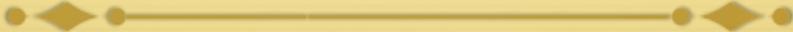


Indicazioni Nazionali

«Si evidenzia l'importanza di connettere **le varie teorie matematiche studiate con le problematiche storiche** che le hanno originate e di approfondirne il significato. Lo studente saprà inquadrare **le varie teorie matematiche studiate nel contesto storico** entro cui si sono sviluppate e ne comprenderà il significato concettuale attraverso una visione storico critica anche in relazione al contesto filosofico, scientifico e tecnologico. lo studente dovrà acquisire il senso e la portata dei principali momenti che caratterizzano la formazione del pensiero matematico: **la matematica nel pensiero greco, la matematica infinitesimale che nasce con la rivoluzione scientifica del Seicento e che porta alla matematizzazione del mondo fisico**, la svolta che prende le mosse dal razionalismo illuministico e che conduce alla formazione della matematica moderna e a un nuovo processo di matematizzazione che investe nuovi campi (tecnologia, scienze sociali, economiche e biologiche) e che ha cambiato il volto della conoscenza scientifica».

La storia della matematica nell'insegnamento ha una lunga tradizione, citiamo a esemplificazione **Joseph Louis Lagrange** (1736-1813) che nelle "Le Lezioni elementari sulle matematiche" all'École Normale, ha inserito la storia della matematica: "[...] lezioni dove si presenteranno gli sviluppi che non potevano entrare nel corso principale e dove si esporrà il percorso analitico degli inventori e gli artifici che hanno impiegato per vincere le difficoltà che potevano fermarli" o **Felix Klein** (1849-1925), che nel suo programma di riforma dell'insegnamento della matematica, che confluì nel Meraner Lehrplan (1905), inseriva tra gli assunti metodologici quello di considerare nell'insegnamento il percorso storico della matematica adottando il "metodo genetico", ovvero presentare una teoria seguendo il modo in cui si è sviluppata nella storia e non nella sua formulazione finale (Giacardi, 2013). Tra gli italiani, non si può non citare **Federigo Enriques** (1871-1946). Egli fondò nel 1923 l'Istituto Nazionale per la Storia delle scienze e la Scuola Universitaria per la Storia delle scienze, quest'ultima era anche rivolta alla formazione degli insegnanti e fu curatore della collana *Per la storia e la filosofia delle matematiche* (1925). Enriques riteneva che l'insegnante dovrebbe presentare ai propri alunni "[...] le origini, le connessioni, il divenire, non un qualsiasi assetto statico [...]" di una teoria (Enriques, 1921).

La storia della Matematica nell'insegnamento



In questa direzione si è sviluppata un'intera branca di ricerca e si sono attuate varie sperimentazioni sia nazionali che internazionali. Citiamo a esemplificazione:

- ✦ **Katz, V.** (ed.) (2000). *Using history to teach mathematics: An international perspective*. The Mathematical Association of America.
- ✦ **Katz, V.** (ed.) (2004). *Historical Modules for the Teaching and Learning of Mathematics*. The Mathematical Association of America.
- ✦ **Furinghetti, F., Radford, L.** (2002). Historical conceptual developments and the teaching of mathematics: rethinking phylogenesis and ontogenesis. In L. English et al. (ed.) (2002) *Handbook of international research in mathematics education*, L. Erlbaum: Mahwah, NJ, 631-654.

Perché la Storia della Matematica nell'insegnamento

- ✦ “umanizzare la matematica” tramite il racconto del vissuto dei suoi protagonisti effettuare interessanti collegamenti con altre discipline, anche dell’ambito umanistico
- ✦ Rendere la matematica una “disciplina viva”, con un passato, un presente e un futuro
- ✦ effettuare approfondimenti matematici, anche personalizzati sulla base dell’interesse dell’allievo
- ✦ fornire una visione poliedrica della tematica trattata, consentendo in tal modo all’allievo di scegliere il punto di vista a lui più congeniale. A tale scopo di fondamentale importanza è il carattere di flessibilità dell’attività del laboratorio, che deve plasmarsi ed adattarsi alle esigenze cognitive ed agli interessi dell’allievo che ne è co-protagonista.

