

*Giornate di studio dell'Insegnante di MATematica*

**ATTI del convegno**

***Giocare con la matematica:  
dall'apprendimento informale all'apprendimento formale***

19-20 OTTOBRE 2018  
DIPARTIMENTO DI MATEMATICA E INFORMATICA  
UNIVERSITÀ DI CATANIA

**Quaderni di Ricerca in Didattica**  
**Quaderno 1 – Numero speciale N. 2, Dicembre 2018**

A cura di

Benedetto Di Paola  
Eugenia Taranto



*“Quaderni di Ricerca in Didattica (Mathematics)”*, n.1 Numero speciale n.2, 2018  
G.R.I.M. (Dipartimento di Matematica e Informatica, Università degli Studi di Palermo)

G.R.I.M. - Gruppo di Ricerca sull'Insegnamento/Apprendimento delle Matematiche

Università degli Studi di Palermo

**ISSN 1: 1592-4424**

**ISSN 2: 1592-5137**



## L'evento è stato promosso dai seguenti enti:

**G.R.I.M.**  
**Gruppo di Ricerca**  
**sull'insegnamento/Apprendimento delle**  
**matematiche**



**Dipartimento di Matematica e Informatica,**  
**Università degli Studi di Palermo**



**Dipartimento di Matematica e Informatica,**  
**Università di Catania**



**Piano Lauree Scientifiche - PLS**



## Con la sponsorizzazione di:

**ASSOCIAZIONE SPORTIVA BRIDGE-**  
**CATANIA**



**CASIO**



**DeAgostini Scuola**



**Kangourou**



**La tecnica della Scuola**



**Reinventore S.R.L.S.**



**Sapyent**



**Zanichelli Editore SPA**



## Indice

Premessa	p. 9
<b>Plenarie</b>	
Giocare con la matematica: argomentare, modellizzare e costruire significati (Antonini S.)	p. 13
Movimenti Amo la Matematica: tra teoria e pratica (Ferrara F. & Savioli K.)	p. 19
Insegnare Matematica tra gioco, divertimento e curiosità (Ragusa A.)	p. 27
<b>Comunicazioni e laboratori - Scuola Primaria e dell'Infanzia</b>	
MagicoAbaco: l'arte del calcolo veloce, preciso e consapevole (Malagoli G.M. & Passerini E.) – Laboratorio	p. 33
Grafica... mente: i grafici a volte sono bugiardi! (Bartolomei G.S.) – Laboratorio	p. 35
Piccoli Makers nella scuola dell'Infanzia (Provito A.) – Laboratorio	p. 37
Giochi matematici per lo sviluppo di competenze (Spagnolo C. & Bolondi G.)	p. 39
Comprensione, rappresentazione, categorizzazione e pianificazione nel problem solving matematico. Un'esperienza didattica alla Scuola Primaria (Di Maira F.)	p. 41
La Ricerca-Azione per l'innalzamento delle competenze di base: esperienze laboratoriali con gli alunni della scuola primaria (Arcidiacono E.)	p. 43
Giochiamo con acqua e zucchero (De Simone D.) – Laboratorio	p. 45
In arte... matematica! (Crivelli L. et al.) – Laboratorio	p. 47
Che cosa mangi a merenda? (Macaluso S. et al.) – Laboratorio	p. 49
Giochiamo con il mostro a quattro mani (Barbanera P. & Foradini P.)	p. 51
Conosco il mio tempo: giochiamo con la statistica (Bongiovanni I. & Enea R.)	p. 53
Ludomatica (Gugino M.A.)	p. 55
<b>Comunicazioni e laboratori - Scuola Secondaria di I grado</b>	
13 carte per aiutare la fortuna. Scommettere col bridge sulla probabilità di vincere (Borzi G. et al.) – Laboratorio	p. 59
Muoversi è pensare: grafici, studenti e funzioni in movimento (Ferrari G.) – Laboratorio	p. 61
L'affascinante mondo dei frattali (Ciarcià C.)	p. 63
Lava e Sbianca o Bianco Pulito? Per un uso didattico dei quesiti INVALSI (Brunelli F.) – Laboratorio	p. 65
Laboratorio-Gara di Giochi Matematici (Danese B.) – Laboratorio	p. 67
A Regola d'Arte Percorsi intrecciati di Matematica e Arte (Bisignani C. et al.) – Laboratorio	p. 69
Gli hashtag della Matematica (Paratore A.)	p. 71
“I PRIMI DELLA CLASSE”: attività di laboratorio sulla divisibilità (Barraco C. et al.)	p. 73
Il ruolo dell'attività laboratoriale nello sviluppo e nell'acquisizione di competenze nella scuola secondaria di I grado (Esposito A. et al.)	p. 77
<b>Comunicazioni e laboratori verticali - Scuola Secondaria di I e II grado</b>	
Una piattaforma digitale per il raggiungimento dei traguardi di sviluppo delle competenze in matematica (Spagnolo C.) – Laboratorio	p. 83
Dalle strategie ai teoremi (Aquino D. et al.) – Laboratorio	p. 85
Forme e Colori della Matematica nella Palermo Felicissima (Di Prima M.C. & Ducato R.) – Laboratorio	p. 87
Problemi “reali” di matematica (Collura D.M. et al.)	p. 91

