Attività4 - Man in the middle

- Materiale: Peg Code di Quercetti, Card Game, un Dado a 12 facce
- Età: a partire da 9 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"
- O-P5-N-4. riconoscere comportamenti accettabili/inaccettabili nell'uso della tecnologia informatica e delle informazioni ottenute per suo tramite

Preparazione: dividi la classe in 2 gruppi: spie e poliziotti. I poliziotti vengono ulteriormente divisi in altri due gruppi distanziati fisicamente: poliziotti del dipartimento Blu e poliziotti del dipartimento Nero, unisci i banchi per creare delle postazioni come nel gioco precedente.

Ogni poliziotto deve avere il Peg Code, alle spie ne basta uno condiviso (se il numero di Peg Code è insufficiente simulalo su un foglio di carta).
Scrivi alla lavagna un numero primo e la radice primitiva di quel numero, ad esempio 13 e 2. Stampa e distribuisci le Card Game ad ogni poliziotto (stampa un numero maggiore di pergamene e consegnane 3/4), invece, il gruppo delle spie deve avere solamente due carte Lock, una carta Key, 4/5 pergamene.

Successivamente ogni poliziotto deve tirare un dado a 12 facce e il numero casuale uscito dovrà essere segnato sulla carta Key, lo stesso procedimento deve essere eseguito da un solo componente delle spie.

Come nel gioco precedente aiuta ogni bambino a calcolare la carta Lock: bisogna elevare la radice primitiva a al numero della carta Lock, il risultato deve essere diviso per il numero primo q e bisogna calcolarne il resto. Il resto deve essere scritto sulla carta Lock. Le spie hanno due carte Lock e devono scrivere su entrambe il risultato.

1	1	2
2	2	4
3	3	8
4	4	3
5	5	6
6	6	12
7	7	11
8	8	9
9	9	5
10	10	10
11	11	7
12	12	1

Figura 1

Scegli adesso delle coppie fisse di poliziotto Blu e poliziotto Nero. Ogni poliziotto Blu deve scrivere sulla pergamena il proprio nome e inserire la propria chiave pubblica, mentre sul retro deve scrivere il nome del compagno a cui è destinata, poi deve chiudere la pergamena con la carta Lock dentro, lasciarla su un banco al centro della classe e tornare al proprio posto (Figura 2).

Figura 2

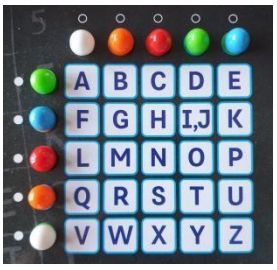
Accendi della musica a tema (ad esempio la musica della pantera rosa), i poliziotti devono girarsi e coprirsi gli occhi, le spie possono entrare in azione e tutte d'accordo devono scegliere una coppia vittima che deve essere la stessa durante tutto il gioco e un messaggio da falsificare: devono prendere la carta Lock inserita nella pergamena, tenerla, sostituirla con la loro carta Lock e rimettere la pergamena a posto. Stoppa la musica, i poliziotti Neri devono recarsi al centro della classe per prendere il messaggio a loro destinato, prendere la carta Lock, e scrivere un messaggio di risposta con il proprio nome e la propria chiave pubblica, cioè la carta Lock (Figura 3).

Figura 3

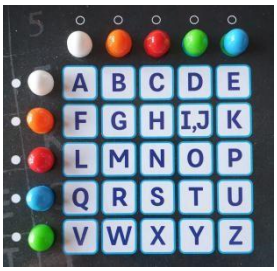
Il messaggio deve essere lasciato al centro della classe, parte di nuovo la musica e le spie devono prendere il messaggio dell'altro componente della coppia, sostituire la carta Lock con la loro e tenersi la carta Lock della vittima a cui l'hanno rubata. Stoppa la musica, i poliziotti Blu prendono i loro messaggi e tornano a posto.

Tutti devono calcolare la chiave condivisa come nel gioco precedente: chiave pubblica elevata alla propria chiave privata, il risultato viene diviso per 13 e il resto della divisione rappresenta la chiave condivisa utilizzata per cifrare e decifrare i messaggi, in questo caso viene utilizzata una configurazione del cifrario di Pigpen, mostrale alla lavagna in modo che ogni bambino, dopo aver calcolato la chiave, configuri nel modo corretto il cifrario.

