Sai mandare un segreto?

Liceo Scientifico Galileo Ferraris – Varese

Classe: 3°D

Insegnante di riferimento: Roberta Bossi

Ricercatore: Giulia Bernardi

Ragazzi partecipanti: Davide Aresu, Angelo Baj, Silvia Biglietto, Edoardo Brisca, Jennifer Carcinale, Lorenzo Cassani, Franz Costantini, Federico Di Cesare, Sara Di Martino, Francesca Dini, Jordi Fabris, Giordano Folla, Alessandra Goggi, Alessandro Nathan, Alessandra Ponti, Micol Pullano, Edoardo Realini, Andrea Santoro, Alessio Stocco, Marta Ton, Marco Vandone, Lucrezia Vecchiato, Martina Zanotti

Fin dall'inizio la sfida di risolvere un problema che avrebbe potuto non avere soluzioni ha suscitato in noi curiosità che ci ha portato ad impegnarci a fondo e ci ha entusiasmato l'idea di un problema che potesse durare molti mesi. Così ci siamo posti varie domande su quale potesse essere l'argomento di questo problema, e quando Giulia, la nostra referente, ce lo ha esposto ne siamo rimasti subito colpiti e molto interessati. Eccolo qui sotto

Mio fratello è molto curioso e spesso riesce a impossessarsi del mio cellulare e a curiosare leggendo i miei messaggi. Purtroppo il mio telefono non ha dei sistemi di sicurezza per impedirlo. Che cosa possiamo fare allora io e le mie amiche per scriverci dei messaggi in modo che mio fratello non li capisca, anche se riuscisse a leggerli? Voi sapreste aiutarmi?
E se invece voleste aiutare mio fratello a leggere anche i miei messaggi protetti, che cosa gli consiglereste di fare?

Si comincia discutendo preliminarmente con Giulia mettendo in luce alcuni punti importanti che elenchiamo.

- Chiamiamo codice il sistema comunicativo concordato per non farsi capire dagli altri, il codice deve essere facilmente utilizzabile in modo da ridurre i tempi di scrittura e lettura da parte di chi lo usa per comunicare.
- Ci è parsa una buona idea usare lo stesso metodo ma con chiave diversa per ridurre il rischio che, intuendo il metodo, si ricavi la chiave. Intendiamo per chiave il mezzo grazie al quale è possibile decifrare il codice.
- Ci è parso necessario che gli interlocutori si accordino sulla chiave da utilizzare, ma solo la prima volta mentre le successive devono potrela ricavare dal metodo deciso.

All'interno della classe sono nate diverse idee a proposito della parola chiave, in particolare utilizzando:

- la data di scrittura del messaggio;
- un'equazione;
- una tabella lettere-numeri come cifrario.

Per quanto riguarda il modo con cui accordarsi sul metodo abbiamo pensato che si potrebbe inviare una lettera e poi bruciarla.

Di seguito elenchiamo le idee sviluppate in quattro gruppi di lavoro durante vari incontri.

GRUPPO ABCCA
Il nostro codice consiste nell'usare l'equazione $y = x(x+1)$ dove il valore della *x* è determinato dalla data di scrittura del messaggio. La somma delle cifre del risultato dell'equazione è il numero della lettera da far corrispondere alla 'A' nell'alfabeto in chiaro.

