Vi proponiamo alcune attività con i sodici crittografici che dovrebbero aiutarvi a preparare le lezioni del prof. Impedovo. La maggior parte delle attività e delle informazioni che qui di seguito vengono proposte sono tratte da un lavoro progettato e realizzato dal prof. Ferdinando Arzarello in occasione di uno "stage matematico" per studenti di quarta liceo tenutosi nel 2003 a Pragelato, in Piemonte. Leggete attentamente effettuate le attività e rispondete alle domande proposte.

IL CIFRARIO DI CESARE

Cesare usava, principalmente per scopi bellici, vari tipi di cifrari.
Nel "De bello gallico" Giulio Cesare spiega come riuscì a inviare un messaggio a Cicerone, fratello di Marco Tullio, assediato e sul punto di arrendersi. Nel messaggio ai caratteri dell'alfabeto latino erano stati sostituiti quelli dell'alfabeto greco. Giulio Cesare usava la **sostituzione**.

Fu raccomandato al messaggero, se non avesse potuto avvicinarsi, di scagliare un giavellotto col messaggio fissato alla punta oltre la recinzione dell'accampamento Sentendosi in pericolo, il Gallo scagliò il giavellotto come gli era stato ordinato. Per caso esso si conficcò in una torre, e per due giorni nessuno lo notò; il terzo giorno fu scorto da un milite, recuperato e consegnato a Cicerone. Egli lesse il messaggio e, passando in rassegna le truppe, annunciò il suo contenuto con gran gioia di tutti.

Il metodo di cifratura spesso usato da Cesare è illustrato da Svetonio nella "Vita dei Cesari", un'opera del II secolo d.C.. Non è per farvi uno scherzo di cattivo gusto che vi proponiamo il testo in latino

> "*Exstant et [epistolae] ad Ciceronem, item ad familiares de rebus, in quibus, si qua occultius preferenza erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro a et perinde reliquas commutet*"

La sostituzione veniva fatta per traslazione di un certo numero di posti. Per esempio ad 'a' veniva sostituito 'd', a 'b' 'e', e così via secondo questo schema in cui l'alfabeto del testo originario è scritto con lettere minuscole, mentre quello del messaggio cifrato con lettere maiuscole.

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

Testo chiaro **v e n i v i d i v i c i**

Testo cifrato **BHQN BNGN BNFN**

Puoi compiere una traslazione di un posto o di due o di tre.. In tutto quante possibili chiavi per cifrare un messaggio ci sono se si usa un alfabeto di ventuno lettere?

E se ne usiamo uno di ventisei lettere?

Quindi, se dobbiamo decifrare un messaggio scritto usando questa cifratura, qual è la probabilità di interpretarlo al primo tentativo? Qual è il numero massimo di prove?

Leon Battista Alberti, architetto e filosofo; impersonò la cultura universale del Rinascimento italiano.

Per aiutarti ad utilizzare il cifrario di Cesare ti è stata data una "macchina per cifrare" costituita da una coppia di dischi concentrici che devi ritagliare e sovrapporre bloccandoli con un fermacampioni; fai così corrispondere due alfabeti sia nella fase di cifratura che di decifratura o di decrittazione; tale "macchina" fu inventata dall'architetto italiano Leon Battista Alberti nel XV secolo.

Un esempio moderno che usa proprio i dischi dell'Alberti è quello rappresentato qui sotto

Disco cifrante dell'esercito confederato, usato nella Guerra civile americana

Da un punto di vista matematico quello che viene fatto quando si usa un cifrario additivo è calcolare

(numero lettera iniziale + numero della traslazione) **modulo** *26* (alfabeto di 26 lettere)

Infatti se, ad esempio, traslo ogni lettera di 17, per la lettera "**p**" rappresentata dal numero 16 otterrò la lettera (16+17) mod 26 = 7 cioè la lettera **G**

Abbiamo visto che esiste un cifrario additivo; ne esiste uno moltiplicativo?
Se cifro la lettera A con un cifrario moltiplicativo di passo 3 che lettera ottengo ?
E se cifro la lettera B ? E la lettera C?

Cifra la parola "Pragelato" usando un cifrario moltiplicativo di passo 3

Per cifrare con un cifrario moltiplicativo, si può usare qualsiasi "passo" ?
Quali inconvenienti possono accadere ?

