Laboratorio di crittografia– l'arte di svelare i segreti

Liceo Matematico

LICEO TITO LUCREZIO CARO RM 1954 CLASSICO-LINGUISTICO

Abstract

Gli obiettivi della crittografia sono fondamentalmente due e sostanzialmente in concorrenza tra loro: da una parte si cerca di sviluppare tecniche sempre più sofisticate per proteggere le informazioni e impedire accessi indesiderati ai dati, dall'altra si cerca di evolvere meccanismi per forzare tali protezioni e raggiungere quelle informazioni che con tanta cura si sono nascoste. I due aspetti, nei secoli, sono andati di pari passo e a ogni progresso in un campo quasi sempre ha fatto seguito la nascita di una tecnica o di una tecnologia per contrastare quel progresso.

Questo percorso laboratoriale si sofferma su alcuni dei metodi e degli algoritmi più famosi ideati dall'uomo attraverso i secoli per nascondere e proteggere messaggi, conversazioni, corrispondenza. Contemporaneamente cerca anche di dare un *assaggio* delle tecniche di criptoanalisi in uso fino all'avvento della crittografia meccanica e automatica, lasciando ampio spazio alla creatività degli studenti.

Il desiderio di svelare segreti è profondamente radicato nella natura umana; la promessa di partecipare a conoscenze negate ad altri eccita anche la mente meno curiosa. Qualcuno ha la fortuna di trovare un lavoro che consiste nella soluzione di misteri, ma la maggior parte di noi è spinta a soddisfare questo desiderio risolvendo enigmi artificiali ideati per il nostro divertimento.
I romanzi polizieschi o i cruciverba sono rivolti alla maggioranza; la soluzione di codici segreti può essere l'occupazione di pochi. *John Chadwick (1920-1998)*

Obiettivi del percorso

- conoscenza di alcuni metodi di crittografia (trasposizione e sostituzione)
- applicazione di elementari tecniche di criptoanalisi
- capacità di valutare, per via empirica, la sicurezza di un metodo di cifratura
- conoscenza delle «macchine cifranti»
- cenni su alcuni temi di Crittografia moderna

Collegamenti con la matematica

- trasformazioni geometriche
- elementi di calcolo combinatorio
- aritmetica modulare
- elementi di statistica descrittiva

Durata dell'attività

20 ore

Che cos'è la crittografia?

E' la scienza che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggi.
Crittografia significa letteralmente «scrittura segreta».
Con questo termine si intende oggi un insieme di tecniche che consentono di trasmettere messaggi mantenendoli segreti a tutti, tranne ad alcune persone che possiedano la chiave per comprenderli.

Proprietà della crittografia:

Segretezza
il messaggio non deve essere leggibile a 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.

Un po' di definizioni....

La **cifratura** è l'operazione con la quale si nascondono le informazioni; essa viene effettuata tramite un procedimento chiamato cifrario.
Il **testo in chiaro** è il messaggio da cifrare.
Il **testo cifrato** è il messaggio trasformato in modo da non essere più leggibile tramite una semplice lettura.
La **decifrazione** è la riconversione di un testo cifrato nella sua forma originaria, cioè nel testo in chiaro.
Il **cifrario** è il procedimento (algoritmo) che consente di crittare e decrittare i testi.

Che cos'è la crittoanalisi?

La **crittoanalisi** è l'arte della "rottura" dei codici e dei cifrari.
La crittoanalisi studia come decifrare un messaggio senza esserne "autorizzati".
La **decrittazione** è la riconversione di un testo cifrato nella sua forma originaria, cioè nel testo in chiaro , senza essere in possesso della chiave.
La crittoanalisi ha il ruolo fondamentale di far capire quanto un sistema di cifratura/decifratura sia sicuro.

Utilizzo tradizionale della crittografia

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

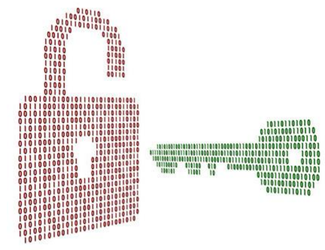
Questa foto di Autore sconosciuto è concesso in licenza da CC BY-SA

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.

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.)



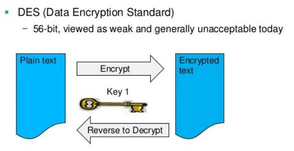
Un altro utilizzo importante è quello della firma digitale e dell'autenticazione dei documenti, che ha applicazioni nella pubblica amministrazione (e-government) e in generale negli aspetti burocratici (contratti, domande, moduli, vari documenti ufficiali, ecc.)

