I CODICI CRITTOGRAFICI

Progetto alunni classe IV B scuola elementare di Finalmarina – studenti del Liceo Scientifico " Issel " di Finale Ligure.

ITINERARIO DI LAVORO

Le insegnanti hanno iniziato le attività relative al Progetto, chiedendo agli alunni di esporre i loro pareri e/o pensieri circa la crittografia e di conseguenza i codici crittografici.
Di seguito si enunciano le risposte date dagli alunni:

- è un codice segreto
  - che si usa ad es. per aprire una cassaforte (Gabriele)
  - che serve per decifrare alcune parole nascoste o per aprire un file (Edoardo V.)
  - che serve per aprire file nascosti, cose segrete (Edoardo T.)
  - dei PC per inviare e ricevere messaggi segreti via PC (Luca)

- è un tipo di scrittura
  - usata per scrivere messaggi segreti (Daria)

- è una scrittura segreta
  - per comunicare con altre persone in segreto (Matteo)
  - per mandare un messaggio ad un'altra persona e solo lei riesce a decifrarlo (Giada)

- è un tipo di scrittura particolare-elaborata
  - per comunicare segreti (Giulia)
  - che si usa per aprire file segreti che non devono essere visti da altre persone (Edoardo B.)
  - che ha un codice e serve per aprire cartelle con messaggi (Davide)
  - molto strano – una volta scoperto aiuta a trovare tesori (Sebastiano)
  - che permette di leggere codici segreti e forse anche di comunicare con un essere non terrestre (Marika)

- è un tipo di disegno
  - riprodotto sul PC in modo segreto per comunicare (Elisa)

- è una scrittura meccanica
  - che si usa sul PC e che conoscono solo poche persone (Beatrice)

- è una password
  - per aprire file e anche per disattivare virus (Alberto)

- è una scrittura virtuale
  - che può fare solo il PC. Noi possiamo controllare, ma non scrivere perché troppo difficile. Può essere usata da persone importanti per scambiarsi informazioni segrete sul nostro pianeta (Leonardo)
  - può essere una specie di cruciverba (Salvatore)

- è un programma virtuale
  - si usa per messaggi segreti (Maria Chiara)

- tipo di scrittura inventata da Einstein
  - serve agli agenti segreti per comunicare (Martina)

- è un argomento di fantascienza
  - inventato dagli alieni per comunicare con uomini prescelti (Francesco)

Durante la discussione viene chiesto da alcuni alunni il significato della parola "crittografia", quando nasce e il motivo per il quale è nata.
Altri alunni hanno provato a rispondere…….

A questo punto, le insegnanti sono intervenute, (è stato ricercato il significato della parola "crittografia" sul vocabolario) poi hanno illustrato, per sommi capi, la disciplina ed i suoi campi di applicazione nella realtà di oggi.
Per alcune di queste applicazioni (soprattutto per quelle via internet) si è notato che gli alunni dimostravano una certa comprensione, altre risultavano invece troppo lontane dalla loro realtà quotidiana esperienziale e quindi non comprese appieno.
Avendo posto gli alunni stessi le domande circa la nascita della crittografia e dei suoi scopi nel passato, si è svolta una breve ricerca di notizie riguardante questo aspetto.
Si è discusso in modo più approfondito del cifrario di Cesare, della sua utilità nel passato e della storia della macchina Enigma.
A questo proposito ci siamo documentati sui seguenti link:
www.liceofoscarini.it (per la crittografia ed il cifrario di Cesare)
www.museoscienze.org/cimeli (per la macchina Enigma)
L'interesse degli alunni si è rivolto soprattutto alla macchina Enigma e molte sono state le domande poste circa il suo utilizzo e l'invenzione di altre macchine.
Abbiamo, quindi, richiesto la collaborazione (al liceo) per trovare notizie su eventuali altre "macchine" inventate.

Con le indicazioni del Prof. Paola abbiamo così ricavato altre notizie sul sito www.siforge.org dove ci siamo documentati (anche se sommariamente) sullo scitale e da chi veniva usato.
Altre documentazioni sono state esperite al link www.matematicamente.it/storia/crittografia .

Aspetti concettuali del sistema crittografico

Abbiamo evidenziato con gli alunni le seguenti componenti.

M- messaggio in chiaro
C- testo cifrato
R- chiave per poter cifrare e decifrare il messaggio

Per rendere più chiari i concetti abbiamo esemplificato con macchina operatoria, già usata nell' aritmetica e conosciuta dagli alunni; ora utilizzata con questi simboli:

M------ | R | -------C

e viceversa per decodificare.

Durante questo lavoro è emersa la figura della spia.