Sareste in grado di trovare una regola che vi permetta di distinguere tra sistemi moltiplicativi "buoni" e sistemi moltiplicativi "poco interessanti" ?

Combinando il sistema additivo con quello moltiplicativo quanti cifrari diversi si possono ottenere ?

Di solito si indica con [a,b] un sistema additivo-moltiplicativo in cui si indica con *a* il numero da aggiungere e con *b* il numero per cui si moltiplica.
Se si procedesse moltiplicando dapprima per *b* e poi addizionando *a* si otterrebbe lo stesso sistema di cifratura?
Perché ?
Prova a cifrare con [6,5] la parola **FERMAT,** usando dapprima il numero somma 6 e poi il moltiplicatore 5. Che parola ottieni ?
Ripeti la cifratura applicando dapprima il moltiplicatore 5 e poi il numero somma 6. La parola cifrata è identica alla precedente ?

Decifra ora la seguente parola:

- **SHABRAB** sapendo che è stato usato un cifrario [s,5] e che il testo in chiaro è un nome italiano

Decifra autore e titolo cifrati con il cifrario di Cesare:

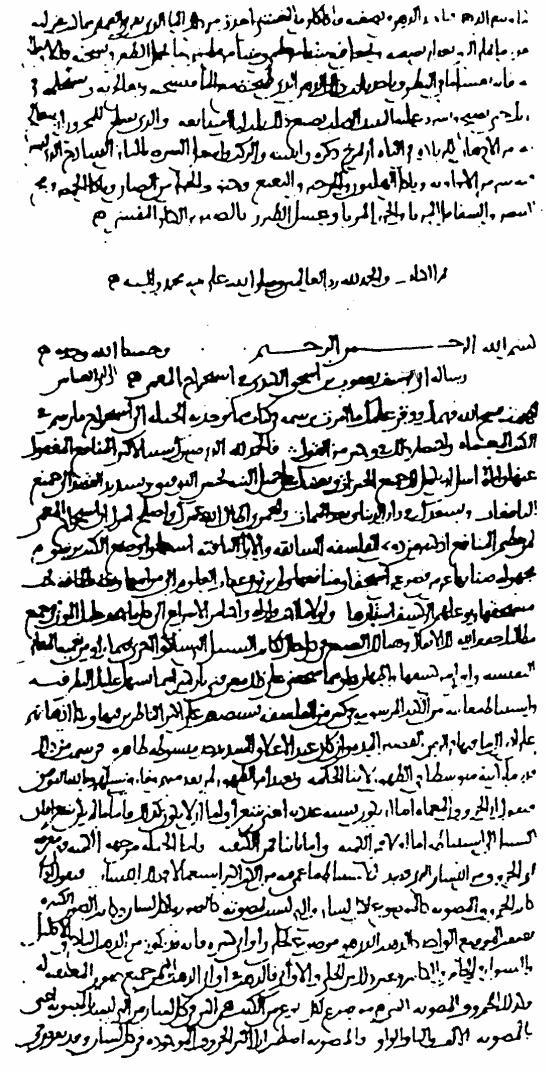
Q	**A**	**H**	**B**	**L**	**W**	**N**	**U**	**H**

M	**P**	**W**	**M**	**W**	**X**	**I**	**Q**	**E**	**T**	**I**	**V**	**M**	**S**	**H**	**M**	**G**
S	**H**	**E**	**P**	**V**	**E**	**G**	**G**	**S**	**R**	**X**	**S**	**G**	**V**	**S**	**Q**	**S**

CIFRARIO MONOALFABETICO CASUALE

Il messaggio che ti è stato consegnato è stato cifrato assegnando ad ogni lettera un'altra lettera in modo del tutto casuale.
Secondo te quante sono le possibili chiavi disponibili?

Alla prima lettera posso far corrispondere una tra 25 lettere (sarebbe poco astuto sostituire una lettera con la lettera stessa). Alla seconda posso far corrispondere una tra le 24 lettere. Alla terza una tra le ……..



25 * 24 * …*….*…. = ..

Cosa hai ottenuto? Pensi che un messaggio cifrato con questo metodo monoalfabetico casuale sia inattaccabile?
Prova a calcolare qual è la probabilità di riuscire a decrittare un messaggio cifrato con una sostituzione monoalfabetica casuale al primo tentativo.

