22/3/2015

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti in Aprile/Maggio 2015

Modulo di Matematica - ITIS “E. Fermi”

Prof. Roberto Zanasi – ITIS “E. Fermi”

Venerdì 10/4/2015 Ore 14,00-16,00	**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
Venerdì 17/4/2015 Ore 14,00-16,00	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 24/4/2015 Ore 14,00-16,00	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Venerdì 8/5/2015 Ore 14,00-16,00	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
Venerdì 15/5/2015 Ore 14,00-16,00	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Venerdì 22/5/2015 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