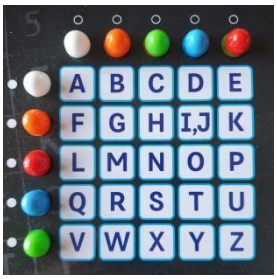
Chiave condivisa = 1



Chiave condivisa = 2

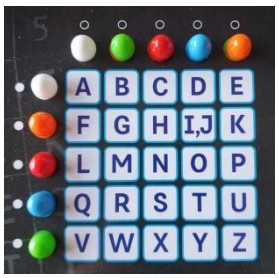


Chiave condivisa = 3

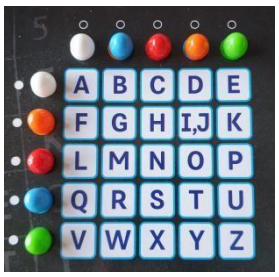


Chiave condivisa = 4

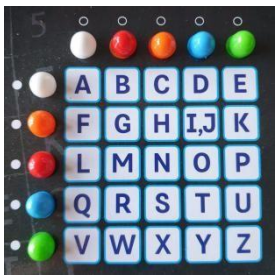
Chiave condivisa = 5



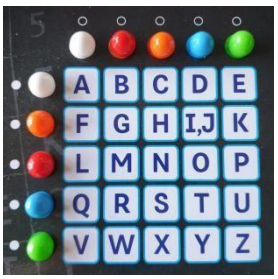
Chiave condivisa = 6



Chiave condivisa = 7



Chiave condivisa = 8



Chiave condivisa = 9

Chiave condivisa = 10

Chiave condivisa = 11

Chiave condivisa = 12

La situazione dovrebbe essere come nella Figura 4:

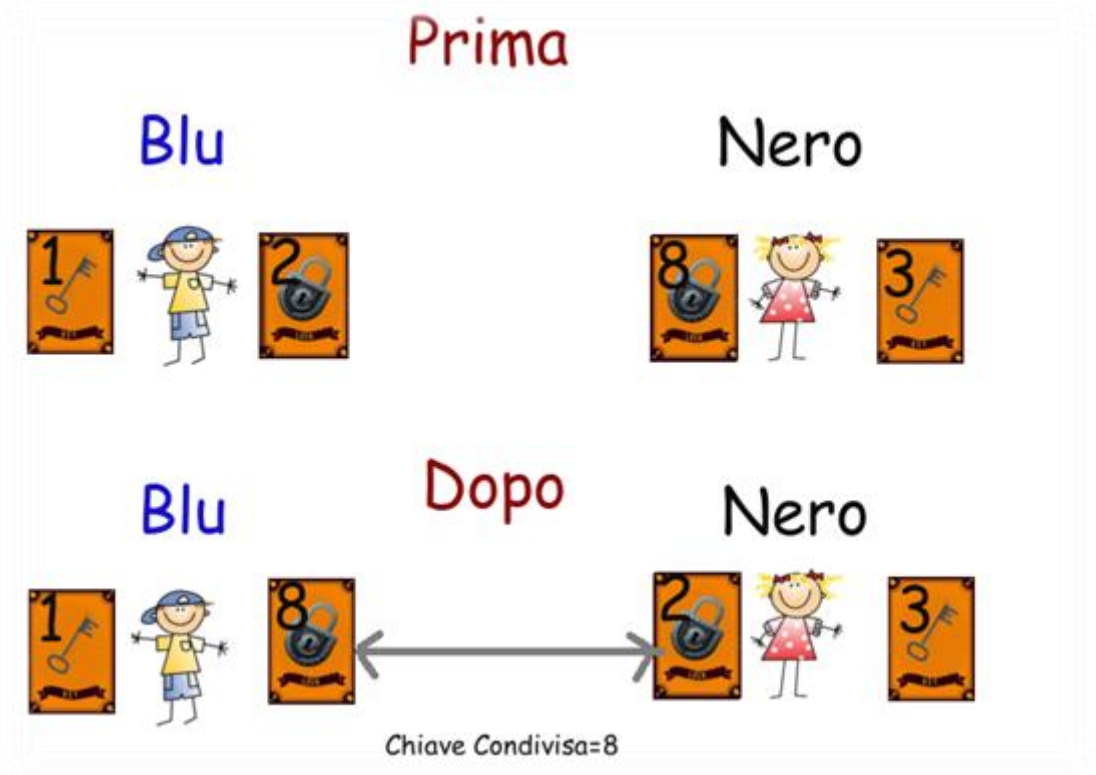


Figura 4

Tranne per la coppia intercettata, Figura 5:

