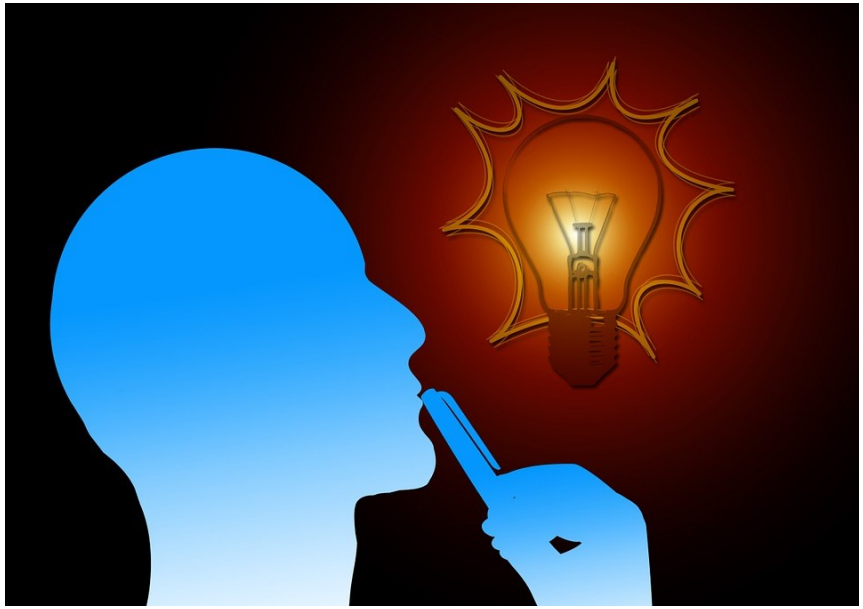
Matematica e Crittografia

Riflessioni ed altro ……



Prof.ssa Maria Antonella Pugliese
Prof. Fabio Bellini
I.I.S CROCE-ALERAMO a.s 2019/2020

Obiettivi generali:

- Mostrare agli allievi che la matematica non è una costruzione neutra, né asociale, ma un prodotto socio-storico-culturale soggetto a interessi e necessità propri di una determinata epoca.

- Sfatare l'idea di successo identificata con risposte corrette date in tempi veloci.

- Allontanare dallo studente una visione dell'apprendimento in cui c'è poco spazio per l'errore e il tempo, centrata più sull'acquisizione di conoscenze e abilità che sulla costruzione di competenze.

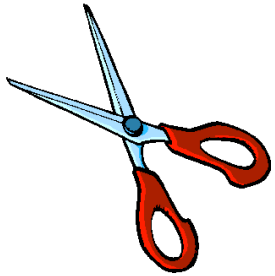
Volevamo che:

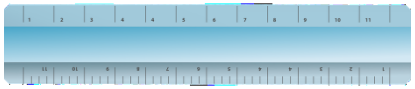
- gli studenti avessero un ruolo attivo: non solo ascoltatori, ma operatori attivi, che lavorando a piccoli gruppi e discutendo fra di loro, costruiscono le proprie conoscenze;

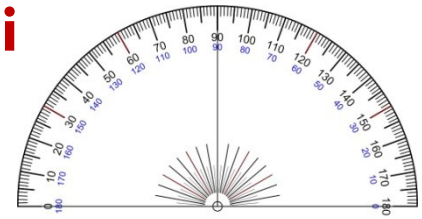
- gli insegnanti avessero il ruolo di guida esperta che osserva e ascolta, che risponde a eventuali domande, che sa indirizzare su una via proficua e distogliere da una via poco significativa, e, soprattutto, che aiuta i ragazzi a tirare le fila dell'attività svolta.

Con quali strumenti abbiamo lavorato?

- Quaderno
- Righello
- Matita, pennarello
- Goniometro
- Cartoncini colorati
- Ferma campioni
- Rotolo di carta scottex
- Nastro bianco
- Spillette
- Forbici







Cosa hanno costruito gli alunni durante i laboratori?