Crittografia

Liceo Classico V.E. II, Palermo

1° Lezione

**Di Liberto Anna Rosa
Salerno Maria Concetta
Sciortino Maria Assunta**

Storia della Crittografia

(Svetonio-Vita di Cesare § 56)

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Restano quelle [le lettere] a Cicerone, così come quelle ai familiari sugli affari domestici, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D per A e così via per le rimanenti.

Storia della Crittografia

(Svetonio-Vita di Ottaviano Augusto § 88)

Orthographiam, id est formulam rationemque scribendi a grammaticis institutam, non adeo custodit ac videtur eorum potius sequi opinionem, qui perinde scribendum ac loquamur existiment. Nam quod saepe non litteras modo sed syllabas aut permutat aut praeterit, communis hominum error est.

Nec ego id notarem, nisi mihi mirum videtur tradidisse aliquos, legato eum consulari successorem dedisse ut rudi et indocto, cuius manu "ixi" pro ipsi scriptum animadverterit.

Quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A.

Storia della Crittografia

(Svetonio-Vita di Ottaviano Augusto § 88)

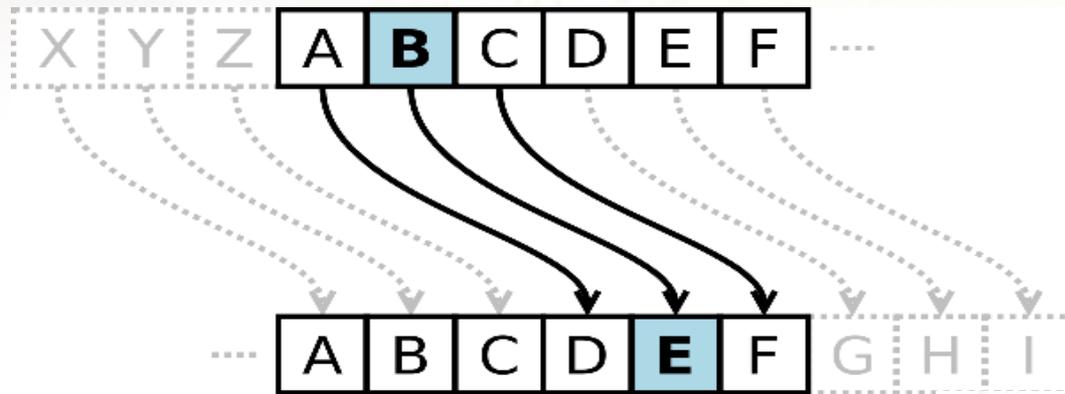
Non rispettava l'ortografia, cioè l'arte di scrivere le parole correttamente seguendo le regole dei grammatici, e sembrava piuttosto seguire l'opinione di coloro che pensano che si debba scrivere come parliamo. E infatti cambiava o saltava non solo lettere, ma anche sillabe intere, che sono errori comuni degli uomini.

Ed io non ne parlerei nemmeno, se non mi sembrasse incredibile quello che alcuni raccontano e cioè che avrebbe sostituito un legato consolare considerandolo rozzo e ignorante, perchè aveva scritto "ixi" al posto di "ipsi".

Tutte le volte poi che scriveva in codice, sostituiva la A con la B, la B con la C e con lo stesso criterio le altre lettere; e la X veniva sostituita da una doppia A.

Cifrario di Cesare

Consiste nel traslare l'alfabeto di tre posizioni.



