Questo materiale è frutto della collaborazione di molte persone:
Maria Rita Agostini, Paola Bulzomì, Andreina D'Arpino, Marco Evangelista, Angela Fanti, Laura Lamberti, Anna Maria Mancini, Cristina Musumeci, Paola Paparini, Marina Pesce, Laura Sopranzi, Valentina Testa, Francesca Tovena, Maura Tuzzolo, Stefano Volpe

I INCONTRO

Nel corso del laboratorio analizzeremo in dettaglio alcuni metodi di cifratura utilizzati nel corso della storia, prestando particolare attenzione agli strumenti matematici coinvolti. Quando il materiale proposto è sovrabbondante, si indicano come facoltative alcune schede.

TAVOLA 1.0 (Facoltativa): il problema della decifrazione

Il primo esempio che viene discusso è stato tramandato da Svetonio, uno storico del II sec d.C. Nella sua Vita dei Cesari parla di un sistema utilizzato da Cesare per cifrare i suoi messaggi: egli spostava di tre lettere ogni lettera del messaggio da inviare.
Se indichiamo con lettere minuscole le 21 lettere dell'alfabeto, ciascuna lettera del nostro messaggio (**testo in chiaro**) sarà sostituita con la lettera che si trova tre posizioni più avanti, e che per comodità indicheremo con caratteri maiuscoli, ottenendo così un nuovo messaggio (**testo cifrato**) apparentemente privo di significato

a b c d e f g h i l m n o p q r s t u v z
D E F G H I L M N O P Q R S T U V Z A B C

Ad esempio se il messaggio da inviare è il seguente:
La madre di Lancillotto era la sacerdotessa di Avalon
il risultato dopo la cifratura sarà:

OD PDGUH GN ODQFNOORZZR HUD OD VDFHUGRZHVVD GN DBDORQ

Possiamo decidere di generalizzare questo sistema decidendo di spostare le lettere non di tre posizioni ma di una quantità arbitraria:
Un sistema di questo tipo, in cui ogni lettera del testo cifrato è ottenuta da una lettera de testo in chiaro spostando di un certo numero di posizioni le lettere, prende il nome di ***cifrario di Cesare*** *o di* ***cifratura per traslazione***.

Il numero di posizioni di cui spostare le lettere è una informazione aggiuntiva che permette di realizzare concretamente il metodo: essa viene detta **chiave di cifratura**.
Come si decifra? La chiave per decifrare si ricava in modo immediato dalla chiave per cifrare: basta spostarsi della stessa quantità di posizioni, ma nella direzione opposta.

TAVOLA 1.1: Cifratura e decifratura per traslazione con chiave assegnata. Una singola scheda (contraddistinta da una lettera dalla A alla F) consiste di 2 pagine. Ciascun ragazzo (o coppia di ragazzi) completa la prima parte della propria scheda, poi decifra la seconda meta' di una scheda preparata da altri. Basta fotocopiare un numero complessivo di schede pari al numero dei partecipanti.

