

Attività1 - Cifrario di Pigpen

- **Materiale:** Peg Code di Quercetti
- **Età:** a partire da 8 anni
- **Competenze acquisite a fine attività:**

Obiettivi di apprendimento al termine della classe terza della scuola primaria:

Ambito dati e informazione:

- O-P3-D-1. scegliere ed utilizzare oggetti per rappresentare informazioni familiari semplici (es. colori, parole, ...)

Ambito consapevolezza digitale:

- O-P3-N-1. riconoscere usi dell'informatica e delle sue tecnologie nella vita comune
- O-P3-N-2. comprendere il concetto di informazioni private e la necessità di tenerle riservate

Obiettivi di apprendimento al termine della classe quinta della scuola primaria

Ambito dati e informazione:

- O-P5-D-1. utilizzare combinazioni di simboli per rappresentare informazioni familiari complesse (es. colori secondari, frasi,...)
- O-P5-N-3. comprendere come la riservatezza delle informazioni digitali può essere tutelata mediante codici "segreti"

Preparazione: posiziona la scheda sopra la tavoletta traforata, inserisci negli appositi spazi i chiodini dei giusti colori e, utilizzando le associazioni di colori alle lettere, crea una parola da far indovinare alla classe. I bambini devono scoprire la parola segreta a partire dal codice colorato e dal cifrario dato. Il primo a decifrare correttamente sarà il vincitore e potrà cifrare una parola da far decifrare agli altri e così via.



Figura 1

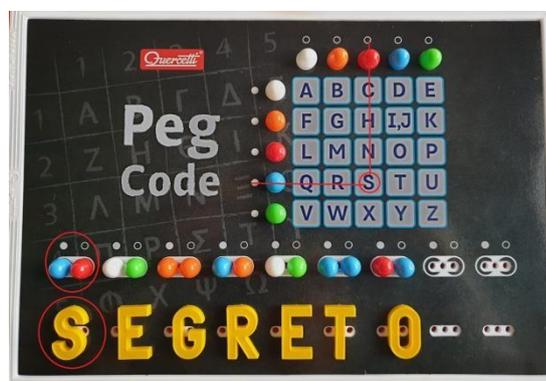


Figura 2

Dopo aver giocato un paio di volte, puoi dividere i bambini in coppie: ogni coppia dovrà creare il proprio cifrario cambiando l'ordine dei chiodini colorati sulla riga, oppure sulla colonna, oppure su entrambi, in modo da scambiarsi messaggi tramite il cifrario creato.

Successivamente domanda alle coppie: cosa potrebbe succedere se inviassero un messaggio cifrato, con il cifrario creato da loro, ad altre coppie?

Se nessuno immagina la risposta mettili alla prova: fai scambiare i codici dei messaggi tra coppie per capire se riescono a decifrarli.

Se ogni coppia ha creato il proprio cifrario, molto probabilmente i cifrari saranno diversi, quindi il codice A, creato dalla coppia A con il cifrario creato A, non è decifrabile dalla coppia B che utilizza il cifrario B, perché la chiave è diversa.

E se inviassero anche il cifrario?

Adesso ogni coppia che ha inviato un messaggio ad una determinata coppia deve mandare anche il cifrario usato, in questo modo sarà possibile per la coppia di destinatari decifrare il messaggio.

Se non si ha il gioco per tutte le coppie è possibile simularlo con carta e colori.

Questo è informatica!

I cifrari sono dei sistemi che permettono di cifrare e decifrare i messaggi a mittente e destinatario se condividono una stessa chiave. La chiave in questo gioco consiste nell'associazione di due colori ad una lettera. Un malintenzionato senza conoscere la chiave, ovvero la posizione dei chiodini colorati sul gioco, non riuscirebbe a decifrare; infatti se riuscisse ad intercettare il messaggio  non capirebbe il significato non essendo a conoscenza dell'associazione delle lettere, come ad esempio la lettera che corrisponde al blu e rosso.

Nella vita quotidiana quante volte capita di voler mandare dei messaggi solo a certe persone? Forse quasi tutti abbiamo inventato e comunicato con un cifrario.

Chiedi: vi è mai capitato di scrivere una parola al contrario? Oppure di utilizzare l'alfabeto farfallino? Continua la discussione facendo raccontare ai bambini le loro esperienze.

In informatica, la crittografia si occupa della sicurezza informatica, e fa sì che i dati, anche se inseriti su internet, rimangano privati, oppure che i messaggi che vengono inviati, ad esempio tramite WhatsApp, siano segreti a tutti gli altri tranne che per i destinatari.

Chiedi ai bambini: cosa potrebbe succedere se qualcuno riuscisse a vedere la carta di credito che i vostri genitori hanno inserito su un sito per fare un acquisto online? Cosa potrebbe succedere se qualcuno riuscisse ad ottenere la password di un vostro gioco?

Si cerca di garantire che le informazioni non possano essere rubate o lette soprattutto su internet, di cui vengono sottovalutati i rischi.

Già in passato era nata la necessità di comunicare in modo sicuro senza che altre persone potessero intercettare i messaggi. Per esempio, in caso di guerra, le informazioni sugli attacchi, schieramenti ecc. non dovevano finire nelle mani dei nemici. Il cifrario più famoso è quello di Cesare.