29/10/2018

Decimo ciclo

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti da Novembre 2018 a Gennaio 2019

Modulo di Matematica - ITIS “E. Fermi”

Prof. Roberto Zanasi – ITIS “E. Fermi”

Lunedì 05/11/2018 Ore 14,15-16,15	**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
Mercoledì 14/11/2018 Ore 14,15-16,15	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)
Mercoledì 28/11/2018 Ore 14,15-16,15	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Lunedì 17/12/2018 Ore 14,15-16,15	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
Lunedì 07/01/2019 Ore 14,15-16,15	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Martedì 15/01/2019 Ore 14,00-16,00	The magic words are “squeamish ossifrage” Il concetto di Zero Knowledge. Partita a “mental poker”.

La coordinatrice del progetto

Anna Maria Prandini