CORSO CRITTOGRAFIA

RELATORE: Alberto Venzo

26 e 27 NOVEMBRE 2026 - dalle 14:00 alle 18:00

SALA CAPRIATE - CORSO D'AUGUSTO, 231 Rimini

Saluti ing. Adriano Angelini Coordinatore commissione Informazione

PROGRAMMA - GIORNATA 1

26 NOVEMBRE 2026 - dalle 14:00 alle 18:00

1. **Introduzione alla crittografia**

Breve storia di come la crittografia nasce e di come la sua importanza ha influenzato e continuerà a influenzare l'economia e il lavoro.

2. **Riferimenti normativi**

Oltre alle principali direttive e norme europee in vigore (CRA e NIS2) verrà introdotto lo standard ISO27001 e come questo può portare effettivamente ad una migliore consapevolezza e a pratiche migliori in tema di sicurezza informatica. Introduzione di ulteriori riferimenti normativi.

3. **Fondamenti della crittografia moderna**

Vengono introdotti i fondamenti principali che la crittografia moderna soddisfa:

- **Integrità**
- **Confidenzialità**
- **Disponibilità**

Descrizione delle teorie che consentono di garantirne l'efficacia di una soluzione crittografica, come l'entropia e la generazione casuale o pseudo-casuale di numeri.

CREDITI FORMATIVI INTERO CORSO:

Architetti: 8 CFP

Ingegneri: 8 CFP

Periti: 8 CFP

Geometri: 8 CFP

REGISTRATI

CORSO CRITTOGRAFIA

RELATORE: Alberto Venzo

SALA CAPRIATE - CORSO D'AUGUSTO, 231 Rimini

PROGRAMMA - GIORNATA 2

27 NOVEMBRE 2026 - dalle 14:00 alle 18:00

1. Principali algoritmi crittografici

Introduzione delle principali categorie di algoritmi di crittografia:

- **Algoritmi simmetrici con cifrary a blocco**
- **Algoritmi stream**
- **Algoritmi asimmetrici**

Descrizione degli standard usati in applicazioni reali, con esempi pratici di codice:

- **Advanced Encryption Standard (AES)**
- **Secure Hash Algorithm (SHA)**
- **Transport Layer Security (TLS)**

2. Principali soluzioni crittografiche per sistemi embedded

Anche i sistemi embedded, che ormai interessano non solo contesti di nicchia, hanno bisogno di uno sviluppo di algoritmi crittografici per poter essere commercializzati e manutenuti. Introduzione dei principali strumenti per firmare digitalmente un programma, in modo da evitare che personale non autorizzato possa prendere il controllo del sistema da remoto o con manomissione fisica del dispositivo.

3. Crittografia quantistica e PQC

Introduzione alla nuova sfida che si andrà a prospettare in tema di sicurezza digitale, in cui saranno presenti anche calcolatori quantistici, alcuni nuovi algoritmi di "Post Quantum Cryptography" (PQC), con un analisi su quali scelte utilizzare e quando.

Con il Patrocinio

FONDAZIONE RETE PROFESSIONI TECNICHE RIMINI

In collaborazione

ordine degli architetti, pianificatori, paesaggisti e conservatori della provincia di rimini

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI RIMINI

ORDINE DEI PERITI INDUSTRIALI della Provincia di Rimini

Collegio Provinciale Geometri e Geometri Laureati di Rimini