Eppure fin dal IX secolo *il filosofo degli arabi* Abu Yusuf ibn Ishaq al-Kindi scrisse una opera, *Sulla decifrazione dei messaggi segreti* , descrive il procedimento crittoanalitico che ha permesso di decifrare messaggi cifrati con questo metodo. Non è stato questo il libro che ha aiutato i crittologhi dei

secoli successivi, in quanto il libro di al-Kindi è stato ritrovato solo nel 1987.

Non preoccupatevi non è un messaggio cifrato ma solo la
Prima pagina del manoscritto di al-Kindi

Fortunatamente ecco una traduzione di quanto al-Kindi ha scritto nei due paragrafi sull'analisi della frequenza:

Un modo di svelare un messaggio crittato, se conosciamo la lingua dell'originale, consiste nel trovare un diverso testo chiaro nella stessa lingua, abbastanza lungo da poter calcolare la frequenza di ciascuna lettera.
Chiamiamo prima quella che compare più spesso, seconda quella che la segue per frequenza, terza la successiva, e così via, fino a esaurire tutte le lettere del campione di testo chiaro.
Esaminiamo poi il testo in cifra che vogliamo interpretare, ordinando in base alla frequenza anche i suoi simboli. Troviamo il simbolo più comune, e rimpiazziamolo con la prima lettera dell'esempio chiaro; il simbolo che lo segue per frequenza sia rimpiazzato dalla seconda lettera, e così via, fino ad aver preso in considerazione tutti i simboli del crittogramma che intendevamo svelare.

Un altra considerazione che aiuta nell'interpretazione di un messaggio sono l'osservazione che le doppie sono molto probabilmente consonanti. Può capitare che due vocali uguali siano consecutive? Quando? Il fatto che *h* si trova solo dopo *c* o *g* , quando è seguita da *i* o da *e*, oppure prima di *o* e *a* , e che *q* è sempre seguita da *u* , unito alla considerazione che sia *h* che *q* sono tra le lettere più rare può aiutare molto chi si appresta a decrittare un messaggio.
A volte l'alfabeto cifrante non viene generato da una disposizione del tutto casuale delle 26 lettere dell'alfabeto, perché ciò costringerebbe il mittente e il destinatario a conservare questo alfabeto cifrante che rischierebbe di cadere in mano dei nemici. Viene usata una parola facile da ricordare, Julius Caesar, le cui lettere vengono scritte all'inizio, senza ripetizioni, e poi di seguito tutte le altre a partire da quella che segue l'ultima. Così, per esempio, SE LA CHIAVE è Julius Caesar, :

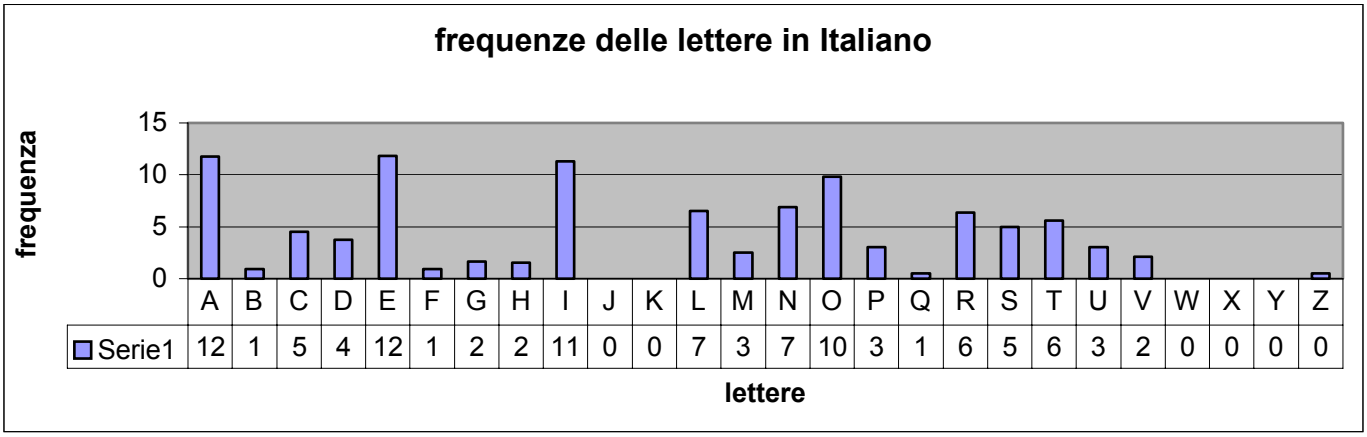
alfabeto chiaro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrante	J	U	L	I	S	C	A	E	R	T	V	W	X	Y	Z	B	D	F	G	H	K	M	N	O	P	Q

