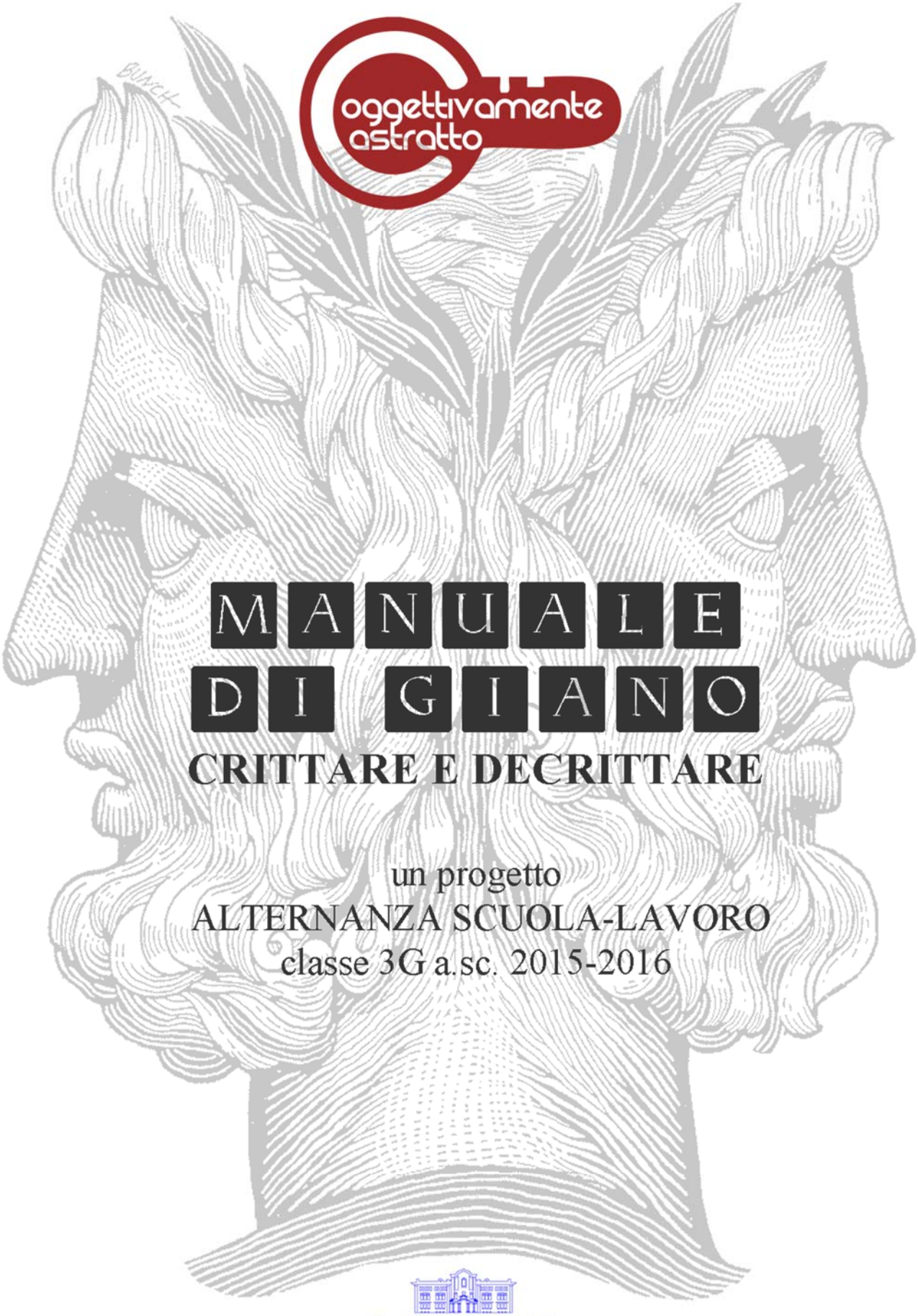
oggettivamente astratto



MANUALE DI GIANO

CRITTARE E DECRITTARE

un progetto
ALTERNANZA SCUOLA-LAVORO
classe 3G a.sc. 2015-2016

MAMIANI
LICEO STATALE - ROMA

Sotto il segno di Giano: il dio della verità e della bugia

Giano - il dio dalle due facce che decretava il passaggio dalla pace alla guerra, che sapeva distinguere il bianco dal nero e il vero dal falso - era una divinità romana molto importante: la leggenda vuole che avesse dimora in quella parte di Roma che ancora oggi chiamiamo in suo onore Gianicolo.

Proprio sulle pendici del piccolo colle di Giano e precisamente in via Dandolo, ha sede il Museo della Matematica del Comune di Roma “Numeria”.

Forse non è un caso se anche la sede storica del Ministero dell'Università, Istruzione e Ricerca sia nella stessa zona. Ci piace pensare che un po' dell'antica magia del Bosco Sacro, che proprio sul Gianicolo estendeva il suo dominio, sia rimasta nell'aria e ci porti fortuna.

La matematica e la didattica hanno - infatti - più che mai bisogno del benevolo sguardo di divinità amiche: forse così noi italiani riusciremo a riguadagnare una posizione decente nelle statistiche internazionali sulle abilità matematiche, che ci vedono adesso come il paese occidentale a maggior tasso di analfabetismo numerico.