Gli alunni hanno provato a trovare soluzioni circa il non rendere possibile ad "estranei" la decodifica del messaggio.
La maggior parte ha concordato sulla necessità di cambiare molto spesso le chiavi di cifratura.
È stato per loro molto difficile accettare che la "spia" possa sempre essere al corrente del tipo di sistema crittografico utilizzato (principio di Kerchoffs).
Gli alunni si sono poi impegnati nel risolvere alcuni giochi crittografici e a scrivere e/o decifrare alcuni brevissimi messaggi, sempre in situazione ludica, a sostituzione monoalfabetica.

La classe è stata divisa in tre gruppi:

1° gruppo cifrava il messaggio
2° gruppo lo decodificava conoscendo la chiave
3° gruppo delle "spie" tentava di decifrarlo non conoscendo la sostituzione delle lettere.

Aspetti matematici: Cerchio-cerchi concentrici-rotazione-permutazioni

Le insegnanti hanno poi supportato gli alunni nella costruzione di un cifrario a rotazione.

Leonardo e Matteo ritagliano…

Marika e Beatrice cercano di eseguire le consegne con precisione

Edoardo V. ascolta le spiegazioni delle insegnanti prima di procedere

Marika ha quasi completato il lavoro

Alberto ed Edoardo T. controllano se è stato eseguito bene il loro lavoro.

Matteo sta ritagliando il disco di decodifica.

Gli alunni si sono cimentati in alcune attività di codifica – decodifica (ogni lettera dell'alfabeto veniva sostituita con quella che la seguiva di tre posizioni – cifrario di Cesare). Si è poi fatto notare che con cifrari a rotazione, tipo quello di Cesare, si ha un numero di possibili cifrari (e quindi un numero di possibili chiavi) uguali al numero delle lettere dell'alfabeto (meno 1 se si esclude la rotazione nulla che lascia il messaggio inalterato). Ci si è quindi chiesto quanti possibili cifrari sarebbe possibile costruire se si eliminasse il vincolo della rotazione, ma si fosse liberi di sostituire ciascuna lettera dell'alfabeto con una e una sola altra lettera dello stesso alfabeto.
A questo punto è stato introdotto anche il termine "permutazione" e il suo significato.
Le insegnanti hanno invitato gli alunni a riflettere su quante potessero essere le chiavi per cifrare con questo sistema. Abbiamo provato praticamente iniziando prima con due lettere, poi con tre, poi con quattro.
Gli alunni si sono resi conto delle varie permutazioni ed è stato ben appreso il concetto almeno fino a quattro lettere.
È stato introdotto anche il termine di numero fattoriale e la sua scrittura.
Non si sono effettuati calcoli oltre il 6! , anche perché non tutti gli alunni hanno compreso appieno il meccanismo.
Il numero delle chiavi possibili sul nostro cifrario è stato dato come notizia dalle insegnanti (essendo numeri troppo grandi) e si è evidenziato davvero lo stupore degli alunni per il numero così grande delle permutazioni possibili.
Si è parlato anche dei metodi statistici per decifrare un messaggio di questo tipo, facendo esempi circa le frequenze delle lettere presenti nella nostra lingua.
Queste frequenze possono aiutarci nella decodifica del messaggio.

A questo proposito abbiamo visto la tabella relativa alle frequenze delle lettere nelle varie lingue ed in particolare nella lingua italiana, sulla pagina del sito del progetto nell'area lezioni-codici crittografici (ossia in una particolare sezione della classe virtuale).
Collettivamente è stato poi scritto un messaggio in chiaro ed individualmente gli alunni hanno provato a tradurlo in messaggio cifrato (con un sistema alla Cesare).

Alcuni alunni preparano un messaggio in codice….

…….altri alunni cercano di decifrare il massaggio

Successivamente il messaggio cifrato è stato inviato agli studenti del Liceo.

Considerazioni finali

Gli alunni sono stati molto motivati ed interessati nello svolgere le diverse attività del progetto, anche se hanno evidenziato più volte il desiderio di un contatto visivo e personale con gli studenti del liceo.
Alcuni si sono dimostrati pronti ad apprendere queste nuove cose, implicanti diversi aspetti cognitivi: storici, matematici, linguistici, informatici…
Altri hanno dimostrato di non essere ancora pronti e/o di essere interessati solo ad alcuni aspetti, fermandosi alla "magia" dei messaggi segreti.
È stata un' esperienza positiva, anche se un maggior tempo a disposizione ed una essenziale sincronicità di attività sarebbero stati più auspicabili.
Per le insegnanti l'esperienza positiva ha prodotto stimoli sia nella ricerca che nella preparazione degli argomenti trattati, non ben conosciuti e/o approfonditi in precedenza.

Le insegnanti
Liliana Palomo
Mariateresa Martini
e gli alunni della classe IV B