Curso Online de Especialización
El Algoritmo RSA: Fortalezas y Debilidades en el Mundo Real

Orientado a: Estudiantes de ingeniería, sistemas y tecnologías de la información
Profesores de seguridad informática y criptografía
Responsables de seguridad
Cuerpos y fuerzas de seguridad del estado
Administración pública y funcionarios del estado
Ingenieros y profesionales de la seguridad

Impartición: online, en español y con plataforma WebEx
Duración: **8 horas**
Certificado de Aprovechamiento: **8 CPE** otorgado por Criptored
Formato: 4 módulos, 4 lecciones de dos horas cada una.
Fecha: a anunciarse próximamente
Días-Horas: Lunes, Martes, Miércoles y Jueves de 16:00 a 18:00 hrs.
Profesores: Dr. Jorge Ramió Aguirre y Dr. Alfonso Muñoz Muñoz
Contacto: jramio@eui.upm.es
Registro: info@eventos-creativos.com

TEMARIO

Módulo 1: Los principios del algoritmo RSA y la criptografía pública (2 horas)
1.1. Historia de la clave pública y RSA
1.2. Algoritmo de generación de claves
1.3. Características de las claves: claves parejas
1.4. Operaciones de cifrado y firma
Profesor: **Jorge Ramió**

Módulo 2: Generación segura de claves RSA. Diseño y configuración (2 horas)
2.1. Parámetros e, d, p y q
2.2. Generación de claves con OpenSSL
2.3. Optimización de RSA. El teorema chino del resto
2.4. Programando RSA: librerías
Profesores: **Jorge Ramió**, **Alfonso Muñoz**

Módulo 3: Seguridad del algoritmo RSA (2 horas)
3.1. Ataques por factorización entera
3.2. Ataques por cifrado cíclico
3.3. Ataques por paradoja del cumpleaños
3.4. Ataques por e pequeño
Profesor: **Jorge Ramió**

Módulo 4: Seguridad de la criptografía pública en el mundo real. Atacando RSA (2 horas)
4.1. Autoridades de certificación y PKI
4.2. Protocolo SSL
4.3. Dispositivos Hardware (tarjetas inteligentes, tokens, etc.)
4.4. Criptoanálisis acústico y variantes
Profesor: **Alfonso Muñoz**

PRECIOS

Curso completo en formato individual: 160 € + 21% IVA
Gratis un ejemplar del libro "Cifrado de las comunicaciones digitales. De la cifra clásica al algoritmo RSA" de la editorial 0xWORD

Curso completo en formato para 2 asistentes: 240 € + 21% IVA
Gratis un único ejemplar del libro "Cifrado de las comunicaciones digitales. De la cifra clásica al algoritmo RSA" de la editorial 0xWORD
Un único enlace WebEx

Los gastos de envío del libro de RSA son gratuitos dentro de España. Para fuera de España tiene un coste, consultar con info@eventos-creativos.com.

Curso completo en formato grupo (máximo 5 asistentes): 400 € + 21% IVA
Gratis un único ejemplar del libro "Cifrado de las comunicaciones digitales. De la cifra clásica al algoritmo RSA" de la editorial 0xWORD
Un único enlace WebEx

Para grupos mayores que 5 asistentes, consultar en registro: info@eventos-creativos.com

Importante: Los residentes fuera de España están exentos de pagar el impuesto del 21%