

– Crittografia di informazioni –

Attività per scoprire alcune semplici caratteristiche

Sommario:

Lo studente svolgendo l'attività scoprirà come è possibile esprimere dell'informazione attraverso l'uso di un codice, potrà osservare quali sono le principali caratteristiche che deve possedere per essere funzionale e quali sono i possibili problemi che si potrebbero verificare se non le possiede.

Competenze richieste:

Per svolgere le attività presentate di seguito non sono richieste competenze particolari.

Vocabolario:

- Codifica: è un processo che permette di rappresentare delle informazioni mediante l'utilizzo di un codice

Età:

- da 9 anni in su

Materiale:

- Fogli di codifica e di lavoro presenti nell'attività
- Carta, matita, penna
- Lavagna e/o proiettore(opzionale)

Competenze acquisite a fine attività:

- ❖ Scegliere ed utilizzare oggetti per rappresentare informazioni familiari semplici (es. colori, parole, ...);
- ❖ Utilizzare combinazioni di simboli per rappresentare informazioni familiari complesse;
- ❖ Riconoscere usi dell'informatica e delle sue tecnologie nella vita comune.

Storia introduttiva:







Davide è un bambino che da sempre ama gli animali e come regalo di compleanno che sarà tra qualche settimana, i genitori gli hanno promesso che adotteranno un animale domestico e potrà essere un cane, un gatto oppure un coniglio, ma questa è una sorpresa.








I genitori hanno affidato a Davide un compito, quello di pensare a qualche nome sia maschile che femminile (ancora non sa il sesso) da dare al loro futuro animale.

Davide è un bambino molto intelligente e da sempre appassionato a giochi di codici segreti decide di inventarsi un codice per l'occasione e sfidare i genitori; dopo aver rovistato tra i suoi giochi trova dei timbri giocattolo con varie figure di cui uno che rappresenta un cane, uno che rappresenta un gatto e uno che rappresenta un coniglio.

Attività – Davide... Cane, gatto o coniglio?

Davide decide di inventarsi per alcune lettere dell'alfabeto una diversa sequenza (codifica) di timbri di cani, gatti e conigli:

Lettera	Sequenza di Cani, Gatti e Conigli
D	
L	
A	
O	
E	
B	

I	
N	
F	
G	
V	
S	
R	

La codifica che ha inventato è univoca perché Davide per ogni lettera ha utilizzato una sequenza differente (sia in lunghezza che di genere); inoltre è stato anche molto ben attento a cercare le sequenze in modo tale da NON creare ambiguità nella traduzione, infatti se osservate ogni sequenza non è un prefisso di alcuna altra sequenza, quindi non ci si può sbagliare.

Esempio per l'insegnante da mostrare agli studenti: se utilizziamo la tabella di codifica fornita da Davide, il suo nome potrebbe venire tradotto (codificato) in modo univoco nel seguente modo:



(D)(A)(V)(I)(D)(E)

Davide, dopo aver pensato a qualche nome ha consegnato ai suoi genitori il foglio contenente la tabella con il codice e quello contenente i nomi codificati (maschile/femminile) da lui pensati per il futuro animale.

Proiettare ora alla classe le sequenze mostrate di seguito e la tabella del codice vista in precedenza, e chiediamo loro: chi è in grado di aiutare i genitori di Davide a scoprire quali sono i nomi da lui scelti che si nascondono dietro a queste sequenze di simboli?

Nomi Maschili:



Nomi Femminili:



3)



Lasciamo agli studenti del tempo per svolgere l'attività, e quando l'intera classe avrà terminato, commentare insieme le soluzioni trovate.

Soluzione:

Nomi Maschili:

Nomi Femminili:

1) **OLAF**

FIONA

2) **BAFFO**

DIANA

3) **DINGO**

NEVE

Anche questa è informatica!

Nell'attività appena svolta, aiutando i genitori di Davide a trovare i nomi per l'animale da adottare, avete avuto modo di vedere come è possibile inventare un codice e utilizzarlo per esprimere dell'informazione.

