Attività5 - Decrypto

- Materiale: Decrypto di Asmodee
- Età: a partire da 11 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 due squadre, squadra bianca e squadra nera, scegli per ognuna un bambino che sarà il codificatore, successivamente leggi le istruzioni del gioco a tutti.
Riassumendo:

1. Ogni squadra ha a disposizione 1 schermo, 1 foglio di appunti, 1 mazzo di carte codice
2. Ogni squadra deve inserire nello schermo 4 parole chiave segrete
3. Il codificatore di una squadra pesca una carta codice che mostra un codice di 3 cifre
4. Il codificatore deve trasmetterlo alla sua squadra fornendogli indizi inerenti alle parole chiave di cui sono tutti a conoscenza
5. Gli avversari nel mentre annotano gli indizi e il codice che la squadra ha associato a questi
6. Si ripete quanto fatto finora per l'altra squadra
7. A partire da ora, ad ogni turno, ogni squadra con gli indizi che ha, senza conoscere le parole segrete dell'altra, è in grado di intercettare il codice.

È consigliata la visione del video https://youtu.be/P8q4gO5wiI4 per capire bene le regole del gioco.

Immaginiamo che la squadra bianca abbia come parole chiave segrete in posizione 1 SOCIAL MEDIA, in posizione 2 RAGNO, in posizione 3 BARCA, in posizione 4 MOTORE e che il codificatore della squadra peschi il codice 3.2.1. da trasmettere ai compagni, per trasmetterlo deve fornire degli indizi ai compagni, sulla base delle conoscenze comuni, ovvero sulla base della conoscenza comune e condivisa della chiave.

Chiedi agli studenti, in questo caso, la chiave da cosa è rappresentata? Dalle 4 parole segrete.

Gli indizi consistono in parole a cui i compagni devono attribuire un numero da 1 a 4 basandosi sulle parole segrete in quelle posizioni.
Nella Figura 1 il codificatore inizia a trasmettere il 3, deve quindi pensare ad una parola che abbia a che fare con la carta in posizione 3, cioè barca, potrebbe pensare a VELA, per trasmettere il 2 deve pensare ad una parola che si possa relazionare alla carta RAGNO, ad esempio, RAGNATELA, infine, per trasmettere 1 deve pensare ad una parola del mondo dei social media come INSTAGRAM.

I compagni devono quindi associare VELA alla barca che corrisponde ad 1, RAGNATELA a ragno che corrisponde a 2, INSTAGRAM a social media che corrisponde a 1. Ecco formato il codice 3.2.1.

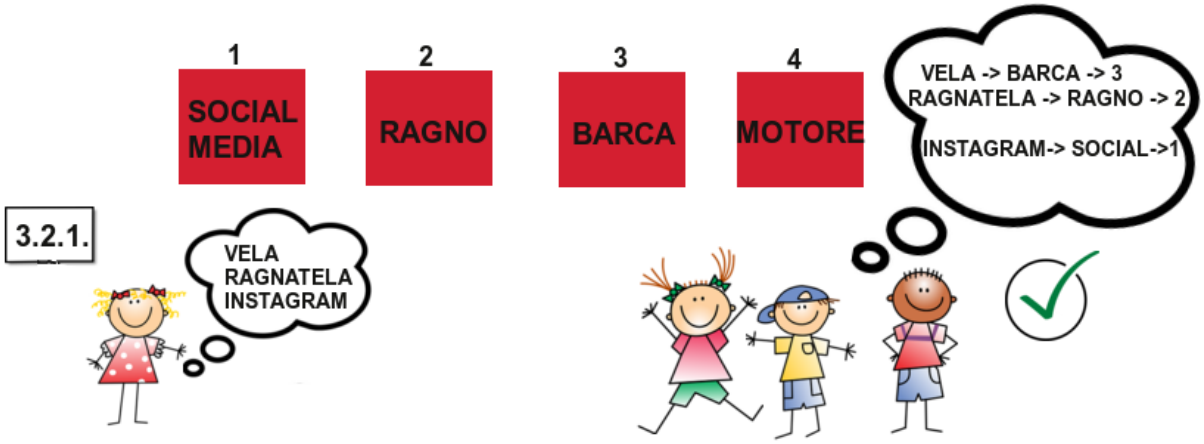

Figura 1

La squadra avversaria può annotare gli indizi dati dal codificatore e il codice formato dai compagni (Figura 2).

