

I contenuti e gli esiti del test saranno rispettivamente proposti e valutati dai responsabili del progetto e se avrai ottenuto una valutazione positiva potrai partecipare ad una visita guidata al palazzo del Bo', incluso l'ingresso al Teatro Anatomico e la visita alla Cattedra di Galileo. Al termine del progetto ti sarà proposto un pomeriggio di accoglienza presso la Scuola Galileiana di Studi Superiori dell'Università degli Studi di Padova

Non è richiesto alcun prerequisito particolare se non alcuni concetti noti dal primo biennio di scuola superiore.

NOTE: ai partecipanti saranno rimborsate le spese di viaggio se effettuate mediante mezzi di pubblico trasporto, previa consegna delle relative attestazioni.

Le domande di partecipazione dovranno essere inviate dai Dirigenti Scolastici delle scuole di provenienza **entro il 30 settembre 2014** per posta elettronica all'indirizzo email cam@math.unipd.it corredate dall'Allegato 1 e, per ogni studente candidato (al massimo 8 per istituto), dai relativi Allegati A e B.

Una commissione selezionerà i partecipanti tra coloro che avranno inviato la loro adesione tramite l'Istituto Scolastico di appartenenza, nei tempi e nei modi previsti. I risultati della selezione saranno comunicati direttamente agli istituti di appartenenza **entro il 7 ottobre 2014.**

Per informazioni scrivere a

cam@math.unipd.it

Referente del progetto

Prof.ssa Patrizia Cuccia

***Docenti del Dipartimento di Matematica della
Università di Padova***

Professori Riccardo Colpi Luisa Fiorot

Con il patrocinio della Scuola
Galileiana di Studi Superiori



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



P.L.S.



Scuola
Galileiana

CRITTOGRAFIA E ARITMETICA MODULARE

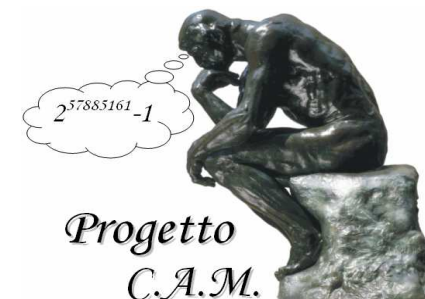
Progetto *C.A.M.*

17 ottobre - 28 novembre 2014

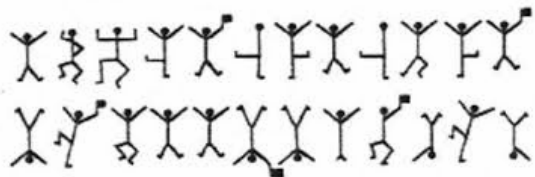
Ore 15.30- 17.30

Dipartimento di Matematica di Padova

Torre Archimede Via Trieste 63



Che cos'è la crittografia? E' la scienza che studia come rendere segreta e sicura la comunicazione, nascondendo il significato del messaggio.



All'inizio la Crittografia era una pratica, un insieme di metodi e di strumenti diversi, addirittura un'arte: l'arte di scambiarsi i messaggi senza farne capire il reale contenuto, anche se erano intercettati.

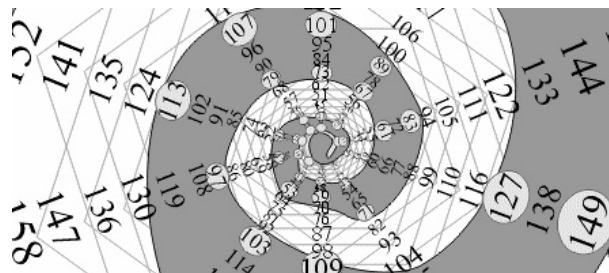
Dal codice di Cesare, all'inchiostro simpatico... e poi irrompe la matematica, in particolare la teoria dei numeri che ha trasformato la crittografia in una scienza "Colui che ama la pratica senza la teoria è come un marinaio che naviga senza timone e senza bussola e non conosce mai dove potrebbe approdare" (Leonardo)

Ruolo fondamentale nella moderna crittografia è la scomposizione di un numero in fattori primi.



Tobia Ravà *Bosco dei numeri primi* (2011)

Quel fascino che per secoli ha catturato l'interesse dei più grandi matematici ha trovato in questi ultimi decenni, con l'evoluzione delle tecnologie informatiche, estese applicazioni nell'ambito della cosiddetta Crittografia a chiave pubblica. Al giorno d'oggi, nell'era della telematica, ciascuno di noi la utilizza per servizi come il bancomat, la posta elettronica o il commercio on-line.



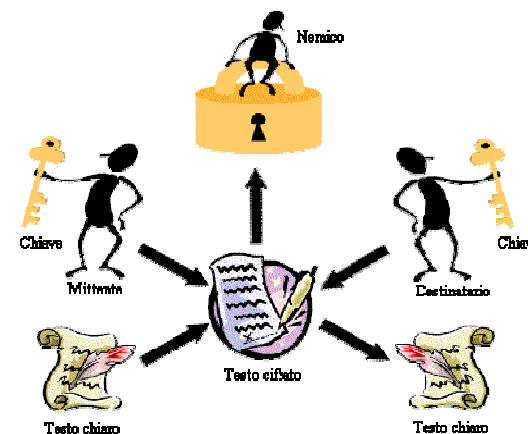
"Ogni nuova soluzione è un nuovo problema"

La storia della crittografia è un alternarsi di nuove idee per crittosistemi e di attacchi agli stessi.



Un ruolo decisivo si è avuto nel corso della seconda guerra mondiale, quando il servizio segreto inglese, con l'aiuto essenziale di Alan Turing (1912-1954), è riuscito a decrittare fin dal 1942 la macchina cifrante Enigma, usata dal comando tedesco.

Per gli studenti



Vuoi

essere un creatore o un risolutore di codici segreti? Se sei interessato a questa eterna lotta fra crittografi e crittoanalisti iscriviti al progetto CAM.

Sarai accompagnato in un percorso che parte dai semplici codici dell'antichità per giungere ai teoremi della matematica modulare che servono per iniziare a comprendere la crittografia moderna. Nel frattempo passerai da un insegnamento di tipo "scuola superiore", guidato da docenti, a un corso di tipo universitario con lezioni di professori del Corso di Laurea in Matematica. Sarai assistito da un tutor studente universitario che ti aiuterà a superare le difficoltà di due approcci così diversi.

Una parte di ciascun incontro sarà dedicato ai laboratori dove tu sarai parte attiva e dove potrai utilizzare e rinforzare le tue capacità creative e organizzative. Alla fine del corso, se lo vorrai, potrai sostenere un test finale con autovalutazione.