Giano con il suo sguardo duplice vedeva chiaro nel passato e lì trovava le ragioni per decidere il da farsi nel futuro: guerra o pace erano scelte nette che andavano tolte dai veli dell'ambiguità e come il suo “gemello” Iktomi, divinità analoga della cultura mitica dei nativi americani della tribù dei Sioux-Lakota, estendeva il suo dominio celeste ai concetti del vero e del falso, ora svelandoli ora nascondendoli ai mortali. Giano era un dio ambiguo e allo stesso tempo capace di chiarezza: criptico e decriptico allo stesso tempo.

Quale migliore “vicino di casa” per Numeria, la dea della matematica? Che cos'è infatti la matematica se non il saper distinguere - con criteri sicuri - il vero dal falso?

Per non parlare della crittografia e della steganografia: arti matematiche bifronti per eccellenza, care agli eserciti e alle cancellerie di tutto il mondo fin dagli albori della civiltà occidentale e oggi momenti fondamentali della sicurezza bancaria e della frontiera della ricerca matematica odierna.

Questo Manuale di crittografia nasce grazie al Protocollo d'intesa tra il Comune di Roma – Sovraintendenza Capitolina, Direzione Musei Scientifici– e il Liceo Mamiani con la finalità di divulgare la cultura matematica attraverso la collaborazione tra il Museo "Numeria" (Comune di Roma) e il Museo Lucio Lombardo Radice (Liceo Mamiani).

Il progetto ha lo scopo di favorire, nell'apprendimento, oltre alle conoscenze di base, l'acquisizione di competenze spendibili nel mondo del lavoro.
Viviamo in un mondo di lavoro "liquido" e competitivo anche a livello internazionale ed é bene abituare i nostri ragazzi a saper fare i curricula, i colloqui di lavoro, ma soprattutto far loro capire che, come diceva Einstein :" in un buon lavoro il genio è il 10% e l'altro 90% è traspirazione".
Può sembrare banale, ma è questo, spesso il messaggio più difficile da trasmettere a dei giovani, così avvezzi al virtuale e alle sue rapide e indolori conclusioni, che spesso non sanno più reggere il duro confronto con la realtà.
Infatti questa dicotomia – di platonica memoria - tra la τέχνη e il pensiero critico non è sempre esistita: nella nostra scuola è retaggio della Legge di riforma Gentile che, ignorando la lezione del nostro Rinascimento, dove l'arte e la scienza si apprendevano andando a "bottega", aveva voluto una scuola lontana dal lavoro pratico, intellettuale o manuale che fosse.
Certo, è facile immaginare uno stage per un ragazzo dell'alberghiero o per uno che vuole diventare chef, ma come la mettiamo con i Licei? E se poi si vuole insegnare ai ragazzi un "mestiere" che abbia a che fare con la cultura matematica la scelta si fa ancora più difficile. Difficile, ma a ben vedere non impossibile: esistono professioni che fanno proprio al caso nostro.
Quella di museologo della matematica ad esempio, che compendia in sé conoscenze di storia della matematica con la museologia, la didattica e la divulgazione.
Fantascienza? No realtà. A Roma esistono ben due realtà "museali" dedicate alla più austera delle scienze: uno è il "museo" del Comune di Roma di cui abbiamo accennato sopra e l'altro è quello del Mamiani, creato dalla passione di Patrizia Cassieri per la disciplina che insegna e dall'entusiasmo dei suoi eccezionali allievi.
Ecco i due soggetti della convenzione, ecco il nostro esperimento.
La scelta di studiare la crittografia è sorta spontanea: al suo interno c'è la storia, la cultura e la matematica classica e la ricerca di frontiera è un campo in continua evoluzione che ben si presta alla realizzazione di nuovi exhibit - macchine esplicative o riproduzioni storiche di crittografi - che andranno ad arricchire il museo del Mamiani.
Anche questo piccolo libro di esempi, spiegazioni e esercizi di crittografia è opera dei ragazzi che si sono davvero meritati i crediti che la Legge concede loro.
Naturalmente, non avrebbero né saputo progettare né realizzare gli exhibit storici, il sito della mostra, il logo e la stesura del presente libricino senza l'aiuto dei loro

insegnanti, tutor a pieno titolo della sperimentazione: Nicoletta Allegretti, Patrizia Cassieri, Alessandra De Angelis e senza i preziosi collaboratori Ezio Bonfanti e Diego Urbani. Un'équipe formata da competenze ed esperienze professionali complementari tra loro e da colleghi che si stimano reciprocamente e lavorano bene insieme. Con questa iniziativa di alternanza scuola/lavoro il Liceo Terenzio Mamiani si è confermato ancora una volta una punta d'eccellenza per la cultura romana.

Un grazie dunque alla Dirigente Scolastica, Dottoressa Tiziana Sallusti, che è ormai molto nota per le sue iniziative culturali e la sua sensibilità didattica, ma anche al Sovrintendente della Sovrintendenza Capitolina ai Beni Culturali, Dr. Claudio Parisi Presicce, che ci ha permesso di stipulare questa convenzione e in ultimo, ma non certo per importanza, un grazie va al Dr. Bruno Cignini, direttore dei Musei scientifici comunali, ornitologo di fama, ma capace di "volare in alto" anche in ambiti culturali diversi dai suoi e che speriamo ci aiuti ad aprire presto la casa di Numeria a via Dandolo. Ma il grazie più grande va ai ragazzi del Liceo Mamiani che hanno dimostrato ampiamente di saper trasformare le nozioni di matematica in un percorso museale interessante, ricco di contenuti storici e gioiosamente adatto a tutti.

Secondo noi, Lucio Lombardo Radice, antico allievo del Mamiani, se fosse vissuto oggi, avrebbe sicuramente scelto di fare questo esperimento di alternanza scuola/lavoro, perché nessuno come lui credeva che la matematica fosse un mestiere da intellettuali e non da contabili.

