



**Università  
degli Studi  
di Palermo**



## **PERCORSO PLS/POT Laboratorio di Crittografia Moderna**

**Istituzione:** Università degli Studi di Palermo - Dipartimento di Matematica e Informatica

**Anno scolastico di riferimento:** 2023/2024 – 2024/25 – 2025/26

**Referente dell'Istituzione per il PLS/POT:** Elena Toscano

**Docente del Percorso:** Cinzia Cerroni/Francesca Benanti

**Titolo del Percorso:** Laboratorio di Crittografia Moderna

**Scuole coinvolte:** Scuole secondarie di secondo grado

**Numero Alunni partecipanti:** 25

**N. Ore Percorso:** 5 ore come approfondimento del percorso PNRR dal titolo "Laboratorio di Storia e Teoria della Crittografia"

**Orario di svolgimento:** da concordare

**Tipologia di formazione erogata:**

- in presenza o in modalità mista o a distanza
- Comune in cui si svolge: Palermo



**Università  
degli Studi  
di Palermo**



**Data di avvio del Programma/Percorso:** da definire

**Data di fine del Programma/Percorso:** da definire

**Luogo di svolgimento:** da definire

**Contenuto del Percorso:**

Pensato come approfondimento del percorso PNRR “Laboratorio di Storia e Teoria della Crittografia”, il presente percorso si propone come obiettivo la descrizione delle idee fondamentali che stanno alla base della Crittografia Moderna quali il concetto di algoritmo di cifratura a chiave asimmetrica, la firma digitale ed i problemi matematici strettamente connessi come l’aritmetica modulare, i numeri primi e la loro distribuzione, l’algoritmo delle divisioni successive. Verrà anche descritto in dettaglio l’algoritmo RSA. Le attività si svolgeranno in laboratorio informatico con l’uso del pacchetto Office e di altri strumenti.