Esempio:
Data 03/04/2014
Equazione y=3(3+1) y=12 → 1+2 → y=3

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

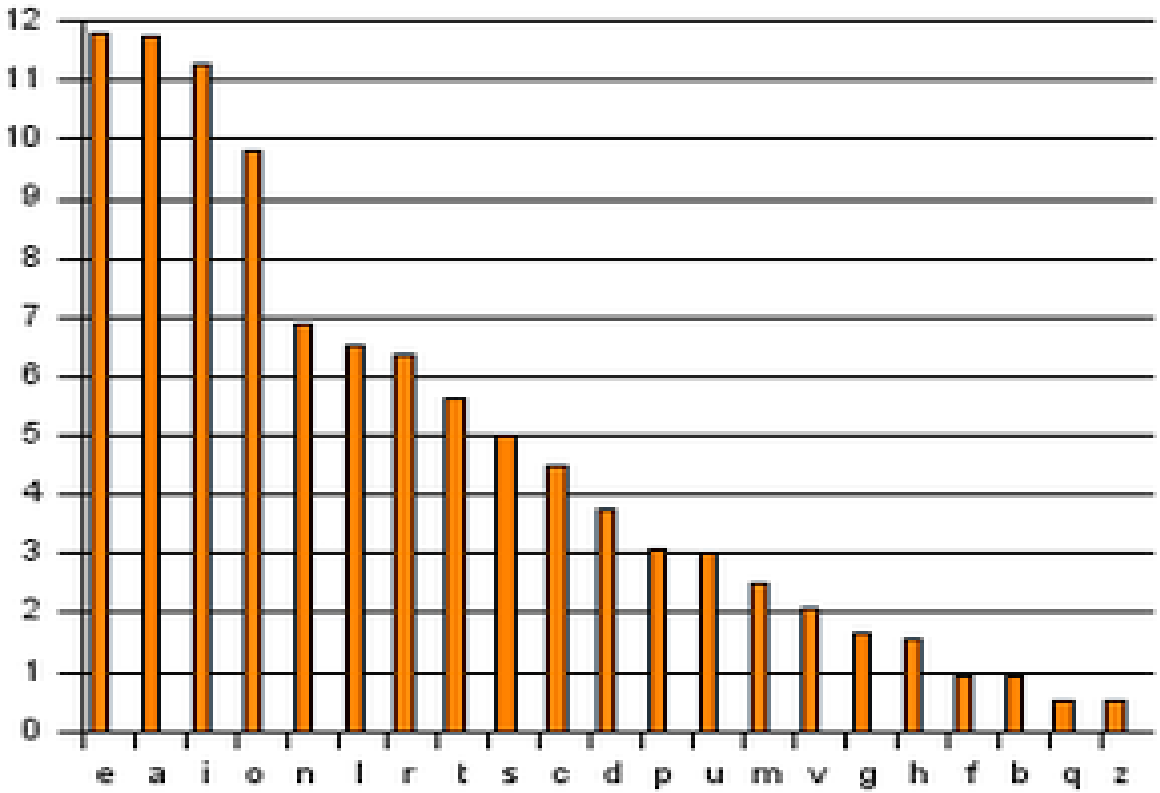
Esempio: CODICE = AMBGAC

Questo codice ha un punto debole. Infatti, per quanto possa essere complicato l'algoritmo, una volta individuata una corrispondenza tra una lettera cifrata e una in chiaro, è sufficiente proseguire l'alfabeto da entrambe le lettere per trovare tutte le sostituzioni.
Pertanto abbiamo deciso di non sviluppare la nostra idea e ci siamo concentrarti sul perfezionamento delle idee degli altri gruppi.
Durante l'ultimo incontro con Giulia abbiamo compreso che quello da noi proposto è un cifrario monoalfabetico (noto come cifrario di Cesare), che è la tipologia di cifrario più semplice da decifrare e ci siamo resi conto che le nostre aspettative erano state parzialmente deluse perché ci aspettavamo una richiesta più attinente alla matematica.

GRUPPO SGSGS
La nostra idea consiste in una tabella in codice binario, che riportiamo di seguito:

--------			DATA				DATA			
-------	E	A	---------	I	O	N	---------	L	R	T
DATA										
DATA										

Metodo di compilazione della tabella:
Abbiamo inserito nella terza e nella settima casella della PRIMA RIGA la chiave di lettura del codice, coincidente con il giorno di invio del messaggio cifrato; i numeri che non appartengono alla data sono poi stati disposti in ordine dopo la settima casella. Abbiamo ideato questa chiave di lettura in modo da rendere il codice, che cambia quotidianamente, più difficile da decifrare senza l'utilizzo della tabella. Tenendo poi conto della PRIMA COLONNA, si lasciano libere le prime due caselle ad essa appartenenti, riempiendo poi le successive due con le cifre del giorno di invio del messaggio.



Nell'immagine sovrastante (fonte Wikipedia) sono riportate le frequenze di utilizzo delle lettere dell'alfabeto italiano all'interno dei testi scritti; abbiamo inserito le sette più utilizzate nella SECONDA RIGA della tabella, saltando le caselle sottostanti la data. Le altre lettere sono poi state disposte in ordine casuale nelle DUE RIGHE FINALI, senza escludere le caselle sottostante la data.
Notando la presenza di due spazi vuoti, abbiamo deciso di riempirli con virgola e punto. Poniamo ad esempio che oggi sia il 2 aprile, la tabella in questo caso sarà:

-	5	6	**0**	7	8	9	**2**	1	3	4
-	E	A	-	I	O	N	-	L	R	T
0	F	H	Z	Q	L	Y	J	K	M	B
2	C	P	U	W	X	S	G	V	,	.

