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

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 ecnica della Scuola

Reinventore S.R.L.S.

Sapyent

Zanichelli Editore SPA

Indice

"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)

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

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 Touring (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
Consegna	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.

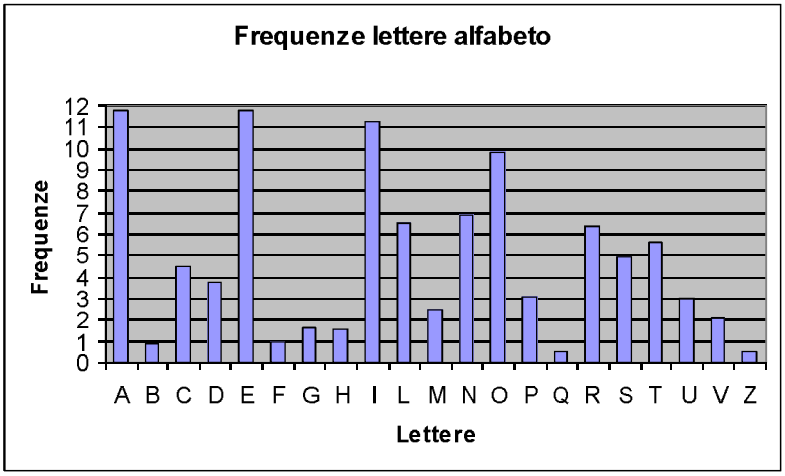

Figura 1. *Tabella delle frequenze dell'alfabeto italiano.*

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.