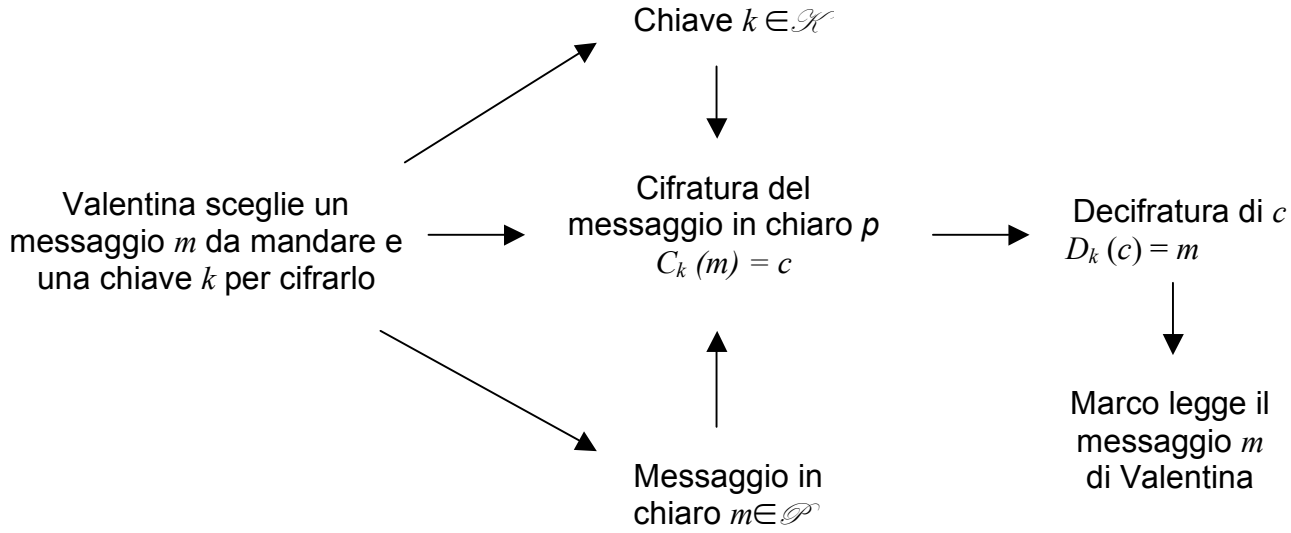
Discutiamo più in generale la nozione di crittografia.
La cifratura è una operazione di passaggio da un messaggio (detto messaggio in chiaro) ad un messaggio il cui significato è "nascosto": ad esempio il passaggio da un linguaggio ad un altro poco diffuso.
La cifratura permette di passare da un insieme di messaggi (detti **messaggi in chiaro**) ad un altro insieme di messaggi (detti **messaggi cifrati**): può dunque essere interpretata come una funzione tra questi due insiemi.

Possiamo cifrare singole parole (basta pensare ad un vocabolario inglese-italiano, ad esempio) o cifrare le singole lettere dell'alfabeto (come fa il cifrario di Cesare).

Un **crittosistema** è costituito da:

- l'insieme dei messaggi in chiaro $\mathscr{P}$ i cui elementi vengono indicati spesso con la lettera m;
- l'insieme delle chiavi $\mathscr{K}$ in cui ogni elemento k determina una trasformazione di cifratura C_k e una trasformazione di decifratura D_k che sono una l'inversa dell'altra;
- l'insieme dei messaggi cifrati $\mathscr{C}$ i cui elementi sono indicati spesso con la lettera c.

Un crittosistema è determinato da una terna $(\mathscr{P}, \mathscr{K}, \mathscr{C})$ e la comunicazione tra due persone, Valentina e Marco, può essere riassunta dal seguente diagramma:



Nel cifrario di Cesare:

- gli elementi $m \in \mathscr{P}$ sono le parole che vogliamo inviare (in una lingua fissata);
- la chiave consiste in fase di cifratura nello spostare di tre posti le varie lettere (C_k) e in fase di decifratura nel rimetterle nella loro corretta posizione (D_k);
- gli elementi c sono il risultato dell'operazione di cifratura.

Quali funzioni possono essere usate per cifrare?
Iniziamo considerando il caso in cui la trasformazione di cifratura opera sulle singole lettere dell'alfabeto: la cifratura può essere realizzata tramite una funzione tra l'alfabeto di partenza (detto **alfabeto in chiaro**) all'alfabeto d'arrivo (detto **alfabeto cifrante**): abbiamo bisogno che a lettere diverse dell'alfabeto in chiaro corrispondano lettere diverse dell'alfabeto cifrante (perché questo ci assicura che, così, è possibile decifrare in modo univoco il testo) .
La funzione cifrante deve quindi essere iniettiva, cioè ad elementi distinti dell'alfabeto in chiaro devono corrispondere elementi distinti dell'alfabeto cifrante.
Chi riceve un messaggio cifrato deve essere in grado di interpretarlo ("decifrare").
Valentina e Marco si devono essere messi d'accordo prima su come "cifrare" e "decifrare" e scegliere un metodo efficace in modo che per gli altri sia sostanzialmente impossibile cifrare e decifrare un messaggio