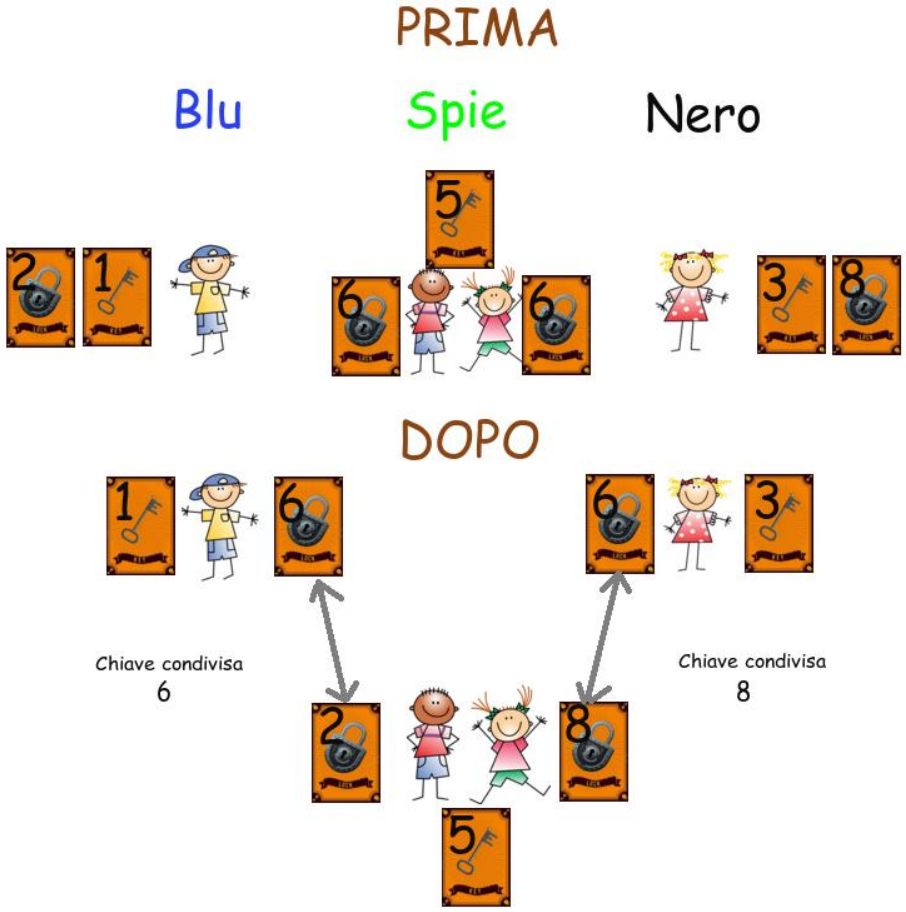


Figura 5

Il poliziotto Blu adesso può scrivere e cifrare un messaggio con la chiave condivisa calcolata, ricordandosi di scrivere sempre sul retro il nome del destinatario.
Dopo averlo riposto al centro della classe parte di nuovo la musica, tutti si girano e si coprono gli occhi, le spie entrano in azione: prendono il messaggio della coppia intercettata, lo decifrano con la chiave che condividono con il proprietario del messaggio, successivamente scelgono un messaggio con cui sostituirlo, lo cifrano con la chiave che condividono con il destinatario della coppia e lo ripongono al centro della classe.