Metodo di applicazione:
Per quanto riguarda le lettere presenti nella prima riga, esse sono codificate dal numero della colonna cui appartengono. Ad esempio la 'E' viene scritta nel messaggio con il numero 5. Le lettere delle successive righe vengono criptate con due numeri: il numero della riga cui appartengono seguito dal numero della colonna. Ad esempio la 'F' viene scritta nel messaggio con il numero 05. Sottolineiamo nuovamente che i numeri associati alle lettere cambiano al variare della data.
Prova ora a decifrare il seguente messaggio utilizzando la tabella sovrastante: 2576825803529467? Ci sei riuscito? La risposta si trova poco più avanti (*).

Problemi:
Per quanto riguarda i giorni 11 e 22, la cui cifra costitutiva si ripete due volte, abbiamo avuto dei problemi perché ad uno stesso numero corrispondevano due diverse lettere; ciò rendeva impossibile la decriptazione del messaggio. Per risolvere questo problema abbiamo deciso che il giorno 11 sarebbe stato sostituito con il numero 32, giorno non riscontrabile in altra parte del mese. Analogamente il giorno 22 corrisponde al numero 34.

(*) Soluzione del messaggio da decifrare: ciao come stai?

GRUPPO NDRVZ

L'idea

Il sistema ideato dal nostro gruppo sostituisce a una singola lettera un valore numerico, individuabile tramite una particolare tabella 11x4. La chiave sta nella data di scrittura del messaggio.

Se, ad esempio, oggi è il 2 di Aprile la data sarà identificata come 02. Le cifre 0 e 2 prendono posto nella prima riga, al centro. Nel caso la data sia composta da un numero doppio (11, 22), le cifre chiave saranno 3 e 2 (32 data impossibile).

	1	3	4	5	**0**	**2**	6	7	8	9
	e	a	i	o			n	l	r	t
0	b	c	d	f	g	h	j	k	m	p
2	q	s	u	v	w	x	y	z		

Nella prima riga prendono posto tutte le cifre, le cifre-chiave vanno al centro, poi a partire dal primo posto a sinistra, si inseriscono le rimanenti in ordine, saltando le cifre già usate.

Nella seconda riga si inseriscono le lettere più frequenti in italiano, a seguire, nelle righe successive ci sono le lettere rimanenti, in ordine alfabetico.

Per sostituire una lettera con l'equivalente cifrato, basta giocare a battaglia navale.

Se la lettera da cifrare è posizionata nella seconda riga, basta usare il numero sopra di essa. Se la lettera sta nella terza o quarta riga, al numero della colonna si antepone quello della riga.

Esempi

a = 3, f = 05, g = 00, y = 26, w = 20.

Come si legge

Si parte da sinistra: se si incontra una cifra-chiave, si considerano quella cifra e quella immediatamente successiva, se invece la prima cifra è una generica, si considera quella da sola.

Esempio pratico

Prendiamo il primo verso del terzo canto dell'Inferno di Dante:
“Per me si va nella città dolente”
si traduce in
0918 081 234 253 61773 034993 04571691

GRUPPO VBBFS

Il primo codice che abbiamo creato era una cifratura per sostituzione mono-alfabetica cioè contraddistinta dalla sostituzione di un numero ad ogni lettera dell'alfabeto. Tale sostituzione derivava dall'utilizzo della data e dunque variava con essa ogni giorno.

A questo primo codice sono state mosse subito due critiche:

- i numeri che sostituiscono le lettere dovevano essere scritti tramite spazi, poiché non erano distinguibili i numeri con una cifra da quelli con due;
- il sistema di numerazione con cui effettuavamo la sostituzione mono-alfabetica era sequenziale e quindi semplice da individuare e comprendere. Infatti era sufficiente trovare una singola lettera nel testo per decodificare tutto il messaggio.