Ci occuperemo soprattutto dei sistemi di cifratura che operano sulle singole lettere dell'alfabeto.
Per semplicità, supponiamo che l'alfabeto cifrante contenga solo lettere che si ottengono cifrando le lettere dell'alfabeto in chiaro; non introduciamo elementi di disturbo nell'alfabeto cifrante.
Nel nostro caso, quindi, dobbiamo verificare che :

- prese due lettere distinte dell'alfabeto in chiaro queste vengano criptate con lettere diverse (iniettività)
- ogni lettera dell'alfabeto cifrante è la cifratura di (almeno) una lettera dell'alfabeto in chiaro (suriettività).

Ovvero dobbiamo verificare che la funzione cifrante C_k sia biunivoca.
Ricordiamo che una funzione tra due insiemi A (dominio) e B (codominio) è biunivoca se è iniettiva e suriettiva.

- È iniettiva se ad elementi distinti di A corrispondono elementi distinti di B.
- È suriettiva se ogni elemento di B è immagine di almeno un elemento di A.

Si osservi che, anche se una funzione C_k è biunivoca, può non risultare opportuna dal punto di vista crittografico: ad esempio, la funzione che associa ogni lettera a se stessa (l'identità) produce un testo cifrato identico a quello in chiaro, e non è vantaggiosa. Più in generale, si chiederà che la funzione di cifratura non cifri mai una lettera con se stessa: dopo aver controllato la biettività della funzione cifrante, occorrerà discutere separatamente la sua convenienza da un punto di vista crittografico. Le possibilità per i cifrari di Cesare nel caso della lingua italiana sono solamente 20 perché ovviamente se una lettera si sposta di 21 posizioni, ritorna al punto di partenza. Mentre nel caso dell'alfabeto inglese abbiamo 25 alfabeti cifranti possibili dato che le lettere sono 26.

NOMENCLATURA:
Cifratura: operazione di passaggio da un messaggio (detto messaggio in chiaro) ad un messaggio (detto messaggio cifrato) il cui significato è nascosto.
Decifratura: operazione di recupero del significato originale (messaggio in chiaro) a partire dal messaggio cifrato.
Alfabeto in chiaro: alfabeto che permette di scrivere tutti i messaggi richiesti
Alfabeto cifrante: alfabeto che permette di scrivere tutti i messaggi richiesti, ma il cui significato non è immediatamente chiaro.
Chiave di cifratura: informazione aggiuntiva che permette di applicare concretamente la cifratura
Chiave di decifratura: informazione aggiuntiva che permette di applicare concretamente la decifratura

Abbiamo visto che volendo cifrare un messaggio usando il metodo di Cesare dobbiamo sostanzialmente traslare le lettere di un certa quantità di posizioni (che decidiamo noi e rappresenta la chiave utilizzata per cifrare). Tale operazione diventa più rapida utilizzando un cifrario rotondo, con due cerchi concentrici.
Assegniamo ad ogni lettera dell'alfabeto italiano in chiaro un numero corrispondente alla sua posizione come nella seguente tabella:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

Tabella 1

Dopodichè decidiamo un numero (ad esempio 5) che rappresenta la nostra chiave e lo sommiamo ad ogni posizione così da ottenere che nell'alfabeto cifrante la A corrisponda alla lettera in posizione 5 cioè alla F, la B alla G,…, la R alla Z, la S che occupa la posizione 16 corrisponda alla A, la T alla B,…., la Z alla E.
Il nodo fondamentale di questa procedura sta nel fatto che quando abbiamo deciso la corrispondenza tra la T e la B abbiamo sostanzialmente ragionato così:

- la lettera T occupa la posizione 17 (ricorda che partiamo dalla posizione 0),
- 17+5=22 ma le posizioni possibili sono 21 e sono numerate da 0 a 20 quindi il numero 22 non corrisponderebbe a nessuna lettera

- $22 = 1 \cdot 21 + 1$ e abbiamo deciso che la lettera T doveva corrispondere a quella in posizione 1 cioè alla B

