17/2/2012

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti in Febbraio/Aprile 2012

Modulo di Matematica - ITIS “E. Fermi”

Prof. Roberto Zanasi – Lab. 3, I piano, ITIS “E. Fermi”

Martedì 21/2/’12 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 28/2/’12 Ore 14,30-**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)
5-10 marzo	… non c’è lezione…
Martedì 13/3/’12 Ore 14,30-16,30	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Martedì 20/3/’12 Ore 14,30-16,30	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
26-31 marzo	… non c’è lezione…
Martedì 3/4/’12 Ore 14,30-16,30	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Venerdì 13/4/’12 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