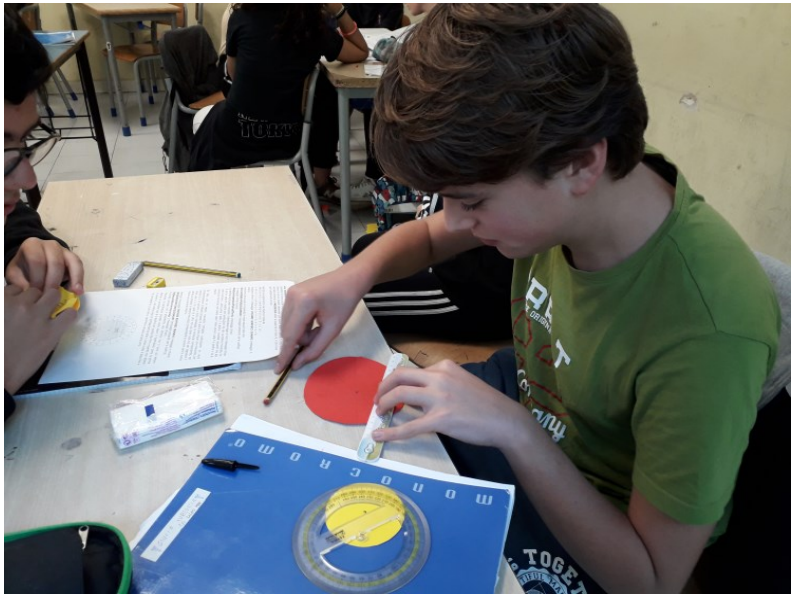
Scitala lacedemonica 400 a.C.

Erodoto (libro VII delle Storie):

> Demarato per avvisare gli Spartani del prossimo attacco del re persiano Serse alla Grecia prese una tavoletta doppia, ne raschiò la cera e poi sul legno della tavoletta scrisse il piano del re. Fatto ciò versò di nuovo cera liquefatta sullo scritto, in modo che, venendo portata vuota, la tavoletta non procurasse nessun fastidio da parte dei custodi delle strade

(prima della battaglia di Salamina, 480 a.C.)

Il disco cifrante di Giovan Battista Alberti 1400



Che cos'è la crittografia:

Obiettivi emersi dalla discussione con gli alunni

- Segretezza: Il messaggio non deve essere leggibile da terzi.
- Autenticazione: Il destinatario deve poter essere sicuro del mittente.
- Integrità: Il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.
- Attendibilità: Il mittente non deve poter negare di aver inviato il messaggio.

Utilizzo tradizionale della crittografia

- Gli usi tradizionali riguardavano quasi esclusivamente gli ambiti militari e di spionaggio/controspionaggio.

- Sono riportati numerosissimi esempi di uso di sistemi crittografici nel corso di guerre, battaglie, rivoluzioni, cospirazioni, complotti.

Utilizzi moderni della crittografia

- L'uso più importante della crittografia in ambito "civile" è quella della sicurezza delle comunicazioni in rete (ad esempio whatsapp)

- Più in particolare le applicazioni di commercio elettronico sono quelle in cui maggiormente è sentita la necessità della sicurezza e della segretezza (scambio di dati sensibili, quali il numero di carta di credito, numero di conti bancari, ecc.)

Svetonio aveva accesso agli archivi della corte imperiale, e poteva quindi consultare gli scritti che vi erano conservati degli imperatori.
In questi due brevi passi riporta l'abitudine di Giulio Cesare e di Ottaviano Augusto di ricorrere ad un semplice mezzo di cifratura di testi, consistente nella sostituzione di ogni lettera del testo con un'altra posta a intervallo fisso nell'elenco alfabetico (la trasposizione è in base 3 per Cesare, in base 1 per Augusto).

extant et ad Ciceronem [scil. *Caesaris epistulae*], *item ad familiares domesticis de rebus, in quibus, si qua occultius*[1] *perferenda erant*[2], *per notas scripsit*[3], *id est sic structo*[4] *litterarum ordine, ut nullum uerbum effici posset: quae si qui inuestigare et persequi*[5] *uelit, quartam elementorum litteram, id est D pro A et perinde*[6] *reliquas commutet*[7].
(*Jul. Caes.* 56, 6-7)

Vi sono anche [lettere di Cesare] a Cicerone, e pure ai familiari su questioni private, in cui, se doveva comunicare alcune informazioni in modo riservato, le trascriveva in linguaggio cifrato, cioè secondo una successione alfabetica disposta in modo tale che non se ne potesse ricavare alcuna parola di senso compiuto: se si desidera comprenderne la chiave e riprodurlo, bisogna sostituire la quarta lettera dell'alfabeto alla prima, cioè la D al posto della A e così tutte le altre.

