Attività3 - Locke and Key

- Materiale: Peg Code di Quercetti, Card Game, un Dado a 6 facce
- 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"

Preparazione: dividi la classe in due gruppi: i Romani e i Barbari. Il gruppo dei Romani viene diviso a sua volta in due gruppi distanziati fisicamente nella classe: gruppo Cavalieri e gruppo Vassalli, unisci i banchi per creare delle vere e proprie postazioni.
Scrivi alla lavagna un numero primo e la radice primitiva di quel numero, ad esempio 7 e 3. Stampa e distribuisci le Card Game ad ogni bambino del gruppo dei Romani.
Successivamente ogni bambino del gruppo deve tirare un dado a 6 facce e il numero casuale uscito deve essere segnato sulla carta Key segreta e privata.

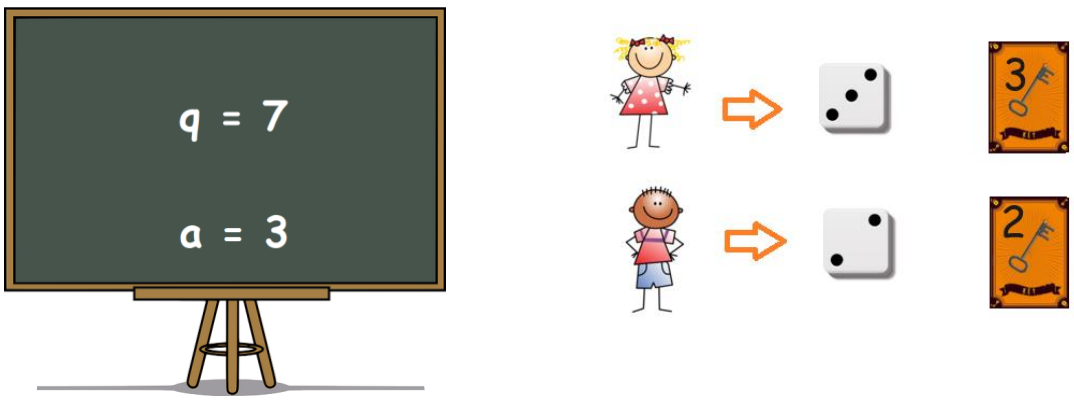

Figura 1

Aiuta ogni bambino a calcolare la carta Lock: bisogna elevare la radice primitiva *a* al numero della carta Key, il risultato deve essere diviso per il numero primo *q* e bisogna calcolarne il resto.
Il resto deve essere scritto sulla carta Lock.

Nella Figura 1 il romano Bob lancia il dado da cui esce il numero 2, scrive allora sulla carta Key il numero 2.