Ed è per questo motivo che la lettera S corrisponde alla A (perché S= posizione 16, 16+5=21, $21 = 1 \cdot 21 + 0$ e la lettera A occupa la posizione 0), la U alla C e così via.
Quindi da un punto di vista matematico quando cifriamo con questo metodo operiamo una somma (per traslare) dopodichè se il risultato è maggiore di *21* ci interessiamo solo al resto della divisione per *21*: le lettere dell'alfabeto sono in corrispondenza biunivoca con i possibili resti della divisione di un intero per *21*. Ogni numero intero rappresenta una lettera: per sapere quale, basta calcolare il suo resto nella divisione per *21* e usare la Tabella 1 per individuare la lettera corrispondente.
(attento alle divisioni in cui compaiono numeri negativi: il resto è l'unico c compreso tra *0* e *20* tale $a = 21 \cdot q + c$ per un numero intero q.)

Proviamo a generalizzare, lasciando libero il numero delle lettere dell'alfabeto, che denoteremo con n *(*con n maggiore di *0)*: in un alfabeto di n lettere, possiamo chiamare 0, 1, ..., *n-1* le lettere e **identificare due numeri che abbiano lo stesso resto nella divisione per *n***. Per brevità, diciamo che due numeri che hanno lo stesso resto nella divisione per n sono **congruenti modulo *n* *(*o mod *n)*** e introduciamo un simbolo: se due numeri $a, b \in \boldsymbol{Z}$ sono ***congruenti modulo n***, scriviamo

$$a \equiv b \bmod n$$

Talora, usiamo l'aggettivo 'congruo' al posto di 'congruente'.
Osserviamo, per definizione, che **ogni numero *a* è congruente mod *n* al suo resto nella divisione per *n*, cioè all'unico *c* compreso tra *0* e *n–1* tale che $a = n \cdot q + c$ per un intero *q*.** Dunque, un qualsiasi numero intero (positivo o negativo) è congruente modulo n ad uno e ad uno solo tra i numeri 0, … , *n–1*.
Cerchiamo di riformulare questo concetto, per poter verificare in modo diretto se due numeri sono congruenti modulo n, senza bisogno di calcolare esplicitamente i resti della divisione per n. Si verifica facilmente che la precedente definizione può essere riformulata come segue:

Definizione Sia n un intero positivo fissato. Due numeri $a, b \in \boldsymbol{Z}$ sono ***congruenti modulo n*** se $a–b$ è un multiplo di n, ovvero,

$$a \equiv b \bmod n \Leftrightarrow (a–b) = n \cdot h \text{ per qualche } h \in \boldsymbol{Z}.$$

Esempi:

1. $25 \equiv 1 \bmod 3$ perché $25 – 1 = 24 = 3 \cdot 8$.
2. $67 \equiv 55 \bmod 6$ perché $67 – 55 = 12 = 6 \cdot 2$.
3. $55 \equiv 1 \bmod 6$ perché $55 – 1 = 54 = 6 \cdot 9$.
4. $–5 \equiv 1 \bmod 6$ perché $–5 – 1 = –6 = 6 \cdot (–1)$.

Osservazioni. Chiamiamo 'congruenza' la relazione definita sugli interi dall'essere congruenti.

1. Ogni numero è congruente a sè stesso, modulo qualsiasi n: dunque per la congruenza vale la *proprietà riflessiva*.
2. $a \equiv b \bmod n \Leftrightarrow (a – b) = n \cdot h \Leftrightarrow (b – a) = n \cdot (-h) \Leftrightarrow b \equiv a$: dunque per la congruenza vale la *proprietà simmetrica*.
3. Notiamo che gli esempi 2 e 3 ci suggeriscono la transitività della congruenza. Infatti vale anche che $67 \equiv 1 \ (6)$ perché $67 – 1 = 66 = 6 \cdot \mathbf{11}$.
   Più in generale se , $a \equiv b \bmod n$, cioè $(a–b) = n \cdot h$ e $b \equiv c \bmod n$, cioè $(b–c) = n \cdot k$, allora $(a–c) = (a – b + b – c) = (a – b) + (b – c) = n \cdot h + n \cdot k = n \cdot (h+k)$ e dunque $a \equiv c \bmod n$.
   Dunque per la congruenza vale la *proprietà transitiva*.
4. **La congruenza modulo *n* è una relazione di equivalenza.**

