13/3/2011

Progetto “CoMETA” all’ITIS “Enrico Fermi”

Argomenti che verranno svolti in Marzo/Aprile 2011

Modulo di Matematica - ITIS “E. Fermi”

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

Mercoledì 16/3/’11 Ore 13,45-15,45	**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
Giovedì 24/3/’11 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 (e' una generalizzazione del teorema di Fermat; ci assicura, ad esempio, che le ultime tre cifre di 3^400 sono 001).
Mercoledì 30/3/’11 Ore 13,45-15,45	Il meraviglioso mondo dei numeri primi (esercitazioni al computer); test di primalità
Mercoledì 6/4/’11 Ore 13,45-15,45	L'algoritmo di Euclide, il concetto di crittografia a chiave pubblica, l'algoritmo RSA
Mercoledì 13/4/’11 Ore 13,45-15,45	Perché l'algoritmo RSA funziona? Tecniche per velocizzare i calcoli e per proteggersi dalle spie. The magic words are “squeamish ossifrage”
Mercoledì 20/4/’11 Ore 13,45-15,45	Il concetto di Zero Knowledge. Partita a “mental poker”.

La coordinatrice del progetto

Anna Maria Prandini