E' questo in sintesi il messaggio che abbiamo cercato di trasmettere ai ragazzi del Mamiani.

Roma, maggio 2016

Wilma Di Palma

Responsabile Museo Matematica "Racconti di Numeria"

Sovrintendenza Capitolina BBCC

Comune di Roma

INDICE

1. CRITTOGRAFIA

L'importanza di comunicare senza essere intercettati è sempre stata una necessità molto sentita fin dalla più remota antichità: re, papi, generali e addetti alle segreterie di stato, tutti hanno cercato di avere a disposizione dei sistemi per nascondere i loro segreti. Ognuno aveva al suo servizio qualche specialista in crittografia, che fosse capace di inventare algoritmi inviolabili. Per contro, l'Intelligence di queste stesse corti, mentre da un lato cercava di nascondere il vero significato dei propri dispacci, dall'altro si adoperava per carpire il segreto di quelli nemici intercettati. Poteva anche darsi che il "matematico" autore dell'algoritmo per criptare i messaggi fosse anche quello che cercava di mettere in chiaro gli scritti dei nemici, come un Giano bifronte: ma nel primo caso faceva della crittografia, mentre nel secondo si trasformava in un crittoanalista. Due mestieri simili, ma non uguali. In breve, si potrebbe dire che la storia della crittografia altro non è se non l'evolversi di algoritmi sempre più sofisticati, che vengono man mano inventati per sostituire i precedenti non più inviolabili. Criptare e decrittare non è un gioco per ragazzi con una certa predisposizione al calcolo matematico: se un tempo su quest'arte si reggevano intrighi, amori, potere e guerre, oggi il suo impiego civile è fondamentale per la sicurezza della nostra identità telematica, dell'intero sistema bancario e quindi dell'economia mondiale.

La crittografia è dunque lo studio di come scrivere messaggi in forma segreta in maniera tale che solo i destinatari autorizzati siano in grado di leggerli in chiaro e capirne così il contenuto. Un criptosistema, o sistema cifrato, è quindi un modo per rendere le comunicazioni più sicure.

Lo schema del sistema crittografico è il seguente:
- il mittente **M** prepara il messaggio **x**,testo in chiaro, da spedire;
- **M** applica al messaggio **x** una procedura, algoritmo di cifratura, definita da unachiave che genera il messaggio **y**, testo cifrato, da spedire al destinatario **D**;
- **D** riceve il messaggio **y** al quale applica un algoritmo di decifratura con chiave,riottenendo il testo in chiaro;
- un eventuale intruso che intercetta il messaggio cifrato **y** non deve poter risalire al messaggio **x**.

I criptosistemi più antichi sono tutti a “chiave privata” cioè chi invia il messaggio e chi lo riceve conoscono entrambi l'algoritmo che tramuta il messaggio da linguaggio naturale, in chiaro, in quello criptato e viceversa. La chiave è un segreto che il mittente e il destinatario conservano gelosamente. Il maggiore svantaggio dei sistemi a chiave privata è il fatto che due utenti devono scambiarsi una chiave in qualche modo sicuro prima di poter cifrare qualunque dato. Inoltre tali chiavi devono essere cambiate spesso e ciò costituisce sicuramente un problema a cui si è cercato di ovviare introducendo dei sistemi a “chiave pubblica”.

1.1 LA SCACCHIERA DI POLIBIO

Polibio nato a Megalopoli, in Arcadia, tra il 205 -200 a. C., storico greco, ricoprì incarichi militari di grande prestigio, arrivando nel 170 a.C. ad occupare la carica di ipparco, comandante di uno squadrone di cavalleria.

L'opera principale di Polibio, *Storie*, nasce direttamente dalla sua esperienza personale e narra le guerre puniche, documentando l'ascesa di Roma da potenza locale della penisola italica a dominatrice assoluta e incontrastata della realtà mediterranea

Polibio ideò il più antico codice poligrafico. Lo storico greco lo descrive come un metodo per inviare messaggi mediante l'uso di torce, come fosse un telegrafo ottico. Questo "telegrafo a fiaccole", nato come sistema di comunicazione a distanza divenne nei secoli successivi un sistema crittografico. Utilizzato dai Romani per le trasmissioni lungo le vie consolari e quelle costiere, il codice, adattabile a qualsiasi lingua, fu alla base di macchine cifranti fino alla Prima Guerra Mondiale.

Esso può essere applicato anche come cifrario a colpi, quello, per esempio, usato dai detenuti: il messaggio viene battuto lasciando una pausa breve tra i due numeri che sostituiscono la lettera e una pausa più lunga tra una lettera e l'altra.

Nel passo delle *Storie* (X,45-47), Polibio descrive l'uso del sistema ma non fornisce indicazioni per la realizzazione di un manufatto utilizzabile per la codifica.

