UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICA
PLAN 2009

CRIPTOGRAFÍA RSA

CARRERA: LICENCIATURA EN CIENCIAS MENCION MATEMATICA PURA

I. IDENTIFICACION

1.	Código	:	Electiva
2.	Horas Semanales de Clase	:	4
	2.1. Teóricas	:	2
	2.2. Prácticas	:	2
3.	Crédito	:	3
4.	Pre-Requisito	:	Ninguno

II. JUSTIFICACIÓN

Los problemas matemáticos en las industrias y empresas pueden surgir en variados contextos, la mayoría de las veces aparecen probablemente definidos y en evolución. Los matemáticos son reconocidos porque pueden ver y entender la naturaleza interior de un problema; determinar qué aspectos interesan y cuales no; y desarrollar una representación matemática que refleje la esencial del problema, que puede ser resuelta numéricamente y que permite estimar comportamientos futuros.

En relación a las oportunidades de los matemáticos en ambientes no académicos, éstos muchas veces no hacen lo mejor posible para su disciplina y para ellos mismos.

Muchas veces, las ramas de la matemática que conocemos hoy en día, surgieron como resultado de un juego. ¿Quién no habrá cambiado una palabra, frase, mensaje en su niñez por un similar, utilizando otras letras, números, en síntesis, otros símbolos? Al hacer esto, nos metemos en la criptografía, sin saberlo tal vez. Éste es un ejemplo básico de cómo una rama de la matemática puede ser utilizado en forma sencilla y de mucha utilidad práctica.

III. OBJETIVOS

Comprender los procedimientos que se emplean para la utilización del sistema RSA.

1. Aplicar nociones elementales de la Teoría de Números para la resolución de algunos problemas de criptografía.
2. Manejar con presición los procedimientos de codificación y de decodificación de informaciones.
3. Demostrar teoremas relacionados con el sistema RSA.
4. Describir situaciones reales donde se aplica el sistema RSA.

IV. **CONTENIDO**

A. UNIDADES PROGRAMATICAS

1. **CONJUNTO DE NÚMEROS ENTEROS**
2. **GENERACIÓN DE NÚMEROS PRIMOS**
3. **TEST DE PRIMALIDAD**
4. **CRIPTOGRAFÍA RSA**

V**. METODOLOGÍA**

- Exposición oral
- Revisión o consulta bibliográfica

VI**. MEDIOS AUXILIARES**

- Textos, materiales de consulta
- Medios audiovisuales

VII**. EVALUACIÓN**

- La evaluación se regirá conforme al reglamento de la FaCEN