aplicaciones a la criptografía: sistemas clásicos, sistemas de clave privada, sistemas de clave publica RSA (introductorio).

6. BIBLIOGRAFÍA

Tema	Básica	Complementaria
Anillo de enteros, Divisibilidad y Aritmética modular. Grupos, Subgrupos, Grupos cíclicos, Teorema de Lagrange. Aplicaciones a la criptografía: sistemas clásicos, sistemas de clave privada, sistemas de clave publica RSA.	(1)	(1)
Grupos normales, grupos cociente, Teoremas de isomorfismo.	(2)	(1)

6.1 Básica

1. M. Pereira, G. Rama. Notas de Matemática Discreta 2. Uruguay, Montevideo.
2. A. Solotar, M. Farinatti, M. Suárez-Álvarez, Anillos y sus categorías de representaciones (notas)

6.2 Complementaria

1. I.N. Herstein. Algebra abstracta. Crupo Editorial Iberoamericano. Mexico.

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos: Es imprescindible un dominio de los temas correspondientes al programa de Matemática Discreta 1. Es necesario un buen dominio de los temas correspondientes al álgebra lineal y al calculo diferencia e integral en una variable.

7.2 Conocimientos Previos Recomendados:

ANEXO A
Para todas las Carreras

A1) INSTITUTO

El curso es dictado por el IMERL

A2) CRONOGRAMA TENTATIVO

Semana 1	División entera y sistemas de numeración.
Semana 2	Divisibilidad y máximo común divisor. Igualdad de Bézout y aplicaciones. Pruebas de irracionalidad. Algoritmo de Euclides extendido (con substitución).
Semana 3	Algoritmo de Euclides extendido (con matrices). Ecuaciones Diofánticas lineales en dos variables. Soluciones naturales (Problema de Frobenius, de las monedas o de los sellos). Teorema fundamental de la Aritmética.
Semana 4	Teorema fundamental de la Aritmética. Congruencias: Definiciones y propiedades. Propiedades de las Congruencias. Algunas aplicaciones: cálculo de restos de potencias y criterios de divisibilidad.
Semana 5	Ecuaciones con congruencias. El inverso modular. El (pequeño) teorema de Fermat y aplicación a la exponenciación modular. Sistema de congruencias y el Teorema chino del resto. Exponenciación y teoremas de Fermat y de Euler. Exponenciación rápida.
Semana 6	La propiedad multiplicativa de la función phi de Euler. Teorema de Fermat-Euler y aplicación a la exponenciación modular. Algoritmo de exponenciación rápida.
Semana 7	Repaso
Semana 8	Grupos: Definición, ejemplos y propiedades. Tablas de Cayley. Grupo de permutaciones Sn. Grupo dihedral Dn.
Semana 9	Grupo aditivo de los enteros módulo n. Grupo multiplicativo de enteros invertibles módulo n. Subgrupos.. Grupos cíclicos y generadores.
Semana 10	Órdenes de elementos y propiedades. Teorema de Lagrange y corolarios. Grupos normales y Grupos cociente.
Semana 11	Homomorfismos e isomorfismos de grupos. Teoremas de isomorfismos.
Semana 12	Raíces primitivas.
Semana	Criptosistemas de César y de Vigenère. Criptosistemas de clave

13	privada, métodos de intercambio de clave (Diffie-Hellman).
Semana 14	Criptosistemas de clave pública RSA. Método de Fermat para factorización.
Semana 15	Repaso.

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

La evaluación de la unidad curricular consistirá en dos parciales teórico-prácticos teórico-prácticos de 40 y 60 puntos.
Del puntaje total obtenido al sumar los resultados de los parciales surgirán tres posibilidades:

a) exoneración del examen final si el estudiante obtiene un puntaje mayor o igual a 60

b) aprobación del curso si el estudiante obtiene un puntaje mayor o igual a 25 y menor a 60

c) insuficiencia en el curso (por lo cual reprueba) si el estudiante obtiene un puntaje menor a 25.

A4) CALIDAD DE LIBRE

La unidad curricular permite acceder a la calidad de libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

Sin cupo