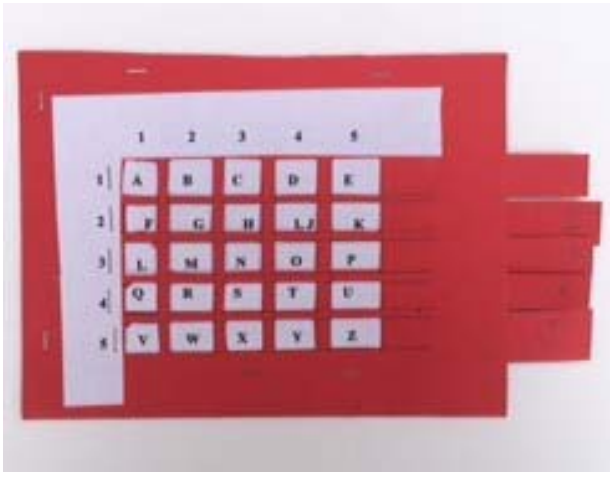
Funzione

La scacchiera di Polibio è un cifrario per sostituzione che associa ad ogni lettera dell'alfabeto in chiaro una coppia ordinata di numeri. L'insieme di partenza è costituito dalle 24 lettere maiuscole dell'alfabeto greco, quello di arrivo dai primi cinque numeri, che i Greci scrivevano utilizzando le lettere minuscole del loro alfabeto.

In questo metodo di cifratura si ha:

- l'alfabeto del messaggio in chiaro
- l'alfabeto del messaggio cifrato
- la corrispondenza biunivoca tra i due alfabeti, definita dalla forma della scacchiera.
- la chiave, definita dalla particolare permutazione delle lettere poste sulla scacchiera.

Prepariamo un modello



Materiale

- Un cartoncino
- Un foglio di carta
- Forbici
- Spillatrice
- Righello

Costruzione

Utilizziamo le forbici per ritagliare sul cartoncino due rettangoli identici e 5 listelli di pari lunghezza. Dopo aver disegnato, su uno di essi, una griglia 5X5, sovrapponiamo i due quadrilateri e con la spillatrice fissiamo tre lati in modo da ottenere una tasca. Applichiamo su ciascun listello, a gruppi di cinque, le lettere dell'alfabeto ordinario precedentemente scritte su un foglio di carta. Inseriamo sulla cornice della griglia, in corrispondenza di righe e colonne, i numeri 1,2,3,4,5. Posizioniamo i listelli in modo tale che siano liberi di scorrere all'interno della tasca.

Come cifrare

Le lettere dell'alfabeto sono disposte nel riquadro centrale secondo l'ordine naturale. Le righe e le colonne sono numerate: tali numeri saranno le "coordinate "delle lettere che costituiscono il messaggio in chiaro. Tutto è pronto per la cifratura.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

TESTO IN CHIARO: **CIAO**

- La lettera **C** si trova nella 1°riga e nella 3°colonna, quindi si sostituisce con la coppia (1;3);
- La lettera **I** si trova nella 2° riga e 4° colonna, quindi (2;4);
- La lettera **A** si trova nella 1° riga e 1° colonna, quindi (1;1);
- La lettera **O** si trova nella 3° riga e 4° colonna, quindi (3;4).

Si ottiene il *TESTO CIFRATO*: **13 24 11 34**

Esercizio 1
TESTO IN CHIARO: **LIBRO**

TESTO CIFRATO:……

Esercizio 2
TESTO CIFRATO: **35 34 31 24 12 24 34**.

TESTO IN CHIARO:.....

Esercizio 3
Cambiamo la disposizione dei listelli, ossia la **chiave**, crittografiamo nuovamente la parola **LIBRO.** Si ottiene il

TESTO CIFRATO……

1.2 IL CIFRARIO DI CESARE

Svetonio nella *Vita dei dodici Cesari,* opera del II secolo d.C.,scrive nel Cap I, paragrafo 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 quis investigare et persequi volet, quartam elementorum litteram, id est D pro A et perinde reliquas commutet."

Dunque Giulio Cesare adoperava per le sue corrispondenze riservate un sistema crittografico per sostituzione. Questo cifrario monoalfabetico è il più antico algoritmo crittografico di cui si abbia traccia storica e il primo in cui si introduce l'uso di una chiave che è il modo con cui opera l'algoritmo di sostituzione delle lettere cifrate a quelle in chiaro. Risultò per molto tempo sicuro ed efficace grazie alle successive forme più raffinate che presero in considerazione per la cifratura tutte le possibili permutazioni delle lettere dell'alfabeto. Furono i crittoanalisti arabi attorno all'anno 1000 a trovare il punto debole della sostituzione monoalfabetica. L'idea vincente fu quella di notare che in ogni lingua le lettere dell'alfabeto appaiono con una loro frequenza caratteristica e il metodo di sostituzione non altera la statistica del messaggio. Da allora questi modelli crittografici divennero decifrabili.

Nella *Vita dei dodici Cesari*, Svetonio descrive l'uso del sistema ma non fornisce indicazioni per la realizzazione di un manufatto utilizzabile per la codifica.

Funzione

Il cifrario di Cesare è un sistema crittografico per sostituzione monoalfetica in cui l'alfabeto cifrante è ottenuto dall'alfabeto in chiaro traslando di k=3 posizioni le lettere. L'insieme di partenza e quello di arrivo sono costituiti dalle 21 lettere dell'alfabeto.

In questo metodo di cifratura si ha:

- l'alfabeto del messaggio in chiaro in lettere maiuscole
- l'alfabeto del messaggio cifrato in lettere minuscole
- la corrispondenza biunivoca tra i due alfabeti
- la chiave, definita dalla scelta del numero naturale k, con $0 < k < 21$.

Prepariamo un modello

Materiale

- Due cartoncini circolari di diametro diverso
- Riga
- Goniometro
- Un fermacampione

Costruzione

Dopo aver sovrapposto i due cartoncini in modo che risultino concentrici, li uniamo al centro con il fermacampione. Così facendo il cartoncino più piccolo potrà ruotare. Successivamente scriviamo le lettere dell'alfabeto nella parte esterna dei due cerchi: in quello più piccolo l'alfabeto minuscolo per cifrare, nell'altro l'alfabeto maiuscolo. Le lettere dei due alfabeti devono corrispondersi nei due cerchi.