La crittografia nella storia
(dall'antichità al 1975)

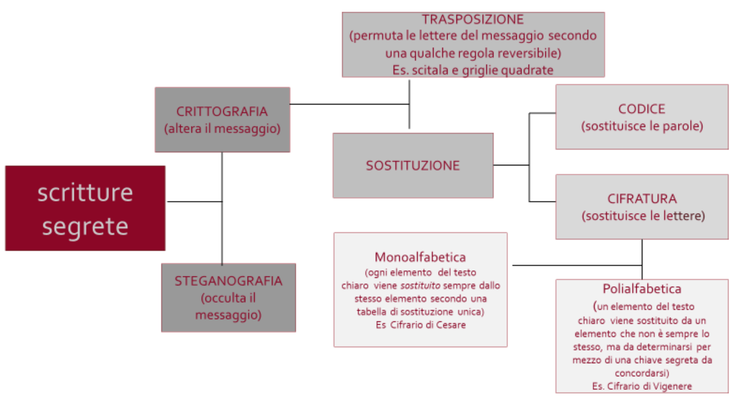
Metodi antichi
- La scitala spartana
- La scacchiera di Polibio
- Il codice atbash
- Il codice di Cesare

Rinascimento
- Blaise Vigenère

XX secolo
- La macchina Enigma (usata dai tedeschi durante la seconda guerra mondiale)
- Il DES (Data Encryption Standard)

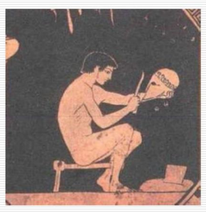


Le attività laboratoriali



Esempi di steganografia

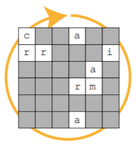
La scritta veniva applicata sul capo rasato di uno schiavo, quindi si attendeva che i capelli ricrescessero e si inviava il messaggero. All'arrivo presso il destinatario, questi rasava nuovamente lo schiavo e leggeva il messaggio.



ITALIA:
nel XVI secolo un modo interessante di recapitare i messaggi era di scriverli con aceto sul guscio di un uovo sodo; il guscio, poroso, permetteva all'aceto di passare e, una volta recapitato il messaggio, era sufficiente sgusciare l'uovo per leggerlo!

Metodi di trasposizione

La scitala spartana
(400 anni a.c.)

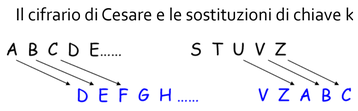


Le griglie quadrate di rotazione

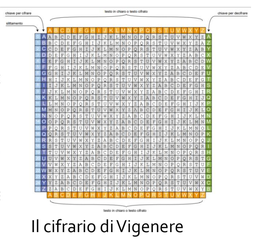
Metodi di sostituzione

La scacchiera di Polibio
(150 anni a.c.)

Il cifrario di Cesare e le sostituzioni di chiave k



È il più antico cifrario di concezione moderna (Svetonio, Le vite di dodici Cesari)

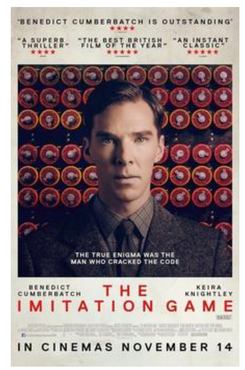


Il cifrario di Vigenere

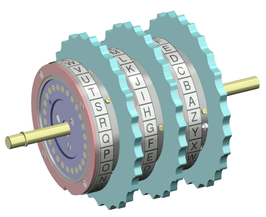
Le macchine cifranti

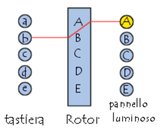
Il disco cifrante di Leon Battista Alberti

La macchina Enigma

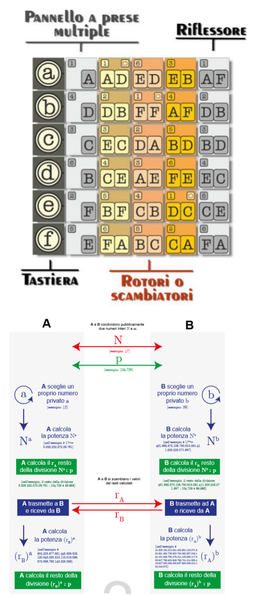


Il funzionamento di Enigma

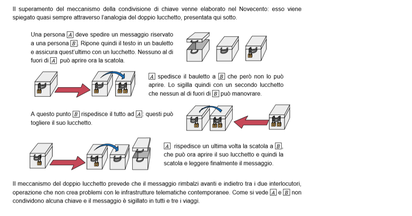




Schema dei rotori della macchina Enigma

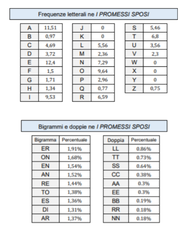


Elementi di crittografia moderna: il doppio lucchetto



Un po' di crittoanalisi: L'analisi delle frequenze

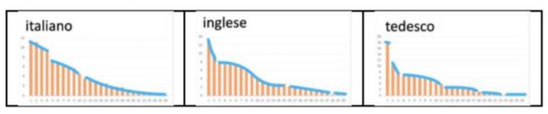
Una semplice crittanalisi statistica basata sulle caratteristiche statistiche delle lingue è in genere sufficiente per forzare il testo.



Frequenza delle lettere in italiano

Lettera	%	Lettera	%	Lettera	%
a	11,74	h	1,54	q	0,51
b	0,92	i	11,28	r	6,38
c	4,50	l	6,51	s	4,98
d	3,73	m	2,52	t	5,63
e	11,79	n	6,88	u	3,02
f	0,95	o	9,83	v	2,10
g	1,65	p	3,05	z	0,49

Le impronte linguistiche



LICEO CLASSICO E LINGUISTICO T. LUCREZIO CARO- ROMA

Gli alunni della classe seconda del Liceo Matematico

Le insegnanti: Erminia Izzo e Francesca Ruzzi con la collaborazione di Claudia D'Armiento