La congruenza divide quindi gli interi in sottoinsiemi tra loro disgiunti:
Definizione Dato $a \in \boldsymbol{Z}$, si denota con $\bar{a}$ oppure con $[a]$ l'insieme

$$\bar{a} = \{ b \in \boldsymbol{Z} \text{ tale che } b \equiv a \bmod n\} \text{ detto } \textbf{\textit{classi resto modulo n}}$$

e si dice che *a* **rappresenta** (o **è rappresentante di**) tale insieme.
A partire dalla prossima lezione, quando sarà chiara la distinzione tra il numero *a* e la sua classe, scriveremo semplicemente *a* per denotare il numero o la sua classe.
Come già osservato, fissato *n*, un qualsiasi numero intero (positivo o negativo) è congruo modulo *n* ad uno e ad uno solo tra i numeri 0, … , *n–1*. Dunque le classi resto modulo *n* sono esattamente *n* e ciascuna di esse ha uno ed un solo rappresentante in $\{ 0, 1, 2, ..., n-1 \}$. Cercheremo di usare sempre il rappresentante della classe scelto con questo criterio.

Definizione L'insieme delle classi resto modulo *n* si indica con $\mathbf{Z}_n$, cioè $\mathbf{Z}_n = \{ \overline{0} , \overline{1} , \overline{2} , ..., \overline{n-1} \}$

Esempio Possiamo calcolare tutte le classi resto modulo 4:
$\overline{0} = \{....,-16,-12,-8,-4,0,4,8,12,....\}$= interi che divisi per 4 danno resto 0
$\overline{1} = \{..,-11,-7,-3,1,5,9,....\}$ = interi che divisi per 4 danno resto 1
$\overline{2} = \{...,-6,-2,2,6,10,...\}$ = interi che divisi per 4 danno resto 2
$\overline{3} = \{..,-9,-5,-1,3,7,11,....\}$ = interi che divisi per 4 danno resto 3.
TAVOLA 1.2: Esempi di congruenze: tramite esempi, i ragazzi imparano a produrre liste di numeri congruenti modulo un numero fissato *n* e si pongono il problema di come discutere in modo diretto la congruenza la due numeri (e in particolare di determinare il rappresentante tra 0 e *n*-1), confortando i resti della divisione per *n* .

Riprendiamo il cifrario di Cesare. Ricordando l'associazione lettera-numero riportata nella Tabella 1, possiamo dire che usiamo come lettere dell'alfabeto in chiaro i numeri interi compresi tra 0 e 20 e che, per criptare tramite un cifrario di Cesare, lavoriamo modulo 21; ad esempio, usiamo come chiave $k = 71$ (cioè trasliamo di 71 posizioni) e cifriamo la lettera D, che corrisponde al numero 3: per cifrarla, devo calcolare 3+71 = 74. Per capire esattamente la posizione di 74 modulo 21 nel mio orologio con 21 ore, devo determinare il numero *c* compreso tra 0 e 20 che sia congruo a 74 modulo 21. Verifico che $74 = 3 \cdot 21 + 11 \equiv 11 \bmod 21$, e cifro la lettera D con 11.
Come lettere dell'alfabeto (in chiaro e cifrante) non uso più i numeri 0, … , *n–1*, ma le classi da essi rappresentate modulo 21: l'alfabeto numerico dei messaggi unitari (le singole lettere) è quindi rappresentato da $\mathscr{P} = \mathbf{Z}_{21}$.
Poiché nel cifrario di Cesare ogni lettera viene sostituita con la lettera che si trova un certo numero di posizioni più avanti abbiamo che l'insieme delle chiavi è $\mathscr{K} = \{ 0, 1, 2, ..., 20\}$.
Il sistema crittografico per traslazione può essere così schematizzato:
data la chiave *k* in $\mathscr{K}$, la funzione cifrante sarà la seguente:

$$C_k : \mathbf{Z}_{21} \to \mathbf{Z}_{21}$$
$$\overline{m} \mapsto \overline{m+k} \bmod 21,$$

mentre la funzione inversa, quella di decifratura, sarà:

$$D_k : Z_{21} \to Z_{21}$$
$$\overline{c} \mapsto \overline{c-k} \bmod 21.$$

TAVOLA 3 La somma in $\mathbf{Z}_5$ e in $\mathbf{Z}_6$.
TAVOLA 4 Il cifrario di Cesare e le congruenze