Ecco pronto il nostro cifrario di Cesare!

Come cifrare

Per crittare e decrittare messaggi basterà scegliere una chiave, ovvero il numero di lettere che intercorrono tra la **A** dell'alfabeto in chiaro e la **a** dell'alfabeto per cifrare, e ruotare in senso antiorario il cerchio più piccolo di tante lettere quanto è il numero della chiave.
Proviamo a scrivere in chiave **(A,3)** il seguente messaggio

TESTO IN CHIARO: **VEDIAMOCI DOMANI**
Dobbiamo spostare il cerchio piccolo di **3** lettere, quindi la **A** corrisponderà alla **d**, la **B** alla **e**, la **C** alla **f** e così via. Si ottiene il testo cifrato: **bhgndprfngrpdqn.**

Esercizio 1

Scegliamo una chiave diversa e crittografiamo i seguenti testi

TESTO IN CHIARO: **I NEMICI SONO VICINI**
TESTO CIFRATO:……..

TESTO IN CHIARO: **SONO A CASA**
TESTO CIFRATO:……..

Esercizio 2

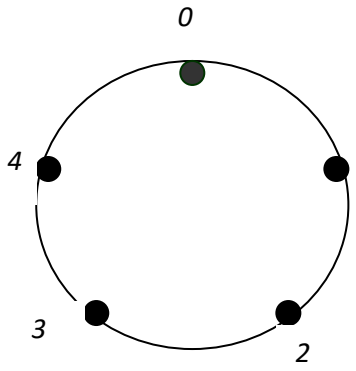
Decrittiamo questo testo in chiave **(A,4)**

TESTO CIFRATO: **golvevoshogizevi**
TESTO IN CHIARO:……

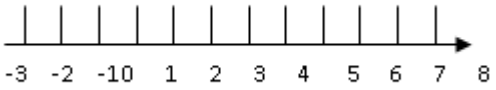
1.2.1 CIFRARIO DI CESARE E ARITMETICA MODULARE

Aritmetica modulare o dell'orologio

L'aritmetica modulare è chiamata anche aritmetica dell'orologio poiché in presenza di una *addizione* o di una *moltiplicazione* modulo *n* si opera come se gli elementi dell'insieme sui quali agisce l'operazione, chiamati classi resto *mod. n,* fossero rappresentati lungo una circonferenza sulla quale vengono segnati *n* punti a intervalli regolari, facendo corrispondere a ogni punto una classe. Se si pone, per esempio, *n=5*, allora sulla circonferenza si individuano 5 punti come nella figura sotto indicata.



Questo quadrante è una scala per il sistema di numerazione *mod. 5*, così come la retta orientata rappresenta una scala per il nostro sistema di numerazione ordinario.



Sulla retta orientata le addizioni si eseguono spostandosi di un certo numero di spazi verso destra; nel sistema *mod.5* i risultati si calcolano ruotando di un certo numero di archi nel verso delle lancette dell'orologio.
Allora, indicati con i simboli $\oplus$ e $\otimes$, rispettivamente, l'operazione di addizione e di moltiplicazione, si ottiene :
$4 \oplus 2 = 1$ perché "spostandosi" di 2 posti, in verso orario, a partire da 4, si "arriva"a 1
$4 \otimes 2 = 3$ poiché $4 \cdot 2 = 8$ e "spostandosi" di 8 posti, in verso orario, a partire dal punto corrispondente allo 0 si "arriva" a 3

Esercizio 1
Costruire la tabella operativa dell'addizione *mod.5*

$\oplus$	0	1	2	3	4
0					
1					
2					
3					
4					

- *proprietà ……...*
- *elemento neutro……*
- *elemento inverso……*
- la somma di due numeri pari è sempre pari?
- la somma di due numeri dispari è sempre pari?
- la somma di un numero pari e di un numero dispari è sempre dispari?

Se con Θ si indica l'operazione inversa dell'addizione ciclica, per eseguire l'operazione

2 Θ 4 basta operare 'direttamente' con l'elemento inverso di 4

- 2Θ4=*……..*

Esercizio 2

Costruire la tabella operativa della moltiplicazione *mod.5*

$\otimes$	0	1	2	3	4
0					
1					
2					
3					
4					

- *proprietà ……...*
- *elemento neutro……*
- *elemento inverso……*
- $3 \otimes x = 1 \Rightarrow x = ...$
- $2^4 = \ldots\ldots\ldots\ldots\ldots$
- $3^4 = \ldots\ldots\ldots\ldots\ldots$

Esercizio 3

Risolvere la seguente equazione nell' insieme delle classi resto *mod.5*

$x \oplus (4\Theta 1) = 2 \oplus (3 \oplus 1)\ \Theta 4 \Rightarrow \ldots\ldots\ldots\ldots\ldots$

Il codice di Cesare

Cifrare e decifrare significa, in estrema sintesi, spostare le lettere dell'alfabeto. Quindi una semplice cifratura in cui l'alfabeto cifrante è ottenuto mediante una traslazione a destra di *3* posti dell'alfabeto ordinario, diventa un'addizione modulare. Infatti se si dispongono in cerchio le *21* lettere dell'alfabeto italiano aggiungendo un *22-esimo* carattere *"spazio"* e si sostituiscono le singole lettere del testo chiaro con quelle ottenute avanzando in senso orario di *3* posizioni, allora il codice di Cesare diventa "addizionare 3 *mod.22"*.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	spazio
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Esercizio 1

1) Scrivere un messaggio ***x*** in chiaro

x:…….

e codificarlo nel messaggio ***y*** utilizzando la chiave *k=3*

y:……..

