Ministero dell'Istruzione, dell'Università e della Ricerca

Istituto di Istruzione Superiore "Benedetto Castelli"
Istituto Tecnico Industriale, Istituto Professionale, Scuola in Ospedale
Via Cantore, 9 25128 Brescia tel 030/3700267 fax 030/395206 e-mail segreteria@itiscastelli.it

Corso di crittografia con Python

Attestato di frequenza

L'allievo _____ ha partecipato a ____ incontri pomeridiani su un totale di 5 del corso che si è tenuto nel nostro istituto a marzo-aprile 2015.

Contenuti del corso

- Introduzione storica alla crittografia.
- Problematiche, campi d'applicazione, panoramica sulle tecniche utilizzate.
- Modello crittografico.
- Algoritmi crittografici "storici": cifrari per sostituzione e a trasposizione.
- Utilizzo di Python da terminale.
- Realizzazione di un semplice cifrario per apprendere le basi del linguaggio Python.
- Implementazione del cifrario di Cesare e tecniche di crittoanalisi basate su attacchi a forza bruta.
- Storia e implementazione del cifrario Enigma, con l'utilizzo di classi in Python.
- Cenni sugli algoritmi a chiave asimmetrica.
- Scambio di chiavi di Diffie-Hellman.
- Generazione di numeri primi grandi con algoritmo di Rabin-Miller.
- Algoritmo a chiave asimmetrica RSA.

Il docente organizzatore
Alessandro Bugatti