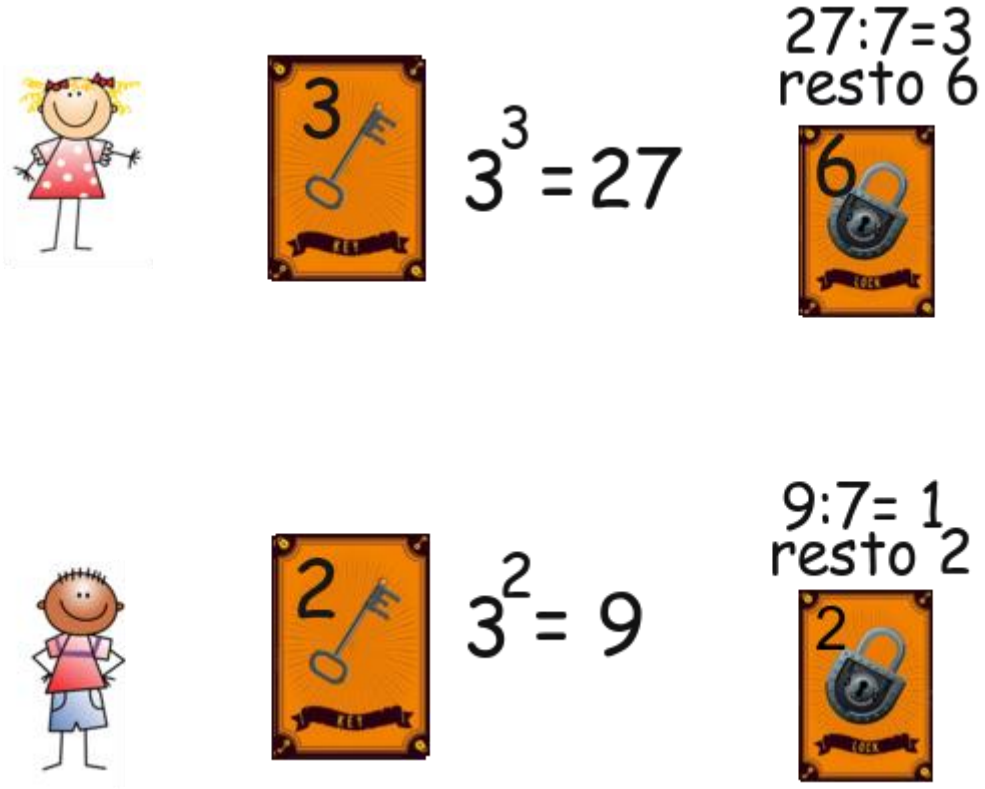

Figura 2

Nella Figura 2 Bob ha come carta Key il 2 calcolato precedentemente, adesso eleva la radice primitiva alla sua carta Key e trova come risultato 9, esegue la divisione del risultato con il numero primo 9:7=1 resto 2 → scrive 2 sulla carta Lock.

I possibili risultati rispettivamente Key e Lock sono: (1,3), (2,2), (3,6), (4,4), (5,5), (6,1).

Non appena le carte sono pronte, ogni bambino del gruppo dei Romani deve essere in possesso del Peg Code (se il numero di Peg Code è insufficiente si può simulare su un foglio di carta), deve posizionare sul banco la propria carta Lock scoperta e, invece, deve tenere ben nascosta la propria carta Key privata.

Inizia il gruppo dei Vassalli che si muove per andare alla postazione del gruppo dei Cavalieri. Ogni vassallo deve prendere la carta Lock di un cavaliere con cui vuole comunicare, deve consegnargli la propria carta Lock e poi tornare alla propria postazione.
I barbari sono liberi di gironzolare nella classe e guardare le azioni dei nemici, per questo motivo Vassalli e Cavalieri non possono parlare e l'unico modo per comunicare è quello di inviarsi messaggi segreti.

Successivamente ogni romano deve calcolare una chiave simmetrica condivisa usando la propria Key e il Lock del compagno appena avuto: bisogna elevare il numero della carta Lock del compagno al numero della propria carta Key, dividere il risultato per *q* e calcolarne il resto. Il resto rappresenta la chiave condivisa per cifrare e decifrare e, in questo caso, individua il numero di posizioni di cui spostarsi nell'alfabeto nel cifrario di Cesare.
Nota: aiuta ogni bambino nei calcoli.

Immaginiamo una situazione come nella figura sottostante, il vassallo ha come carta Key 2 e come carta Lock 2 (come calcolato nella Figura 2), decide di effettuare lo scambio di informazioni con il cavaliere Carlo, che ha come carta Key 6 e come carta Lock 1, quindi scambia le loro carte Lock.
Adesso devono entrambi calcolare la chiave condivisa che utilizzeranno entrambi per comunicare sulla base della loro carta Lock e della chiave Lock appena ricevuta.

Il cavaliere Carlo prosegue nel calcolo uguale a quello svolto precedentemente, ciò che cambia è la carta Lock, infatti utilizzerà non più la sua ma quella nuova ottenuta dallo scambio. Deve quindi elevare la carta Lock alla propria carta Key $2^6 = 64$, dividere questo risultato per il numero primo 7: 64:7=9 resto 1. Il resto 1 indica la chiave condivisa, in questo caso rappresenta il numero di posizioni in cui spostarci nel cifrario di Cesare.

Anche il vassallo Bob allo stesso tempo calcola la chiave condivisa elevando la carta Lock alla propria carta Key $1^2 = 1$, divide il risultato per il numero primo 7 in modo che il resto gli indichi la chiave condivisa: 1:7=0 resto 1.

