Attività2 - Cifrario di Cesare

- Materiale: Peg code di Quercetti
- Età: a partire da 8 anni
- Competenze acquisiste 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, ...)
- Ambito consapevolezza digitale:
- O-P5-N-3. comprendere come la riservatezza delle informazioni digitali può essere tutelata mediante codici "segreti"

Utilizzando il gioco Peg Code, che si basa sul cifrario di Pigpen, possiamo adattarlo e usarlo per simulare altri cifrari, ad esempio quello di Cesare.

Preparazione: posiziona la scheda sopra la tavoletta traforata come nel gioco precedente. Adesso i bambini proveranno ad usare il cifrario di Cesare dove il metodo per la cifratura e la decifratura sono leggermente diversi tra loro. Crea una parola da far indovinare alla classe che deve scoprire la parola segreta. Il primo a decifrare correttamente sarà il vincitore e potrà cifrare una parola da far decifrare agli altri e così via.

Per cifrare: ogni lettera viene sostituita dal codice colorato della lettera che dista 3 posizioni dalla tabella.

Vediamo un esempio: per cifrare "ciao" la "c" deve essere sostituita con la lettera distante di tre posizioni nella tabella che è la "f", eseguendo questo metodo per tutte le altre lettere il risultato finale sarà: "fmdr" scritto in codice  .

Per decifrare bisogna trovare la lettera che corrisponde al codice dei due colori e tornare indietro di 3 posizioni. Arancione e Bianco corrispondono alla "f" ma tornando indietro di tre posizioni la "f" corrisponde alla lettera "c".

Figura 1

Dopo qualche turno puoi cambiare metodo di gioco e dividerli in coppie. Ogni coppia deve avere un PegCode o un foglio su cui è simulato con carta e colori e si deve mettere d'accordo sul numero di posizioni di cui spostarsi nell'alfabeto, non per forza 3. A turno un componente della coppia cifra e l'altro decifra.

È consigliata la visione del quesito Crittografia su https://bebras.it/lib/libretto-esempi.pdf

Questo è informatica!

Il cifrario di Cesare viene detto a sostituzione monoalfabetica perché ogni lettera viene sostituita sempre dalla stessa: la lettera "c" verrà sempre sostituita nelle altre parole dalla lettera "f" a cui corrisponde Arancione e Bianco. La lettera con cui verrà sempre sostituita però dipende dalla chiave: il numero di posizioni dello spostamento.

Domanda per gli studenti: cosa succederebbe se utilizzassimo uno spostamento di 25 posizioni?
La lettera verrebbe sostituita con sé stessa, quindi affinché questo cifrario sia utile bisogna utilizzare uno spostamento compreso tra 1 e 24 posizioni.

Il cifrario di Cesare prende il nome da Giulio Cesare, che lo utilizzava per proteggere i suoi messaggi segreti spostandosi sempre di 3 posizioni. Al tempo era sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato. Anche la regina di Scozia Maria Stuarda fece uso del Cifrario per impedire alla guardia di comprendere il messaggio contenuto in una lettera, con la quale stava progettando un complotto, vale a dire l'omicidio della Regina inglese Elisabetta I. La lettera venne, però, subito decrittata per la semplicità del metodo utilizzato (utilizzava 2 posizioni).

Per utilizzare i cifrari visti finora, e molti altri, bisogna prima decidere la chiave da utilizzare e in seguito si può cifrare e decifrare utilizzandola, nel caso del Cifrario di Cesare bisognerà stabilire i colori da associare alle lettere e di quante posizioni ci si dovrà spostare nella tabella dell'alfabeto mentre nel cifrario di PigPen bisognerà stabilire solo i colori da associare in ogni lettera.

Per scambiare il messaggio in modo sicuro la chiave deve essere segreta a chiunque altro. Come può avvenire in modo sicuro questo scambio di informazioni sulla chiave senza che l'avversario possa intercettarla e usarla per leggere i nostri messaggi?
Esiste un metodo per lo scambio di chiavi chiamato Diffie-Hellman. Questo algoritmo fu uno dei primi algoritmi a chiave pubblica.