20/1/2016

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti da Febbraio ad Aprile 2016

Modulo di Matematica - ITIS “E. Fermi”

Prof. Roberto Zanasi – ITIS “E. Fermi”

Martedì 23/2/2016 Ore 14,30-16,30	**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
Martedì 1/3/2016 Ore 14,30-16,30	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)
Martedì 8/3/2016 Ore 14,30-16,30	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Martedì 15/3/2016 Ore 14,30-16,30	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
Martedì 22/3/2016 Ore 14,30-16,30	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Martedì 5/4/2016 Ore 14,30-16,30	The magic words are “squeamish ossifrage” Il concetto di Zero Knowledge. Partita a “mental poker”.

La coordinatrice del progetto

Anna Maria Prandini