Quotiens autem [*scil. Augustus*] *per notas scribit*[8], *B pro A, C pro B ac deinceps eadem ratione*[9] *sequentis litteras ponit; pro X autem duplex A.*
(Aug. 88, 3)

Ogni volta poi che [Augusto] scrive in linguaggio cifrato, sostituisce la B alla A, la C alla B e così via le lettere seguenti secondo il medesimo criterio; al posto della X però la doppia A.

Il laboratorio è stato per gli alunni occasione per ….

- Confrontarsi su ipotesi, percorsi e strategie all'interno del piccolo gruppo.
- Saper ascoltare e convincere attraverso l'argomentazione
- Elaborare, comunicare spiegazioni e argomentazioni nel contesto del problema nel confronto con gli altri gruppi
- Costruire relazioni positive tra pari e con i docenti, migliorando l'autostima e la conoscenza di sé.

E tutto questo giocando!

- **Criptare e decriptare messaggi attraverso i cifrari**
- **Parole crociate crittografate**
- In questo tipo di cruciverba non sono presenti le definizioni; ogni casella, non nera, riporta invece un numero. Bisogna riempire la griglia tenendo presente che a numero uguale corrisponde lettera uguale.

  La crittografia si occupa di tutti i metodi in grado di rendere un messaggio incomprensibile alle persone a cui non è destinato.
  E' una tecnica utilizzata da secoli per la codifica di messaggi e sviluppatasi soprattutto durante il periodo della guerra.
  Esistono molti modi per decriptare un messaggio.
  La tecnica chiamata "analisi delle frequenze" permette, con l'uso di un semplicissimo algoritmo, di decriptare un testo dove a ogni lettera è stato arbitrariamente assegnato lo stesso numero.
  Nella lingua italiana, le lettere utilizzate con maggior frequenza sono, nell'ordine
  E, A, I, O, N, R, L, T, S, C, D, U, P, M, V, G, B, H, F, Q, Z, X, J, K, Y, W
  La crittografia applicata all'enigmistica ha permesso la creazione di uno schema di parole crociate senza definizioni, dove, solo con l'ausilio degli incroci e rispettando la regola che a numero uguale corrisponde lettera uguale, si arriva alla soluzione.

Come....

Per svolgere le attività laboratoriali sono stati divisi sempre in 4 gruppi spontanei. In questo modo hanno collaborato più facilmente.

Prima attività:

- Costruzione della scitala spartana.
- Utilizzo della scitala per capire quale fosse la chiave
- Introduzione storica al Cifrario di Cesare (messaggio di Svetonio)

Seconda attività:

- Esercizi per criptare e decriptare semplici messaggi con il cifrario di Cesare....deduzione della chiave
- Introduzione all'aritmetica modulare attraverso il cifrario
- Aritmetica dell'orologio

Terza attività:

- Costruzione del disco cifrante di Giovan Battista Alberti
- Spiegazione del funzionamento
- Esercizi per criptare e decriptare semplici messaggi con il disco di Alberti

Quarta attività:

- Cifrario di Vigenere
- Spiegazione del funzionamento
- Esercizi per criptare e decriptare semplici messaggi con il cifrario di Vigenere
- Uno strumento usato per la crittanalisi: analisi delle frequenze…parole crociate crittografate
- Cenni su Enigma attraverso un video

Criticità e miglioramenti.

Le quattro lezioni -laboratorio di 90' sono risultate insufficienti a formalizzare la matematica presente e programmata.

Ci proponiamo di presentare in un altro anno scolastico lo stesso laboratorio affrontando lo studio della teoria dei numeri primi e approfondendo l'aritmetica modulare.