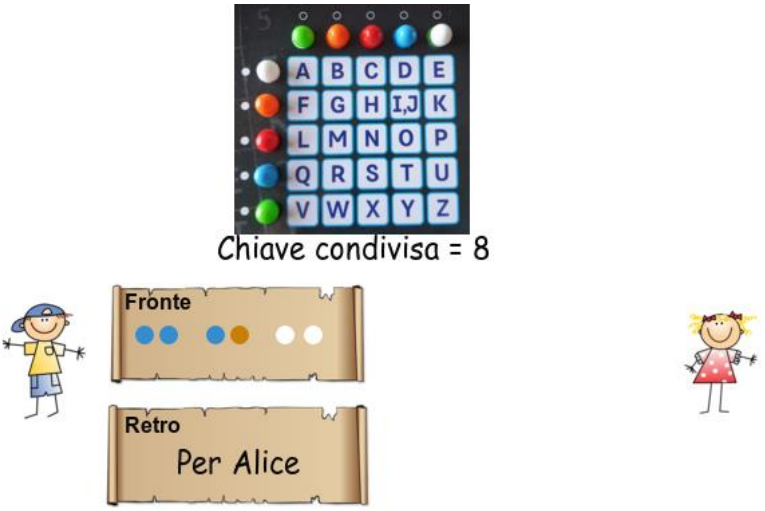


Figura 6

Stop alla musica, ogni poliziotto nero prende il messaggio e lo decifra con la chiave condivisa che ha calcolato, successivamente scrive un messaggio di risposta, lo cifra e lo ripone al centro della classe.
Lo scopo è quello di rispondere con una parola/messaggio che abbia un senso con il messaggio ricevuto in modo da accorgersi se si è stati vittima delle spie ricevendo messaggi falsificati.

Via alla musica, le spie prendono il messaggio di risposta, lo decifrano con la chiave che condividono con il proprietario del messaggio, scelgono un messaggio con cui sostituirlo, lo cifrano con la chiave condivisa con il destinatario e lo ripongono al centro della classe. Stop alla musica, i poliziotti blu prendono e decifrano il messaggio di risposta.

Adesso chiedi ai poliziotti se sono sicuri di aver comunicato con il compagno stabilito. Se la coppia che è stata realmente intercettata pensa di aver ricevuto messaggi falsificati, vince!

Questo è informatica!

Abbiamo visto che per mandare messaggi in codice bisogna mettersi d'accordo sulla chiave, che può essere il numero di posizioni di cui spostarsi nell'alfabeto, oppure una configurazione colorata, ma anche lo scambio di questa informazione deve avvenire in modo segreto, ad esempio, con il metodo Diffie-Hellman che prevede l'associazione ad ogni utente di una chiave privata, segreta, e una chiave pubblica, visibile a tutti.

Ogni utente utilizza la chiave pubblica dell'utente con cui vuole comunicare e la propria chiave privata per generare una chiave condivisa con quell'utente, anch'esso userà la chiave pubblica e la propria chiave privata per calcolare, anche se in modo diverso, la chiave condivisa che sarà identica.

Grazie alla matematica, lo scambio della chiave avviene in modo segreto, ma in questo gioco ci siamo accorti di come un'intercettazione potrebbe passare inosservata, qualcuno potrebbe intercettare un messaggio e fingersi qualcun altro.

L’uomo nel mezzo, nel gioco le spie, intercetta i messaggi di Bob e Alice che non si scambiano le chiavi tra loro, ma, le spie si scambiano le chiavi con Alice e con Bob.

La comunicazione avviene tra le spie e Alice, e, tra le spie e Bob e le due vittime non se ne accorgono. Bob non manda direttamente il messaggio ad Alice ma lo manda inconsapevolmente alle spie, le spie lo leggono, possono modificarlo e lo rinviano ad Alice, Alice legge il messaggio falsificato dalle spie pensando che sia Bob e, quando risponde, il messaggio non viene inviato direttamente a Bob ma passa dalle spie che lo leggono, lo modificano e inviano questa risposta falsa a Bob, Bob lo legge pensando che sia la riposta di Alice.

Questo è possibile, diversamente dal gioco precedente, poiché come avviene nella realtà, nella rete internet, non si vede la persona con cui ci si scambia la chiave, con cui si comunica, e qualcuno potrebbe fingersi qualcun altro. Questo metodo funziona solo se si comunica su un canale sicuro sul quale non ci sono malintenzionati, oppure, se la coppia <identità, chiave pubblica> è firmata da un Autorità Centrale, saremo sicuri della persona e la corrispondente chiave con cui scambiamo i messaggi. Questa firma è come l’ologramma sulla banconota che, se mossa, cambia forma e ci assicura la validità della banconota.