7/4/2013

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti in Aprile/Maggio 2013

Modulo di Matematica - ITIS “E. Fermi”

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

Lunedì 15/4/’13 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
Lunedì 22/4/’13 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)
Lunedì 29/4/’13 Ore 14,00-16,00	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Lunedì 6/5/’13 Ore 14,00-16,00	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
Lunedì 13/5/’13 Ore 14,00-16,00	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie.
Lunedì 20/5/’13 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