PERCORSO PLS/POT “Laboratorio di Storia e Teoria della Crittografia

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 Storia e Teoria della Crittografia

Scuole coinvolte: Scuole Secondarie di Secondo Grado

Numero Alunni partecipanti: 25

N. Ore Percorso: 20 ore

Orario di svolgimento: da concordare

Tipologia di formazione erogata:

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

La costruzione di messaggi segreti è antica, forse quanto la comunicazione tra gli uomini. Seguendo il percorso storico si svolgeranno attività di cifratura e decifratura di testi facendo uso dei principali cifrari a sostituzione mono e polialfabetica (cifrario di Cesare, cifrario di Leon Battista Alberti, di Vigeneré), dei cifrari a trasposizione e del moderno RSA (crittografia a chiave pubblica). Si utilizzeranno inoltre, tecniche di crittoanalisi statistica per la decifrazione. Queste attività si svolgeranno in laboratorio informatico, con l'uso del pacchetto office e di altri strumenti. Si tratterà anche la storia moderna della crittografia legata alle Macchine Enigma e ad Alan Turing.