Chiario ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrato DEF GHIJKLMNOPQRSTUVWXYZABC



Cifratura e decifratura

- Cifrare la frase: **AUGURI DI BUON NATALE**

Chiario **AUGURIDIBUONNATALE**
Cifrato **DXJXULGLEXRQQDWDHOH**

- Decifrare la frase: **DXJXULGLEXRQQDWDHOH**

Cifrato **DXJXULGLEXRQQDWDHOH**
Chiario **AUGURIDIBUONNATALE**

Applicazione laboratoriale

Cifrare le seguenti frasi latine:

- **Carpe diem**
- **Ubi maior minor cessat**
- **Labor omnia vincit**

Decifrare le seguenti frasi:

- **GXOFLVLQIXQGR**
- **YLYHUHHVWFRJLWDUH**
- **VFLHQWLDSRWHQWLDHVW**

Crittografia

Liceo Classico V.E. II, Palermo

2° Lezione

**Di Liberto Anna Rosa
Salerno Maria Concetta
Sciortino Maria Assunta**

Crittografia

- Cosa si intende per Crittografia?

Il termine *Crittografia* viene dalla composizione di due parole greche:

- κρυπτός [kryptós], "*nascosto*",
- γραφία [graphía], "*scrittura*".

Letteralmente significa *scrittura in codice*



024FG002	53D03C00
887525C1	4F553F
4242434E	3D4A6
553D4553	414
00312E30	5424
4CC	024E4E4F
21	8833B0CC
CB3EE8EF	DF038D7F
04143B75	4F571C83
B57C659E	C820FE07

Si tratta dell'arte di scrivere messaggi segreti che possono essere letti e compresi soltanto dal destinatario.

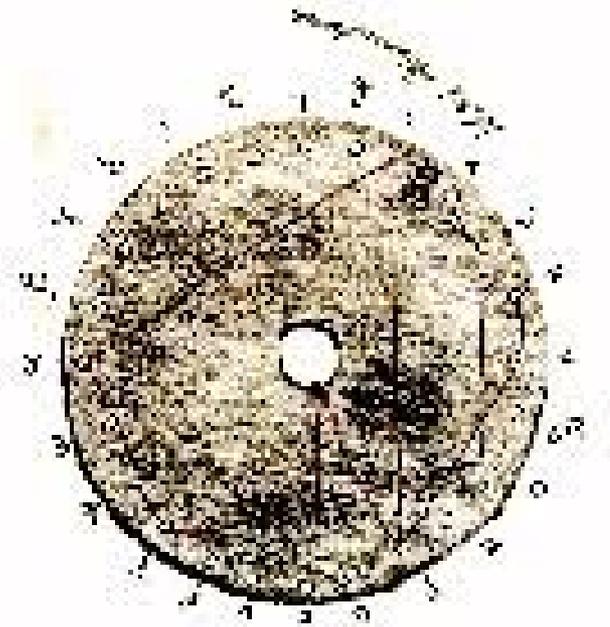
La Crittografia nell'antica Grecia

Le più antiche tecniche di cifratura:

- Scitala



- Disco di Enea il Tattico



Storia della Crittografia

Cifrario Monoalfabetico

Un cifrario a sostituzione monoalfabetica è un sistema crittografico che sostituisce ogni lettera di un alfabeto con un'altra dello stesso alfabeto.

Esempi:

- Codice di Cesare
- Atbash

Atbash

A = Z	N = M
B = Y	O = L
C = X	P = K
D = W	Q = J
E = V	R = I
F = U	S = H
G = T	T = G
H = S	U = F
I = R	V = E
J = Q	W = D
K = P	X = C
L = O	Y = B
M = N	Z = A

