CRIPTOGRAFÍA

Al terminar la actividad el asistente podrá (descripción de objetivos de la actividad):

Comprender la mayoría de los criptosistemas empleados en la actualidad para garantizar seguridad informática, conocer su complejidad computacional, el grado de seguridad que ofrecen y sus debilidades.

Conocimientos previos necesarios:

No se requieren conocimientos específicos. Únicamente una formación técnica y cierta madurez en Matemáticas.

Acción formativa dirigida a:

Materia destinada estudiantes de Ingeniería de Telecomunicación, de Ciencias de la Computación y de Matemáticas, y a cualquier persona de formación técnica que tenga interés en la materia.

Temas a desarrollar:

1. Seguridad de la Información.
1.1 Introducción a la Seguridad de la Información.
1.2 Criptografía clásica.
1.3 Servicios de seguridad.
1.4 Tipos de cifrado.

2. Cifrado en flujo.
2.1 El cifrado de VERNAM.
2.2 Cifrado en flujo.
2.3 Registros de desplazamiento.
2.4 El algoritmo de Berlekamp-Massey.

3. Cifrado en bloque simétrico con clave secreta.
3.1 Cifrado en bloque simétrico.
3.2 El cifrado Data Encryption Standard (DES).
3.3 Modos de cifrado.
3.4 El cifrado Advanced Encryption Standard (AES).
3.5 Funciones hash: Algoritmos SHA.

4. Fundamentos matemáticos
4.1 Teoría de números.
4.2 Factorización de enteros.
4.3 Generación de números primos.
4.4 Cuerpos finitos.
4.5 Logaritmo discreto en un cuerpo finito.

5. Cifrado en bloque simétrico con clave pública.
5.1 Cifrado de clave pública.
5.2 Intercambio de claves de Diffie-Hellmann.
5.3 Algoritmo RSA (Rivest, Shamir, Adleman).
5.4 Algoritmo ElGamal.
5.5 Firma digital: Algoritmo DSA.

6. Introducción a los criptosistemas elípticos.
6.1 Fundamento de los criptosistemas con curvas elípticas.
6.2 El problema del logaritmo discreto.
6.3 Criptografía con curvas elípticas.
6.4 Codificación de datos en curvas elípticas.

Condiciones generales	
La acción formativa cumple las siguientes condiciones generales: http://www.cfp.upv.es/cond_gen?4	
Organizadores:	
Responsable de actividad	ALICIA ROCA MARTINEZ
Datos básicos:	
Tipo de curso	FORMACIÓN ESPECIFICA
Estado	TERMINADO
Duración en horas	25 horas presenciales, 5 horas a distancia
Créditos ECTS	3
Información técnica docente	Materia destinada a estudiantes de Ingeniería de Telecomunicación, de Ciencias de la Computación y de Matemáticas, y a cualquier persona de formación técnica que tenga interés en la materia.
Dónde y Cuándo:	
Dónde	VALÈNCIA
Horario	TARDE
Observaciones al horario	Jueves 16:00 a 18:00, los días 7, 14, 21, 28 de febrero, 7, 14, 21, 28 de marzo, 4 y 11 de abril. Viernes 15:30 a 18:00, los días 22 de febrero, 8 de marzo
Lugar de impartición	Aulas 2.5, 2.9 y 2.13 CFP
Fecha Inicio	7/02/19
Fecha Fin	11/04/19
Datos de matriculación:	
Matrícula desde	23/01/19
Inicio de preinscripcion	8/01/19
Mínimo de alumnos	5
Máximo de alumnos	25
Precio	200,00 euros
Observaciones al precio	150,00 € - Alumno UPV 150,00 € - Alumni UPV Plus 150,00 € - Personal UPV 200,00 € - Público en general
Profesorado:	
ROCA MARTINEZ, ALICIA	