La codifica di informazioni può essere fatta in diversi modi; il codice inventato da Davide dell'attività precedente è un esempio di quella che in Informatica viene chiamata **codifica a lunghezza variabile** in cui per codificare i caratteri si utilizzano un numero variabile di bit.

Mentre in altre codifiche, (ad esempio nel codice ASCII) viene usata una **codifica a lunghezza fissa**, in quei casi tutti i caratteri vengono codificati utilizzando delle sequenze distinte ma con lo stesso numero di bit.

Abbiamo quindi visto che esistono codifiche a lunghezza variabile e che, come nel caso del Codice inventato da Davide, è normale osservare che alcune lettere siano codificate utilizzando una sequenza più breve e altre una sequenza più lunga.




Nella codifica a lunghezza variabile, quale potrebbe essere una tecnica intelligente per scegliere a quale carattere assegnare una codifica più breve e a quale assegnarne una più lunga? Una tecnica utilizzata è quella di andare a calcolare la frequenza con cui i caratteri vengono utilizzati; e assegnare a quelli utilizzati più frequentemente una codifica più breve, mentre a quelli utilizzati meno frequentemente una codifica più lunga.











Prima di concludere l'attività, è importante però mettere in evidenza alcune caratteristiche fondamentali che sono presenti nel codice inventato da Davide.

Infatti alla base della Crittografia in Informatica si ha che un codice utilizzato per esprimere dell'informazione per essere funzionale, tra le tante caratteristiche che deve possedere, c'è anche il fatto che deve essere **univoco** e **NON ambiguo**.

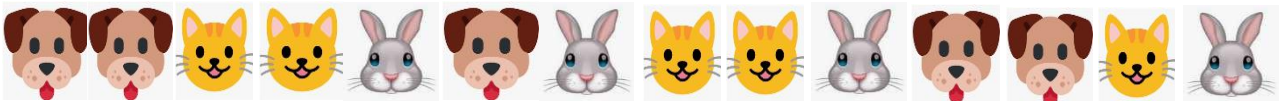
Durante l'attività avete già avuto modo di vedere che il codice inventato da Davide è univoco perché per ogni lettera ha utilizzato una sequenza differente di simboli (sia in lunghezza che di genere); inoltre è stato anche molto ben attento a cercare le sequenze in modo tale da NON creare alcuna ambiguità nella traduzione, infatti se osservate ogni sequenza non è un prefisso di alcuna altra sequenza, quindi è impossibile sbagliarsi; data una sequenza di simboli ci sarà una e una sola possibile traduzione.

Domanda: Perché queste caratteristiche appena viste sono così importanti? Provate a svolgere la stessa attività vista in precedenza utilizzando però questa volta quest'altra tabella di codifica (questa tabella, anche se a prima vista sembra molto simile alla precedente, non lo è affatto perché a differenza di quella utilizzata prima questa presenta un codice ambiguo).

Lettera	Sequenza di Cani, Gatti e Conigli
D	
L	
A	

O	
E	
B	
I	
N	
F	
G	
V	
S	
R	

Quali sono le possibili interpretazioni della seguente sequenza di simboli?



Interpretazione 1:

(D)(D)(O)(L)(D)(L)(O)(L)(D)(D)(?)(L)

Interpretazione 2:

(D)(A)(N)(L)(I)(D)(D)(?)(L)

Interpretazione 3:

(D)(A)(V)(I)(D)(E)

Etc...

In questo caso, dato che ci sono molte possibili interpretazioni della sequenza, senza altre informazioni o suggerimenti, come è possibile capire qual è la corretta traduzione? Purtroppo, non è possibile saperlo.

Da questo esempio è quindi possibile capire che se si vuole esprimere dell'informazione utilizzando/inventando un codice, quest'ultimo per essere funzionale deve necessariamente anche essere **univoco** e **NON ambiguo**.