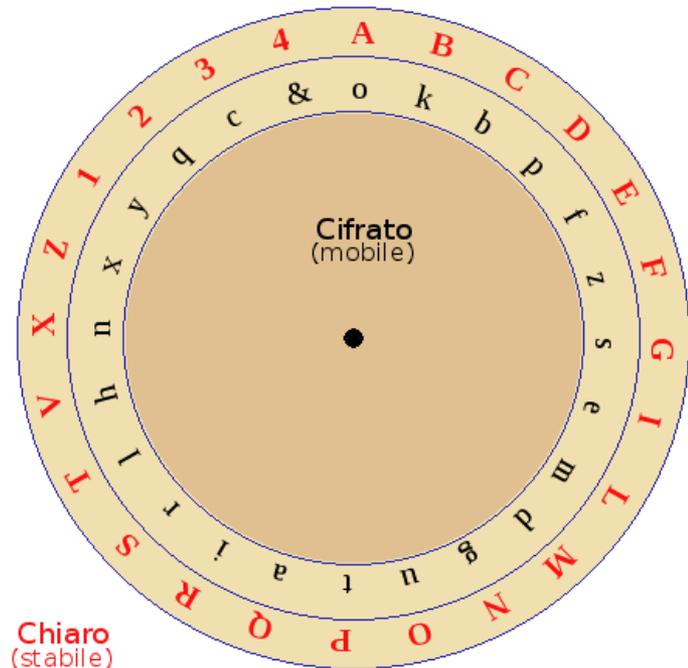
Storia della Crittografia

Cifrario Polialfabetico

In crittografia, un cifrario a sostituzione polialfabetica non utilizza lo stesso alfabeto per cifrare un messaggio ma, fa uso di più alfabeti, usando opportune regole.

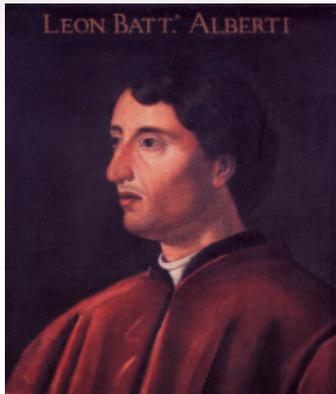
Esempio

- Disco Cifrante di Alberti

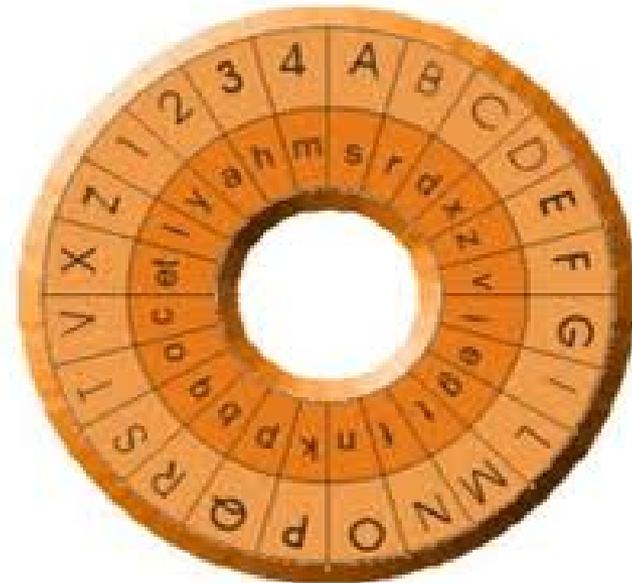


Storia della Crittografia

Disco Cifrante di Alberti



Leon Battista Alberti propose un disco composto da due cerchi cifranti concentrici: uno esterno fisso, formato da 24 caselle che contenevano 20 lettere latine maiuscole ed i numeri 1 2 3 4 per il testo chiaro; un disco interno mobile con le 24 lettere minuscole per il testo cifrato.



E adesso...COSTRUIAMOLO NOI !!!

I collegamenti interdisciplinari



- ✦ Latino
- ✦ Storia (antichità, II guerra mondiale, oggi – whatsapp)
- ✦ La Statistica (crittoanalisi statistica)
- ✦ algebra modulare e combinatoria
- ✦ percorso verticale (dalla II alla V)

Conclusioni



L'esperienza nei liceo matematico e maturata nel tempo nei laboratori PLS ha mostrato che gli studenti sono molto motivati nello studio degli argomenti, sia strettamente di crittografia (codici) sia di matematica, quali le frequenze statistiche e l'algebra modulare, necessari alla comprensione e all'uso di alcuni codici. Il percorso storico che fa vivere personaggi e avvenimenti e l'interdisciplinarietà stimolano gli studenti. Inoltre, il tema si adatta bene alle indicazioni nazionali sulla verticalità, potendo essere svolto a più livelli scolastici con diversi approfondimenti.