PROPUESTA DE PROGRAMA DE ASIGNATURA "Curvas Elípticas en Criptografía"

1. Nombre de la asignatura. Curvas elípticas en criptografía.

2. Créditos. 3

Objetivo de la asignatura.
Presentar a los estudiantes con los principios básicos del uso de curvas elípticas en criptografía.

3. Metodología de enseñanza.

Se darán 15 hs. presenciales, desglosadas en 12 hs. de clases teóricas y 3 hs. de consultas. Se estiman 12 hs. adicionales de trabajo individual del estudiante para asimilar el contenido de las clases. El examen final domiciliario con ejercicios a resolver tiene una carga estimada de trabajo de 25 hs.

4. Temario.

1. Curvas elípticas como grupos
2. El tamaño de una curva elíptica
3. Calcular el tamaño
4. Polinomios de división
5. Logaritmo discreto sobre curvas elípticas especiales
6. Seguridad práctica con clave pública
7. Las curvas NIST

5. Bibliografía.

Material presentado por el profesor basado en el nuevo libro que está escribiendo sobre el tema.

6. Conocimientos previos recomendados.

Fundamentos de álgebra, algoritmia y programación.

Anexo

1) Cronograma tentativo: Se darán cuatro clases teóricas de tres horas cada una. El desglose de horas por tema es el siguiente:

1. Curvas elípticas como grupos (1 hora)
2. El tamaño de una curva elíptica (2 horas)
3. Calcular el tamaño (2 horas)
4. Polinomios de división (2 horas)
5. Logaritmo discreto sobre curvas elípticas especiales (2 horas)
6. Seguridad práctica con clave pública (2 horas)
7. Las curvas NIST (1 hora)

2) Modalidad del curso y procedimiento de evaluación.

Proyecto final con ejercicios a resolver individualmente.

3) Materia para Ingeniería en Computación.

Arquitectura, Sistemas Operativos y Redes de computadores.

4) Previaturas para Ingeniería en Computación.

Para el Plan 97 se exige Geometría y Álgebra Lineal 1 (examen), Geometría y Álgebra Lineal 2 (examen), Matemática Discreta 1 (examen), Matemática Discreta 2 (examen), Probabilidad y Estadística (Examen) y Programación 3 (curso).

Esta asignatura no puede ser tomada como parte del plan 87.

5) Esta asignatura no adhiere a resolución del consejo sobre condición de libre.