Le frequenze delle lettere variano da una lingua all'altra; le informazioni principali sono contenute nella seguente tabella

FREQUENZE POSTE IN ORDINE DECRESCENTE

ITALIANO		FRANCESE	INGLESE	SPAGNOLO	TEDESCO
E	11,79	E	E	E	E
A	11,74	N	T	A	N
I	11,28	A	A	O	R
O	9,83	S	O	S	I
N	6,88	R	I	R	S
L	6,51	I	N	I	T
R	6,37	U	S	N	U
T	5,62	T	R	L	D
S	4,98	O	H	D	A
C	4,50	L	L	C	H
D	3,73	D	D	T	G
P	3,05	C	C	U	L
U	3,01	M	U	P	O
M	2,51	P	M	M	C
V	2,10	V	F	Y	M
G	1,64	F	P	Q	B
H	1,54	B	G	G	Z
F	0,95	G	W	V	F
B	0,92	X	Y	H	W
Q	0,51	H	B	F	K
Z	0,49	Q	V	B	V
J	0	Y	K	J	P
K	0	Z	X	Z	J
W	0	J	J	K	Q
X	0	K	Q	W	X
Y	0	W	Z	X	Y

Nell'istogramma qui sotto è ricapitolata la frequenza delle lettere nella lingua italiana



Noterai delle differenze fra la frequenza delle lettere data per la lingua italiana nella tabella e quelle da te calcolate. Secondo te a cosa possono essere dovute ?

Ci possono essere altre ragioni che modificano la frequenza delle lettere ?

Qualche ulteriore esercizio e un'altra idea per cifrare

Sia dato un messaggio in lingua italiana.
(Considerare l'alfabeto di 26 lettere:ABCDEFEGHIJKLMNOPQRSTUVWXYZ).
Utilizziamo un codice che è formato da un alfabeto di 26 numeri appartenenti a $\mathbf{Z}_{26}$ facendo corrispondere alla lettera A il numero 1, alla lettera B il numero 2 e così via, fino alla lettera z cui corrisponde 0. Le parole codificate saranno quindi numeri (un numero per ogni lettera del messaggio originale) separati da una virgola.
I seguenti esercizi sono stati assegnati quale lavoro di gruppo in aula di informatica, con l'ausilio di Derive, in una prima liceo classico composta da studenti fortemente demotivati all'attività matematica e con gravissimi problemi di preparazione (a.s. 1994-1995).

1. Esercizio (codice 1)
Dato il messaggio HOYCAPITO, codificarlo nel codice scelto (la lettera Y indica uno spazio di separazione).E' importante utilizzare una lettera per indicare lo spazio fra due parole? Perché? Questo codice è facile da scoprire? Perché?

2. Esercizio (codice 1)
Scegliete un elemento invertibile di $\mathbf{Z}_{26}$ (quali sono gli elementi invertibili di $\mathbf{Z}_{26}$? Perché?) e moltiplicatelo per tutti gli elementi del vettore con cui avete codificato il messaggio precedente; scrivete il vettore così ottenuto utilizzando i rappresentanti di $\mathbf{Z}_{26}$ sopra individuati. Come dovrà operare chi riceverà il messaggio codificato, conoscendo la chiave, a decodificarlo?
E' facile scoprire questo codice? Perché?

Esercizio 3 (codice 2)
Trasformare la successione di numeri
8,15,24,3,1,16,9,20,16
nella seguente successione di coppie:
[8,15],[24,3],[1,16],[9,20],[16,25]
Che funzione ha l'ultimo elemento dell'ultima coppia?
Moltiplicare ogni coppia ottenuta precedentemente per una matrice invertibile 2x2 a elementi in $\mathbf{Z}_{26}$(quali sono le matrici invertibili?) per esempio A= $\begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix}$.Decodificare il messaggio così ottenuto.
Ritenete che questo codice sia più sicuro del codice 1? Perché?