In questo caso il calcolo è stato effettuato da entrambi in modo corretto, la chiave condivisa è la stessa (Figura 3).

Figura 3

I vassalli, quindi, cifrano il messaggio utilizzando il Peg Code e la chiave di Cesare appena calcolata, riportano il codice colorato sulla pergamena, e al tuo via, devono riuscire a consegnare i messaggi al cavaliere giusto mentre i barbari cercano di fermarli: se un barbaro prende toccando un romano esso dovrà rimanere fermo in attesa che un compagno vassallo lo liberi toccandolo.
Non appena un cavaliere riceve un messaggio può iniziare a decifrarlo con la chiave di Cesare calcolata precedentemente; i barbari non possono né fermarlo né infastidirlo.

Al tuo stop tutti devono fermarsi e ritornare alle proprie postazioni, anche chi non è riuscito a consegnare il messaggio. La coppia che decifra correttamente per prima sarà la vincitrice. Al prossimo turno partiranno i cavalieri per comunicare con i vassalli.

Scambia anche i barbari e continua a farli giocare a turno in modo che tutti provano tutti i ruoli almeno una volta.

Attenzione: se una coppia non esegue i calcoli correttamente la chiave di Cesare condivisa non sarà la stessa quindi il messaggio non sarà decifrabile.

Immaginiamo ad esempio che il cavaliere Carlo non ricordi le tabelline ed esegua: 64:7 = 8 resto 8, Carlo pensa che 8 sia la chiave condivisa quindi si sposterà nel cifrario di Cesare di 8 posizioni per comunicare con Bob che invece si è spostato di una posizione. Cosa succederà?
Il messaggio decifrato da Carlo risulterà incomprensibile.

Provalo con i bambini: fai in modo che ogni cavaliere sbagli il calcolo, fai scrivere ai vassalli un messaggio con la chiave esatta calcolata in precedenza, e fai decifrare il nuovo messaggio ai cavalieri consapevoli di avere una chiave condivisa errata. Si accorgeranno che effettivamente non potranno decifrare in modo corretto il messaggio.

Questo è informatica!

I cifrari sono simmetrici o asimmetrici.

I cifrari simmetrici sono detti anche a chiave condivisa: la chiave è la stessa per cifrare e decifrare, e sono quelli che abbiamo visto finora (Pigpen e Cesare).

I cifrari asimmetrici sono detti a chiave pubblica e privata: ogni utente possiede una coppia di chiavi di cui una è pubblica, visibile da tutti, che tutti possono utilizzare per cifrari i messaggi a lui destinati, un'altra privata che detiene solo lui e che usa per decifrare i messaggi ricevuti. È come se tutti lasciassero dei lucchetti aperti su un banco.
Chi vuole inviare un messaggio prende il lucchetto del destinatario con cui chiude una scatola contenente il messaggio e solo il destinatario, proprietario del lucchetto, ha la chiave giusta per aprirlo.

Quest'ultimo tipo di cifratura, quella asimmetrica, in generale è usata per lo scambio segreto di chiavi simmetriche.
Ogni utente, infatti, calcola una chiave privata e sulla base di questa calcola la chiave pubblica da rendere nota a tutti.

Anche se può sembrare un calcolo complicato, in realtà è molto semplice, mentre il calcolo inverso è impossibile! Quindi la chiave privata non può essere scoperta.
In seguito, sulla base della propria chiave segreta e della chiave pubblica della persona con cui vogliamo comunicare, si può calcolare una chiave simmetrica condivisa eseguendo il calcolo: chiave pubblica del compagno elevata alla propria chiave privata, il risultato viene diviso per il numero primo q e poi viene calcolato il resto.
Il resto calcolato sarà proprio la chiave simmetrica condivisa da un vassallo e un cavaliere per comunicare e solo loro la conosceranno perché entrambi i loro calcoli, anche se diversi, portano allo stesso risultato...sembrerebbe magia ma è pura matematica!

Tutto questo funziona perché i bambini vedono chi arriva a scambiare le carte Lock, quindi sono sicuri di conoscere la persona con cui stanno comunicando...