Esercizio 2
Sapendo che la chiave cifrante è *k=2*, decodifica il seguente testo

x: *RFRPSPEQFG*

y:……..

Esercizio 3
Se si cambia l'algoritmo di cifratura "addizionare 2 *mod.22"* in "moltiplicare 2 *mod.22"* qual è il messaggio cifrato del seguente testo in chiaro?
x: N*AVI*

N = $[11] \to 11 \cdot 2 = 22 \to [0] = A$

A= $[0] \to 0 \cdot 2 = 0 \to [0] = A$

V= $[19] \to 19 \cdot 2 = 38 \to [16] = S$

I= $[8] \to 8 \cdot 2 = 16 \to [16] = S$ Si ottiene un codice valido? Perché?

1.3 IL DISCO DI ALBERTI

Leon Battista Alberti (Genova 1404 - Roma 1472), una delle figure più significative dell'Umanesimo italiano, di cui seppe interpretare le ambiguità e gli splendori, contribuì, attraverso i suoi studi, a tracciare una nuova mappa di valori critici e un diverso metodo di interpretare il mondo. Alberti fu un pensatore e uno scienziato "universale", dai mille interessi e ribelle ad ogni definizione: è stato al tempo stesso un grande architetto, un matematico, un fine letterato, un latinista, un musicista, un uomo di Chiesa e un astuto diplomatico. Nel primo trattato di storia della crittografia, *De componendis Cyfris* (1467), egli, con approccio scientifico, analizza l'uso delle vocali, delle consonanti e la frequenza delle lettere nelle parole. Comprende, così, le inefficienze dei sistemi monoalfabetici e, al fine di renderli meno vulnerabili, introduce un codice crittografico polialfabetico che applica attraverso il **Disco cifrante**, primo dispositivo nella storia della crittografia. Il testo rimase volutamente inedito e fu dato alle stampe solo nel 1568. Da allora divenne punto di partenza ineludibile per storici della matematica e studiosi di crittografia. Nel metodo di Alberti gli alfabeti sono due e la chiave varia in continuazione durante la codifica. Dunque, lo studio delle frequenze non dà risultati perché la stessa lettera chiara è cifrata sempre con lettere diverse. Enigma, utilizzata dai nazisti nel corso della Seconda Guerra Mondiale, è considerata la versione elettromeccanica ed evoluta del disco cifrante di Leon Battista Alberti.

Funzione

Il crittografo di Alberti è un dispositivo meccanico che realizza permutazioni variabili delle lettere dell'alfabeto. Di questo oggetto devono esistere due copie: una in uso al mittente e l'altra per il destinatario. Essi concordano segretamente la chiave cifrante costituita da una coppia di caratteri che determinano la corrispondenza iniziale tra i caratteri del disco di diametro maggiore e quelli del disco interno. Al termine di questa procedura i due interlocutori sono pronti a scambiarsi i loro messaggi segreti.

Prepariamo un modello

***Materiale*:**

- Due cartoncini di colore diverso
- Fermacampione
- Riga

***Costruzione*:**

Dai cartoncini ritagliamo due cerchi di raggio diverso. Dividiamo il cerchio di raggio maggiore in 24 settori su ognuno dei quali scriviamo in carattere maiuscolo le seguenti lettere e i seguenti numeri: A, B, C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, Z, 1, 2, 3, 4. Prendiamo adesso il cerchio con raggio minore e dividiamo anch'esso in 24 settori su ognuno dei quali scriviamo in minuscolo i seguenti caratteri: x, y, q, c, j, o, k, b, p, f, z, s, e, m, d, g, v, t, a, i, r, l, h, n.

Sovrapponiamo i due cerchi in modo tale che risultino concentrici, foriamo con le forbici il centro comune e inseriamo il fermacampione. A questo punto il cerchio di raggio minore, contenente l'alfabeto cifrato può ruotare su quello esterno contenente l'alfabeto in chiaro.

Come cifrare

Ruotiamo il disco mobile fino a far coincidere la minuscola **i** sotto la maiuscola **A** definendo, in questo modo, la chiave. Adesso siamo pronti per cifrare!

TESTO IN CHIARO: **OGGETTIVAMENTE ASTRATTO**

Ad ogni lettera maiuscola in chiaro, letta sul disco fisso, sostituiamo la corrispondente minuscola, cifrata sul disco mobile secondo la chiave **(A,i)**

TESTO CIFRATO: **kyynssqeijnosnizsfissk.**

Cambiamo ora chiave e scegliamo (**A,p)**. Ruotiamo il disco mobile fino a far coincidere la minuscola **p** sotto la maiuscola **A** definendo la chiave. Adesso siamo pronti per cifrare

*TESTO IN CHIARO***: CODICE**

Per maggiore sicurezza inseriamo nel testo in chiaro un numero, a scelta, tra 1 e 4 che ci consente di cambiare la chiave in corso d'opera, per esempio

TESTO IN CHIARO: **CO3DICE**

Ad ogni lettera maiuscola, in chiaro, letta sul disco fisso, sostituiamo la corrispondente minuscola, cifrata sul disco mobile secondo la chiave **(A,p)**, finché non incontriamo il numero **3** che dice di sostituire la chiave **(A,p)** in **(A,k)** poiché **k** è la lettera del disco mobile corrispondente al numero **3** sul disco fisso. Quindi continuiamo nella codifica secondo la nuova chiave

