MINISTERO DELL'ISTRUZIONE
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
LICEO SCIENTIFICO STATALE
<VITO VOLTERRA>
00043 Ciampino (Roma) – Via dell'Acqua Acetosa, 8/A – sito web: liceovolterra.edu.it
Tel. 06/121126380 Fax 06/7963473 - CF 80200130583 – C.M. RMPS29000P – e-mail: rmps29000p@istruzione.it

Ciampino, 29/11/2022 Circ. n. 155

Agli studenti delle classi quarte
Ai docenti
Al personale ATA
Al DSGA
Al Sito WEB del Liceo

OGGETTO: Laboratorio di crittografia.

Si comunica che nel mese di **gennaio 2023** sarà attivato il progetto "Laboratorio di crittografia", inserito nel PTOF della scuola.

Il progetto è rivolto agli studenti interessati delle classi quarte per un numero massimo di 25 partecipanti, sarà svolto in presenza e strutturato in una serie di 4 incontri pomeridiani.

Il corso, usando la metodologia della didattica laboratoriale, si propone come obiettivo principale una introduzione alla crittografia e alla teoria dei codici, mostrando come il processo di codifica/decodifica di un messaggio cifrato si basi su un esempio di matematica discreta: l'aritmetica modulare. L'attività sarà svolta sollecitando l'analisi e la discussione dei punti di forza e di debolezza delle ipotesi formulate dagli studenti sulla base di tavole ed esercizi a loro proposti.

Programma del corso

Prima Lezione 23 gennaio 2023 dalle 14.30 alle 16.30

A partire dal sistema crittografico di Cesare, verrà ricordata la nomenclatura principale relativa alla crittografia e verrà introdotta la definizione di congruenza tra numeri interi. Si osserverà come l'utilizzo dell'addizione negli interi modulo n semplifichi l'utilizzo del sistema di Cesare. L'analisi delle frequenze illustrerà la debolezza di ogni sistema crittografico che si basi sull'utilizzo di un unico alfabeto cifrante.

Seconda Lezione 30 gennaio 2023 dalle 14.30 alle 16.30

L'introduzione del prodotto modulo n permetterà di introdurre i cifrari affini, ottenuti componendo prodotto e somma. Si osserverà che non tutti gli elementi possono essere utilizzati per moltiplicare e si illustrerà il problema di caratterizzare le chiavi.

Terza Lezione 6 febbraio 2023 dalle 14.30 alle 16.30

MINISTERO DELL'ISTRUZIONE
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
LICEO SCIENTIFICO STATALE
<VITO VOLTERRA>
00043 Ciampino (Roma) – Via dell'Acqua Acetosa, 8/A – sito web: liceovolterra.edu.it
Tel. 06/121126380 Fax 06/7963473 - CF 80200130583 – C.M. RMPS29000P – e-mail: rmps29000p@istruzione.it

Verrà introdotto ed utilizzato un esempio di cifrario polialfabetico, il cifrario di Vigenere.

Quarta lezione 13 febbraio 2023 dalle 14.30 alle 16.30

Il cifrario di Vigenere sarà perfezionato con il cifrario One Time Pad (o cifrario di Vernam), l'unico cifrario del quale possiamo dimostrare matematicamente l'inviolabilità; verranno discussi pregi e difetti del nuovo sistema. Introduzione al sistema di cifratura RSA.

Per le iscrizioni inviare una email entro il **22 dicembre 2022** alla prof.ssa Marina Pesce (marina.pesce@liceovolterra.edu.it) o alla prof.ssa Laura Sopranzi (laura.sopranzi@liceovolterra.edu.it) specificando nome, cognome e classe.

Il laboratorio sarà attivato solo con un numero minimo di 15 studenti iscritti.

Il Dirigente Scolastico
Emilia D'Aponte
(firma autografa sostituita a mezzo stampa ex art. 3 co. 2 D. lgs. 39/93)