03/02/2018

Nono ciclo

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti da Febbraio a Marzo 2018

Modulo di Matematica - ITIS “E. Fermi”

Prof. Roberto Zanasi – ITIS “E. Fermi”

Venerdì 16/2/2018 Ore 14,00-16,30	**ALGORITMI DI CRITTOGRAFIA A CHIAVE PUBBLICA** Preliminari teorici (la matematica che si usa; la crittografia classica): - aritmetica modulare (l'aritmetica dell'orologio) Esercitazioni al computer
Lunedì 05/03/2018 Ore 14,00-16,30	Il piccolo teorema di Fermat (aiuta nel calcolo dei resti quando si divide un intero per un numero primo). La funzione di Eulero ed il teorema di Eulero (generalizzazione del teorema di Fermat)
Venerdì 09/03/2018 Ore 14,00-16,30	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Lunedì 12/3/2018 Ore 14,00-16,30	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Venerdì 23/3/2018 Ore 14,00-16,30	The magic words are “squeamish ossifrage” Il concetto di Zero Knowledge. Partita a “mental poker”.

La coordinatrice del progetto

Anna Maria Prandini