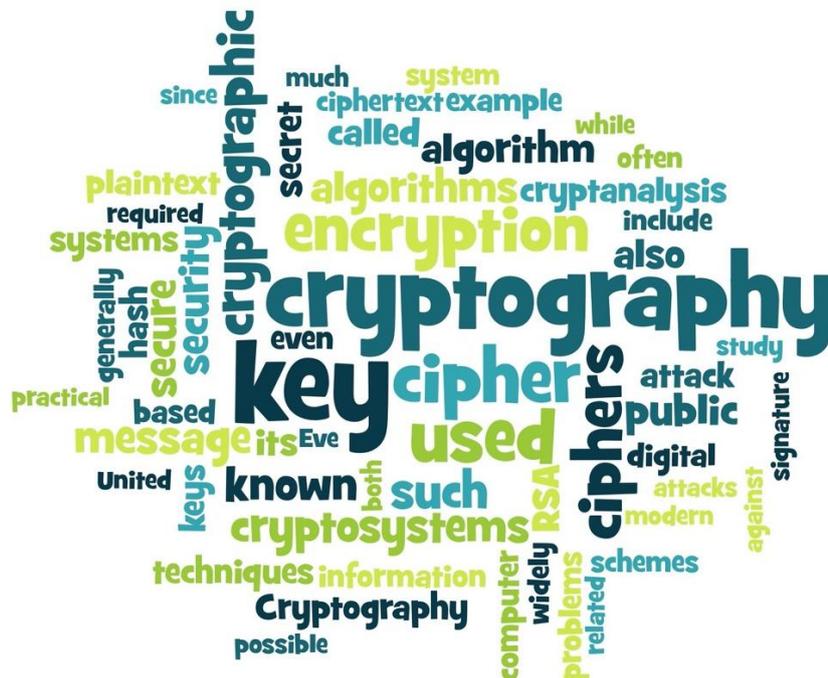


organizza:

**II SEMINARIO GRATUITO
EVENTO FORMAZIONE FAD SINCRONA CIRC. CNI. 537/2020**

"“Gli strumenti per proteggere e cifrare i nostri dati digitali: la Crittografia”.”



Finalità del seminario

Siamo abituati a pensare che la crittografia sia una materia astrusa, riservata ai matematici e che non riguarda gli utenti comuni.

In realtà la crittografia esiste da secoli ed oggi – con l'informatica di massa e l'uso di internet – viene utilizzata in moltissime nostre attività. Possiamo affermare che ogni giorno e più volte al giorno usiamo la crittografia: quando inviamo un messaggio con WhatsApp, così come quando scriviamo un email o navighiamo nel web.

In questo seminario faremo una breve storia della crittografia. Illustreremo poi i principi base della crittografia moderna ed i suoi molti utilizzi.

Lo scopo del seminario non è certamente quello di diventare esperti delle tecniche e degli algoritmi crittografici (che sono molti e complessi), ma capire come e quando usarla. Perché questi strumenti sono utili, anzi necessari, per proteggere i nostri dati e le nostre comunicazioni, ancor di più oggi con gli obblighi di sicurezza imposti dal GDPR.

QUANDO

VENERDI' 17 SETTEMBRE 2021 ore 14.30 -18.30

DOVE

Evento Webinar Online con la Piattaforma GoToWebinar

Iscrizione attraverso il portale www.iscrizioneformazione.it. In seguito all'iscrizione verrà inviato due giorni prima dell'evento un Link di registrazione alla piattaforma GoToWebinar sulla mail indicata nel portale [Iscrizione Formazione al momento della registrazione](http://www.iscrizioneformazione.it). L'utilizzo del Link consentirà l'accesso alla stanza virtuale.

PROGRAMMA DEL CORSO

14.30: Collegamento alla piattaforma virtuale e Apertura dei lavori del Presidente Ordine degli Ingegneri di Forlì-Cesena

14:35 – 16:30 - Inizio momento formativo:

- Cosa è la crittografia
- Cifrari storici: dal codice di Atbash al cifrario di Cesare e Leon Battista Alberti
- La cifratura polialfabetica: il cifrario di Vigenère
- Alan Turing e la macchina Enigma
- La nascita della crittografia moderna: il Principio di Kerckhoffs
- Crittografia simmetrica (a chiave privata)
- Crittografia asimmetrica (a chiave pubblica o a doppia chiave): Diffie-Hellman e RSA
- Gli algoritmi di hashing. Il salt

16:30 – 16:40 : Pausa

16.40 – 18.30: Applicazioni pratiche di crittografia:

- la crittografia end-to end (2E2)
- la PGP (Pretty Good Privacy)
- la posta elettronica certificata (PEC)
- comunicazioni sicure su Internet: Https e TLS
- la firma digitale
- i certificati digitali. Le CA (Certification Authority)
- La crittografia come misura di sicurezza per il GDPR

DOCENTE: Giorgio Sbaraglia, ingegnere, svolge attività di consulenza e formazione per la sicurezza informatica e per il GDPR.

Tiene corsi su questi temi per molte importanti società italiane di formazione, tra le quali la 24Ore Business School(<https://www.24orebs.com/docenti/giorgio-sbaraglia>).

È membro del Comitato Scientifico CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato “Innovation Manager” da RINA.

Ricopre incarichi di DPO (Data Protection Officer) presso aziende e Ordini Professionali.

È autore dei libri:

- **“GDPR kit di sopravvivenza”** (Editore goWare),
- **“Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!”** (Editore goWare),
- **“iPhone. Come usarlo al meglio. Scopriamo insieme tutte le funzioni e le app migliori”** (Editore goWare).

Collabora con **CYBERSECURITY360** <https://www.cybersecurity360.it/about> testata specialistica del gruppo Digital360 per la **cyber security**.

Scrive anche per ICT Security Magazine <https://www.ictsecuritymagazine.com> e per www.agendadigitale.eu/ e per la rivista **CLASS**.

Il seminario è riservato ai soli iscritti all’Ordine Ingegneri della Provincia di Forlì-Cesena e riconoscerà ai partecipanti n. 4 CFP