“Geometra amanuense o Geometra digitale?” (Ruggeri A.R.)	p. 93
SIRENE, framework per l'insegnamento della matematica (Averna G.)	p. 95
Lezioni Americane (Danese B.)	p. 97
L'E.A.S. come metodologia didattica per l'insegnamento della matematica nella Scuola Secondaria di Primo Grado (Votino G.)	p. 99
Gare a squadre: gioco, divertimento o passione? (Messina S. & Pennisi M.)	p. 101
<b><i>Comunicazioni e laboratori - Scuola Secondaria di II grado</i></b>	
Robot e matematica (Castagnola E.)	p. 105
La danza serpentina dei pendoli (Bramanti G.)	p. 107
La rappresentazione prospettica dell'ipercubo (Occhipinti A.)	p. 111
L'uso di Kahoot per migliorare gli esiti in matematica (Chiovetta C. & Drago C.)	p. 113
Scommettiamo... sulla matematica (Cerruto N.)	p. 117
Dai paradossi di Zenone ai punti di accumulazione (Chiaramonte G.)	p. 121
Le sorprese del triangolo di Tartaglia (Inturri A. & Margarone D.)	p. 125
Dai quadrilateri ortici alla fisica del tavolo da biliardo (Adesso M.G. et al.)	p. 127
Codici e segreti: percorso di crittografia tra storia e interdisciplinarietà (Cerroni C.)	p. 129
Matematica & Cartoon: un binomio vincente in contesti atipici (La Fortuna A.)	p. 131



# Codici e segreti: percorso di crittografia tra storia e interdisciplinarietà

Cinzia Cerroni

Dipartimento di Matematica e Informatica, Università di Palermo

E- [cinzia.cerroni@unipa.it](mailto:cinzia.cerroni@unipa.it)

**Abstract/Riassunto.** Nel seguito viene illustrato un percorso di Crittografia, che partendo dai primi codici della storia (codice di Cesare, Vigenere, etc.), passando attraverso la crittoanalisi statistica e la macchina Enigma e Alan Turing (seconda guerra mondiale), arriva alla Crittografia a Chiave Pubblica, ovvero l'algoritmo dell'RSA.

## 1. Introduzione

La storia della matematica nell'insegnamento ha una lunga tradizione, citiamo ad esempio Joseph Louis Lagrange (1736-1813) che nelle “*Le Lezioni elementari sulle matematiche*” all'École Normale, ha inserito la storia della matematica 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).

### 1.1 Il Percorso laboratoriale di Crittografia

La crittografia si presta a un percorso che segue l'evoluzione storica degli argomenti. Inoltre, la sua valenza interdisciplinare, stimola la motivazione allo studio di argomenti di matematica (quali la matematica dell'orologio, la statistica, la combinatoria etc.) e a temi storici collegati (seconda guerra mondiale etc.).