CRITTOANALISI

Se intercettiamo un messaggio che sappiamo essere stato criptato col metodo della traslazione per decifrarlo dovremo scoprire quanto vale *k*, cioè la chiave. Talora è possibile decodificare un messaggio pur non conoscendo la chiave *k*.

Nel caso del cifrario di Cesare è possibile pensare di procedere per tentativi. Infatti i cifrari possibili sono 20 nel caso di un testo scritto in lingua italiana (25 se il testo è in inglese). Ma i tempi di decifratura potrebbero essere troppo lenti.
Uno strumento essenziale è l'**analisi del testo**. Poiché nella lingua italiana la maggior parte delle parole termina con una delle vocali *a,e,i,o* vorrà dire che le lettere finali delle parole del messaggio cifrato dovranno essere una di queste lettere. Purtroppo si fa presto ad eludere questa considerazione spezzando il messaggio in blocchi della stessa lunghezza il che rende complicata la ricostruzione delle singole parole. Però si può ricorrere ad altre considerazioni. Se nel testo ci sono lettere consecutive identiche all'interno della stessa parola, queste necessariamente devono essere consonanti. Si hanno poi ulteriori informazioni, fornite dalla cosiddetta analisi delle frequenze. In ogni lingua ci sono lettere che compaiono nei testi con maggiore frequenza ed altre più raramente, ad esempio nella lingua italiana le lettere più frequenti sono nell'ordine *e,a,i* mentre le meno usate sono *q,z*. Altre informazioni si possono reperire dalla frequenza delle doppie, dalla tendenza di certe lettere a non gradire la vicinanza di altre, ecc.
Riportiamo di seguito una tabella riassuntiva delle frequenze nella lingua italiana (in un linguaggio non tecnico e in testi non appositamente costruiti per eludere l'analisi delle frequenze).

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

Supponiamo di intercettare il seguente messaggio:
TRT QRDIAR NTMNFZ N GLPRIN
e di voler scoprire cosa significhi.
Riportiamo la frequenza delle lettere nel nostro messaggio

Lettera	Occorrenze	Lettere	Occorrenze	Lettera	Occorrenze
A	1	H	0	Q	1
B	0	I	2	R	4
C	0	L	1	S	0
D	1	M	1	T	3
E	0	N	4	U	0
F	1	O	0	V	0
G	1	P	1	Z	1

Primo tentativo: inizio dalle lettere terminali di una parola e associando loro le vocali, in ordine di frequenza: **R = e, N = a , T = i, Z = o,**
si ottiene **iei QeDIAe aiMNFZ a GLPeIa**
Rivediamo alcune scelte (la prima parola non ha senso), ponendo ora **T = n**, (è la seconda consonante per frequenza: la prima è L che non sembra adatta), **R = o, Z = e.**
Otteniamo **non QoDIAo anMaFe a GLPoIa**
Ora introduciamo le consonanti più frequenti ancora mancanti (**l**, **r**,**t**,**s,c**) e reintroduciamo la **i**. Proviamo con **I = l**, **A = i**, **D = t**, **F = r, G = s** , **L=c:**

non Qotlio anMare a scPola

Posso modificare ancora **D = g** e continuare...
È chiaro che il modo di procedere è molto falsato perché stiamo facendo l'analisi di un testo troppo breve, ma l'importante è aver sottolineato come le tante possibilità teoriche possano essere notevolmente ridotte usando informazioni sul linguaggio e procedendo sistematicamente per tentativi.

TAVOLA 5: L’analisi delle frequenze