*TESTO CIFRATO***: zikfmpz**

<u>COME DECIFRARE</u>

TESTO CIFRATO: **lfqsskyfixqi**
Utilizziamo la stessa chiave **(A,i)** e ad ogni lettera cifrata minuscola, letta sul disco mobile, sostituiamo la corrispondente maiuscola, in chiaro sul disco fisso.
TESTO IN CHIARO: **CRITTOGRAFIA.**

Esercizio 1
Chiave segreta **(A,r)**
TESTO IN CHIARO: **CHIAVE**

*TESTO CIFRATO***: …… .**

Esercizio 2
Chiave segreta **(A,h)**
TESTO IN CHIARO: **INDA2GINE**

TESTO CIFRATO: **……..**

Esercizio 3
Chiave segreta **(A,s)**
TESTO CIFRATO: **ighlbpbollerloqqzcxjdvb**

TESTO IN CHIARO: **…….**

2. STEGANOGRAFIA

Il termine steganografia, composto dal greco *στεγανός* “impenetrabile” e dal tema di *γράφω* ”scrivo” , coniato dall’umanista tedesco Tritemio (Giovanni Tritheim, 1462-1516), rappresenta l’insieme delle tecniche che consentono di inviare un messaggio nascondendo agli occhi di un eventuale osservatore, non il contenuto, ma il messaggio stesso. Fino alla pubblicazione dell’opera di Tritemio, *Steganographia, hoc est ars per occultam scripturam animi sui voluntatem absentibus aperiendi,* la steganografia era considerato un metodo di scrittura crittografico. Essa invece, al contrario della crittografia come si evince dal titolo dell’opera, parte dal presupposto che il messaggio segreto è completamente occultato e, quindi, impossibile da trovare. Nel corso dei secoli, sono stati ideati numerosi metodi steganografici, tutti molto diversi tra loro. Nelle *Storie* di Erodoto (libro V, 35) si racconta che Istieo, alla vigilia della prima guerra persiana, fece tatuare un messaggio, sul capo rasato di uno schiavo, per incoraggiare Aristagora di Mileto a ribellarsi a Serse:
”*Accadde che contemporaneamente gli giungesse anche da Susa da parte di Istieo il messaggero dalla testa segnata, che annunziava ad Aristagora di ribellarsi al re. Infatti Istieo, volendo dare ad Aristagora l’ordine di ribellarsi, non aveva alcun altro modo per annunziarglielo con sicurezza, essendo le strade sorvegliate; allora, fatta rasare la testa al più fido degli schiavi, vi impresse dei segni, e aspettò che ricrescessero i capelli. Non appena ricrebbero, lo spedì a Mileto, non comandandogli null’altro se non che, quando giungesse a Mileto, dicesse ad Aristagora di fargli radere e guardare la sua testa: i segni impressi ordinavano, come già prima ho detto, la rivolta*.”
Nel libro VII delle *Storie* si racconta dell’espediente usato da Demarato che dall’esilio intendeva avvisare gli Spartani del progetto di invasione da parte del re Serse: ”*…allora escogitò questo stratagemma: presa una tavoletta doppia ne raschiò la cera e poi sul legno della tavoletta scrisse il piano del re. Fatto ciò versò di nuovo la cera liquefatta sullo scritto, in modo che, venendo portata vuota, la tavoletta non procurasse nessun fastidio da parte dei custodi delle strade. Ma quando giunse a Sparta, gli Spartani non riuscivano a comprendere cosa essa significasse prima che - a quanto mi hanno trattato - la figlia di Cleomene e moglie di Leonida, Gorgo, avendolo essa compreso, lo suggerì loro, invitandoli a raschiare la cera e dicendo che avrebbero trovato lo scritto sul legno. Dandole ascolto lo trovarono e lessero e poi lo spedirono agli altri Greci*.” Nella *Naturalis Historia* (libro XXVI, 39) Plinio il Vecchio (I sec. d.C.) parla di un inchiostro simpatico, estratto dal lattice di una pianta e utilizzato dagli amanti per scambiarsi messaggi. Il testo, una volta essiccato l’inchiostro, poteva essere letto dopo averlo cosparso di cenere: “ *Tithymallum* (forse Euphorbia catapuzia) *nostri herbam lactariam vocant, alii lactucam caprinam, narrantque lacte eius inscripto corpore, cum inaruerit, si cinis inspergatur, apparere litteras, et ita quidam adulteras adloqui maluere quam codicillis*.” 36

2.1 LA GRIGLIA DI CARDANO

Medico, filosofo e matematico italiano di grande rinomanza nel XVI sec., Girolamo Cardano (Pisa 1501 – Roma 1576) è ancora ricordato per la disputa sostenuta con Niccolò Tartaglia a proposito della formula di risoluzione delle equazioni cubiche, nota come formula di Cardano, e per l'invenzione della sospensione che da lui ha nome. Infatuato dell'astrologia, fu uno di quegli uomini strani e bizzarri, bersagliato dalla fortuna e dalla sua stessa indole. Si racconta che avesse predetto come data della propria morte il settembre del 1576; ma siccome l'epoca fatale si avvicinava e non c'era nessun sintomo di una malattia che potesse ucciderlo, temendo che il sopravvivere portasse troppo discredito alla sua scienza, non prese più cibo e si lasciò morire di fame.