Il percorso è stato più volte sperimentato nei laboratori PLS dell'Università di Palermo e ha una durata che va dalle 15 alle 20 ore. Le metodologie usate sono quella laboratoriale, del cooperative learning e del problem solving. Si presentano agli studenti gli argomenti e si distribuiscono loro delle schede di lavoro con le quali confrontarsi.

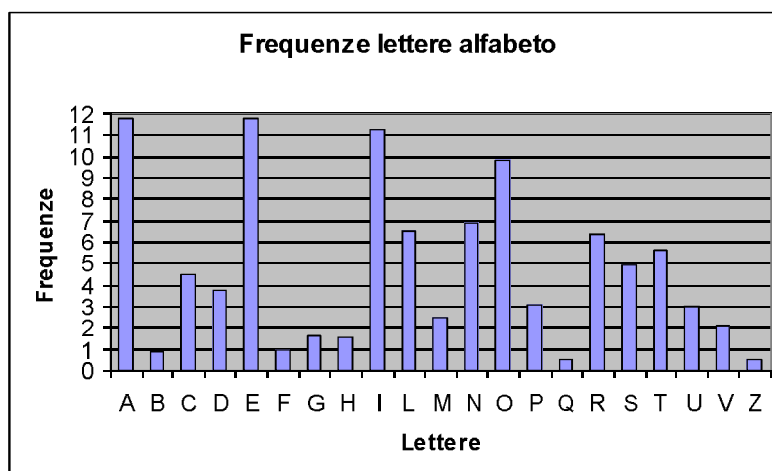
Il primo incontro si articola con un excursus storico degli argomenti dai primi codici del passato fino alla crittografia a chiave pubblica, ognuno di essi viene poi sviluppato nei successivi incontri. Uno dei primi codici che si affronta è il *Codice di Cesare*, così chiamato perché riportato nell'opera di Svetonio, del II secolo d.C., dal titolo “*Vita dei Cesari*”, da cui si evince che ciascuna lettera del messaggio viene sostituita con quella tre posti più avanti nell'alfabeto. Dopo una breve presentazione del codice, si distribuiscono agli studenti delle schede di lavoro sia di cifratura che di decifratura, con le quali confrontarsi.

	Testo in Chiaro	Testo Cifrato con Codice di Cesare
	Oggi è una bella giornata	RLLN H AQD EHOOD LNRUQDZD
<b>Consegna</b>	Cifrare la frase con il codice di Cesare con $k = 3$	

**Scheda 1.** Esempio di scheda di lavoro con soluzione.

Un possibile approfondimento interdisciplinare può andare sia nella direzione di leggere e tradurre l’opera di Svetonio, sia in quella di approfondire la storia romana.

Il laboratorio prosegue con lo studio e l’applicazione dei codici a sostituzione polialfabetica, quali il disco cifrante di Leon Battista Alberti (1404-1472), che si può usare sia come cifrario a sostituzione monoalfabetica che polialfabetica e il cifrario di Vigenère, scoperto da Blaise de Vigenère (1523-1596) nel 1586 e rimasto inviolato per secoli. Ci si dedica successivamente all’analisi delle frequenze delle lettere nelle lingue (ad esempio Italiano e Inglese) e alla loro applicazione alla crittoanalisi statistica. Un testo cifrato con cifrari a sostituzione monoalfabetica (codice di Cesare) può essere decifrato calcolando la frequenza delle lettere cifrate e confrontandola con quella delle lettere dell’alfabeto.



**Figura 1.** Tabella delle frequenze dell’alfabeto italiano.

Il percorso si conclude con la storia di Enigma, di Alan Touring (1912-1954) e con lo studio dell’algebra modulare e della crittografia a chiave pubblica, in particolare l’RSA. Per approfondimenti si veda Singh (1999).

### Bibliografia

- Enriques, F. (1921). *Insegnamento Dinamico*. Bologna, Università.  
 Giacardi, L. (2013). *La Storia della Matematica nell’insegnamento*. Roma. <http://crf.uniroma2.it/wp-content/uploads/2013/07/GIACARDI-StoriaInsegnamento.pdf>  
 Singh, S. (1999), *Codici e Segreti*, Rizzoli.