Esercizio 4 (codice 3)
Inventate un codice più sicuro utilizzando matrici 3x3.

Esercizio 5 (codici variabili)
Inventare un codice 2 più sicuro, utilizzando matrici invertibili 2x2 i cui elementi siano variabili, ma il cui determinante sia costante, per esempio una matrice che contenga un parametro *t* (che non ne modifichi il determinante) che vari al variare del vettore per cui la matrice si moltiplica.
Risposte ad alcuni degli esercizi proposti nella scheda 7

1. Esercizio (codice 1)

Lo spazio consente maggiore leggibilità; il codice è facile da scoprire perché è sufficiente conoscere il numero corrispondente a una lettera e si individua tutto il codice.
MESS1:=[8,15,25,3,1,6,9,20,15]

2. Esercizio (codice 1)
Basta moltiplicare per l'inverso di 5. Il codice è facile come l'altro: anche in tal caso lettere e numeri si corrispondono sempre nello stesso modo. Se quindi si inviano messaggi di una certa lunghezza, conoscendo la frequenza delle lettere in testi di una data lingua, è possibile ricostruire il testo con una certa facilità. Si tratta di un problema standard nelle settimane enigmistiche.
CIFRA1:=MOD(5*MESS1,26)
ELEMENTI:=VECTOR(k,k,0,15)
INVERSO(n):=MOD(n*ELEMENTI,26)
MESSAGGIO1:=MOD(21*CIFRA1,26) (e si riottiene quello di partenza)

Esercizio 3 (codice 2)
MESS2:=[[8,15],[24,3],[1,16],[9,20],[16,25]]
m:=[[2,1],[1,2]]
CIFRA2:=MOD(MESS2*m,26)
INVERSO(3)
m^{-1}
INVERSOm:=MOD(9*m^{-1},26)
MESSAGGIO2:=MOD(CIFRA2*INVERSOm,26) e si riottiene il messaggio di partenza
Per calcolare l'inversa di una matrice A=[[a,b],[c,d]] *invertibile:*
a) controllare la condizione necessaria e sufficiente di invertibilità: ad-bc$\neq 0$
b) determinare l'inverso di E= *ad-bc nell'anello in cui ci si trova*
c) scrivere la matrice inversa A^{-1} = [[*d*E,-*b*E],[-*c*E,*a*E]], *riducendo i termini al modulo in cui ci trova*.
Il codice 2 è più sicuro del codice 1, in quanto solo le coppie di lettere hanno la stessa codifica (e in più solo se iniziano entrambe a un posto dispari), mentre può accadere che a una A corrisponda, nello stesso messaggio, una volta una lettera e una volta un'altra. In tal caso una semplice informazione sulla frequenza delle lettere in una certa lingua non garantisce la certezza di infrangere il codice.

Esercizio 5 (codici variabili)
Si può usare, in $\mathbf{Z}_{26}$ *la matrice A* =[[5,-3+*t*],[15,2+3*t*]]=[[5,23+*t*],[15,2+23*t*]]
assegnando a t *il valore* 0 *e il valore* 1 *rispettivamente nella prima e nella seconda riga, in modo che quando si moltiplichi per il primo o per il secondo vettore colonna del messaggio di partenza, si abbiano decodificazioni differenti dei due vettori.*

Potete sistemare quanto ora presentato collegandovi al sito web:
http://alpha01.dm.unito.it/personalpages/cerruti/cp0/crittoprimistart.html
Un altro sito in cui vengono trattati temi relativi alla crittografia, ma di lettura, a mio avviso, meno semplice è:
http://www.tonycrypt.com/

Chi volesse anticipare alcuni temi che verranno trattati dal prof. Impedovo può collegarsi al sito:
http://alpha01.dm.unito.it/personalpages/cerruti/cp0/crittoprimistart.html

Per approfondimenti autonomi si rinvia all'ottimo lavoro del Liceo Foscarini:
http://www.liceofoscarini.it/studenti/crittografia/index.html