La sua concezione enciclopedica del sapere è all'origine della mole di opere pubblicate tra cui *De subtilitate,* 1550*,* e *De rerum varietate,* 1557 (*) nelle quali si trovano i nuovi alfabeti a chiave numerica auto cifrante, un'originale cifra polifona e soprattutto la celebre **griglia** a finestre su cui molte cancellerie europee impostarono per tutto il Cinquecento e il Seicento le corrispondenze. Questo è un sistema di permutazione meccanica delle lettere del testo in chiaro, che soltanto mediante l'uso di un apposito foglio di metallo con finestre, permette di selezionare solo le parti da leggere.

Funzione

La griglia di Cardano serve sia per la scrittura che per la lettura di un messaggio. L'intento è quello di celare il testo originario senza modificarlo in alcun modo; per questo motivo, è considerata una forma di steganografia.

Per scrivere il messaggio in chiaro si appoggia la mascherina su un foglio quadrettato e si inseriscono le singole lettere nei fori, ripetendo l'operazione dopo ognuna delle successive rotazioni di 90° della griglia. Si toglie la griglia e si cerca di riempire il resto del foglio con una successione "casuale" di lettere. In alternativa, le nuove lettere inserite potrebbero anche dar luogo ad una frase di senso compiuto.

Per la lettura basta applicare sul foglio una griglia, identica a quella usata dal mittente, ed individuare le lettere che restano scoperte.

(*) *Desubtilitate*, apud Sebastianum Henricpetri, Basileae, 1547. p. 320; *De rerum varietate libri XVII*, per H. Petri, Basileae, 1557, lib. XII, capI.XI. pp. 457 -465

Prepariamo un modello

Materiale:

- Un foglio di cartoncino rigido
- Un foglio di carta
- Forbici
- Righello.

Costruzione:

Ricaviamo, con le forbici, dal cartoncino rigido e dal foglio di carta, due quadrati identici. Col primo realizziamo la griglia ritagliando le caselle secondo il modello proposto.

Suddividiamo il secondo in sei righe e sei colonne. Posizioniamo la griglia sul foglio di carta quadrettato e cominciamo a scrivere il messaggio, da sinistra verso destra, a partire dal primo quadretto vuoto in alto a sinistra. Successivamente ripetiamo per tre volte la stessa operazione ruotando la griglia, ogni volta in senso orario, di 90° fino a completare la scrittura del testo in chiaro. A questo punto, tolta la griglia, è necessario riempire i quadretti vuoti con alcune lettere scelte in modo casuale.

Il destinatario del messaggio deve essere in possesso di una griglia identica a quella del mittente. Per leggere il messaggio deve posizionare la griglia sopra il foglio di carta ricevuto dal mittente e leggere il testo che filtra dalle aperture.

BIBLIOGRAFIA

- ✓ S. SINGH, *Codici & segreti,* Milano, 1999
- ✓ C. TOFFALORI, *Algoritmi*, Bologna, 2015
- ✓ GUERAGGIO, *Matematica*, Milano, 2012
- ✓ R. BETTI, *La crittografia*, *Lettera Matematica Pristem*, n°49, 2003
- ✓ P. PRETO, *I servizi segreti di Venezia*, Milano 2010
- ✓ SVETONIO TRANQUILLO, *Le vite dei Cesari*, a cura di G. Vitali, Vol. I, 56, Bologna, 1951 (Biblioteca Mamiani)
- ✓ ERODOTO*, Storie,* a cura di A. Izzo D'Accinni, D.Fausti vol. III,pp 42,43,pp 488,489, Milano, 2004 (Biblioteca Mamiani)
- ✓ Les Belles Lettres, Pline *L'ancien, Histoire Naturelle*, livre XXVI, 39 (Biblioteca Mamiani)
- ✓ *NUOVA ENCICLOPEDIA POPOLARE ITALIANA*, vol. IV, s.v. Cardano Girolamo, Torino, 1857 (Biblioteca Mamiani)
- ✓ *ENCICLOPEDIA DEGLI ANEDDOTI*, vol. I, 2324, Milano, 1946 (Biblioteca Mamiani)

Progetto Alternanza Scuola Lavoro
realizzato in collaborazione con

ROMA
Sovrintendenza Capitolina ai Beni Culturali
U.O. Musei Scientifici e Planetario-Museo Civico di Zoologia
Museo della Matematica

OFFICINE TERENZIO

Responsabile
Patrizia Cassieri

Tutor esterni
Wilma Di Palma (Comune di Roma), Ezio Bonfanti,
Diego Urbani (Officine Terenzio)

Tutor interni
Nicoletta Allegretti, Alessandra De Angelis

Project Team
Irene Azzara (Project Manager),
Lorenzo Riola (Chief Engineer), Pietro Salviati (Workshop Assistant)
Giovanni Mancini (Art Director),
Renato Bettini (Webmaster), Adriano Consolo (Web Designer)
Francesca Valeria Samà, Francesca Agostinelli, Giorgia Sacco (Writers)

Collaboratori
Davide Ahmar, Arianna Ambrosini, Luca Barbarito, Davide Bellumori, Margherita Cerioli, Dante Shintaro Cometti,Virginia Costa, Francesco D'Angelo, Giovanni Di Leo, Filippo Girardi, Filippo Iacchia, Gustavo La Cava, Giulia Melchiorre, Lorenzo Meledandri, Marco Nicoletti Altimari, Ilaria Orsi, Laura Perrucci, Valeria Pizzuto, Barbara Judith Salzano, Edoardo Soderini, Jacopo Pasquale Vitale, Leonardo Zozi.