Modifiche e codice finale

Queste critiche ci hanno portato a compiere delle modifiche grazie alle quali abbiamo dato origine a questo nuovo codice:

- è ancora una sostituzione mono-alfabetica;
- il numero dei caratteri del nostro codice coincide con il numero di giorni che

contraddistingue il mese della data:

- poiché il numero delle lettere dell'alfabeto è minore dei giorni del mese abbiamo aggiunto dopo la 'z' una serie di spazi fino ad arrivare al numero di giorni predefinito;
- in base al numero del giorno abbiamo deciso di iniziare a numerare dalla lettera a cui corrispondeva tale numero;
- abbiamo proseguito la numerazione saltando sempre una lettera (abbiamo così risolto il problema della sequenzialità del codice);
- una volta esaurita la numerazione ne applichiamo una seconda in modo tale da aumentare la variabilità del codice;
- ora ad ogni lettera corrispondono due numeri (abbiamo così risolto il problema del 'non': si veda più avanti nelle Conclusioni con Giulia (**)).

Esempio:
Data 10/04/13

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	_	_	_	_
12	27	13	28	14	29	15	30	16	01	17	02	18	03	19	04	20	05	21	06	22	07	23	08	24	09	25	10	26	11
42	57	43	58	44	59	45	60	46	31	47	32	48	33	49	34	50	35	51	36	52	37	53	38	54	39	55	40	56	41

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
1	2	3	4	5	6	7	8	9	0	.	:	;	“	,	?	!	(	)	*	@	+	-	/	%

Di conseguenza la frase MATH_AND_JEANS si trascrive:
184236301012032811014442335 1.
In questo modo, se in una frase di 14 lettere non ci fossero lettere ripetute, avremmo 2^14=16384 modi diversi per scriverla.

CONCLUSIONI CON GIULIA
Durante l'ultimo intervento di Giulia abbiamo capito che ci sono diversi tipi di crittogramma, i più semplici da decifrare sono quelli per sostituzione monoalfabetica ossia quelli che associano ad ogni lettera un’altra lettera.
In questo caso le lettere nascoste sono facili da individuare attraverso le parole monosillabiche come “non”, dove compaiono due lettere consecutive (**).
Da questo abbiamo potuto notare che i nostri primi codici erano facilmente decifrabili perché seguivano tutti questo tipo di cifrario.
Abbiamo per questo cercato di complicare i nostri codici seguendo il secondo metodo che Giulia ci ha proposto, il crittogramma di Babbage, secondo il quale ad ogni lettera corrisponde una coppia di altre lettere ed è più difficile da decrittare: per farlo bisogna infatti trovare stringhe di caratteri che si ripetono.

LE CONCLUSIONI DEI VARI GRUPPI DI LAVORO:
Inizialmente eravamo molto dubbiosi in merito al problema: ci aspettavamo, infatti, che fosse più complesso e che richiedesse più conoscenze scolastiche, come l'utilizzo di leggi o teoremi.

Alcuni di noi fin da piccoli hanno cercato di occultare i messaggi con dei fantasiosi metodi per nasconderne il contenuto a genitori o amici. Inoltre ci ha incuriosito il fatto che questo problema ce lo avesse posto un'università di alto calibro e quindi ci siamo messi in gioco e ci siamo confrontati volentieri con le altre classi.

L’esperienza complessivamente è stata interessante oltre che istruttiva, ci ha permesso di

capire un’applicazione moderna della matematica e, soprattutto nell’ultimo incontro abbiamo potuto capire, con lo stupore di tutta la classe, che ciascuno dei nostri sistemi di crittazione (creato nell’arco di circa cinque mesi) si decritta facilmente in una decina di minuti se non in minor di tempo con l’ausilio di un computer.
Abbiamo anche scoperto, dopo una breve spiegazione della storia della crittografia, che esistono sistemi di crittazione molto più complicati e difficili da capire rispetto al modello base creato da noi in classe.

Ci interessava poter lavorare in gruppo e ci è piaciuto il problema posto. Essendo inoltre un argomento che negli ultimi anni ha preso sempre più piede nella nostra società, è infatti usato molto dai governi, è stato interessante capire le varie metodologie possibili per risolvere il nostro problema. Abbiamo potuto esprimere le nostre idee, discuterne insieme e divertirci a sperimentarne sempre di nuove.

Abbiamo speso molte ore di lezione (alcune anche dopo l'orario scolastico) per questo progetto, ma ne siamo stati ripagati appieno. Le lezioni sono state piuttosto interessanti e l’aiuto di Giulia è stato essenziale per capire meglio le varie debolezze e i punti di forza di ciascun sistema.

Fin da subito abbiamo aderito a questo progetto con entusiasmo e voglia di mettere in gioco la nostra logica. Abbiamo infatti lavorato duramente ma anche con piacere poiché questa iniziativa ci ha permesso di collaborare tra di noi per creare un nostro codice.