LICEO SCIENTIFICO STATALE V.VOLTERRA – CIAMPINO

Relazione **Piano Lauree Scientifiche** : "CRITTOGRAFIA E NUMERI PRIMI"

Responsabile : Prof.ssa Laura Sopranzi.

Anno scolastico 2010/11

Il progetto Lauree Scientifiche ha lo scopo di stimolare le vocazioni scientifiche nei giovani, proponendo la *"didattica laboratoriale*" come nuova metodologia di approccio alle discipline : uso di schede di auto-apprendimento, deduzione guidata delle conclusioni e sistemazione teorica finale dei concetti

I laboratori sono progettati attraverso una collaborazione paritaria tra l'Università e la Scuola Superiore.

Il Liceo Scientifico "V.Volterra" in collaborazione con l'Università di Tor Vergata, nella persona della Prof.ssa Francesca Tovena, ha proposto un laboratorio di crittografia al fine di fornire agli studenti le conoscenze matematiche necessarie per descrivere la crittazione dei messaggi.

Nel corso del laboratorio sono stati analizzati alcuni metodi di cifratura utilizzati nel corso della storia sviluppando l'impianto matematico che ne consente la realizzazione.

La cifratura permette di passare da un insieme di messaggi (detti in chiaro) ad un altro insieme di messaggi (detti cifrati) e può dunque essere interpretata come una funzione tra questi due insiemi. Le funzioni di cifratura adatte devono essere biunivoche tra insiemi finiti. Sono stati utilizzati il cifrario di Cesare, il cifrario affine, il cifrario di Vigenére, One Time Pad e la cifratura a blocchi, ogni volta alla ricerca di una crittazione più efficace. Si è passati dai sistemi di cifratura simmetrici a quello non simmetrico a chiave pubblica universalmente noto e attualmente più diffuso : l'RSA.
L'impianto matematico che consente la realizzazione dei metodi di cifratura consiste nel lavorare nell'insieme dei numeri interi. E' stata definita la relazione di *congruenza modulo n* e le operazioni in Z_n (addizione, moltiplicazione, potenze) introducendo così gli studenti all'aritmetica modulare. Sono stati utilizzati l'algoritmo euclideo per il calcolo del MCD e l'identità di Bezout come strumenti fondamentali per trovare l'inverso in Z_n alla ricerca di una buona funzione di cifratura. Sono stati usati il Teorema di Eulero e il piccolo teorema di Fermat per determinare l'esistenza di un esponente corretto da usare per ottenere una funzione di cifratura. Per la realizzazione del sistema RSA sono state usate le potenze, il teorema di Eulero e la scrittura a blocchi.

L'obiettivo raggiunto è stato avvicinare gli studenti alla teoria dei numeri tramite l'uso della crittografia ed imparare a codificare e decodificare semplici messaggi utilizzando metodi diversi.

Il laboratorio è stato rivolto agli studenti di quarta e si è sviluppato, dopo la conferenza introduttiva tenuta dalla Professoressa Tovena il 18 ottobre 2010 in sei incontri (29/10; 05/11; 12/11; 26/11 03/12 07/12) .

Il laboratorio ha visto la partecipazione assidua e attiva di trentacinque studenti . Tutti hanno frequentato con regolarità ed entusiasmo ed hanno conseguito l'attestato rilasciato dall'Università di Tor Vergata.

Personale docente e Ata coinvolto :
Laura Sopranzi: responsabile del progetto (18 ore Idei +18 ore organizzazione/preparazione/realizzazione del corso(fis))
Anna Mancini: collaboratore (18 ore organizzazione/preparazione/ realizzazione del corso (fis)
Marina Pesce: collaboratore (18 ore organizzazione/preparazione/ realizzazione del corso (fis))
Collaboratore scolastico : tre ore
Collaboratore amministrativo: due ore.