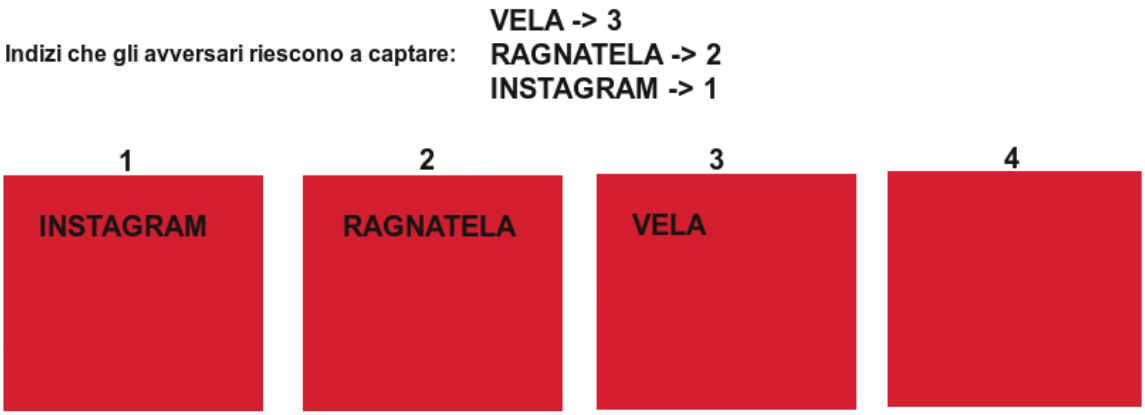

Figura 2

La squadra avversaria può annotare gli indizi dati dal codificatore e il codice formato dai compagni.
Lo stesso meccanismo avviene per la squadra bianca che, al turno della nera, cerca di captare gli indizi.
Dopo qualche turno la situazione della squadra nera potrebbe essere la seguente:

Figura 3

Variante leggermente più complessa:

Introduci una nuova regola di fine round: non vince il gioco la squadra che ha 2 segnalini Intercettazione, e la squadra che ha 2 segnalini Comunicazione Errata non perde la partita, ma vince la partita la squadra che per prima, con le informazioni a disposizione, riesce ad indovinare le parole chiave della squadra avversaria.

Un consiglio per rendere difficile la scoperta delle parole chiave è quello di dare indizi non troppo “facili” e “banali”.

La squadra nera, ad esempio, con le informazioni ottenute per la parola segreta 1, potrebbe subito dedurre che Instagram, Facebook, Tik Tok, Snapchat sono dei social media quindi la parola chiave potrebbe essere Social Media; potrebbe essere anche molto facile riuscire a dedurre la parola segreta Ragno a partire da Ragnatela, Otto, Animale, Veleno; mentre è difficile pensare alla parola Motore conoscendo solo Macchina e Combustione.

Questo è informatica!

Nella vita reale, quando è impossibile riuscire ad intercettare la chiave per indovinare il metodo di cifratura con lo scopo di decifrare i messaggi segreti si può attuare un’altra tecnica chiamata Crittoanalisi Statistica.

La crittoanalisi è la scienza parallela alla crittografia, infatti essa è volta a eliminare le protezioni offerte dalla crittografia tramite lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione.
Uno di questi metodi è effettuare l'attacco con testo in chiaro scelto che presume che l'attaccante abbia la capacità di scegliere del testo in chiaro arbitrario da fare cifrare ed ottenere il corrispondente testo cifrato. L'obiettivo dell'attacco è quello di ottenere quante più informazioni possibili in modo da ridurre la sicurezza dello schema di cifratura. Nel peggiore dei casi, un attacco con testo in chiaro scelto può arrivare a rivelare la chiave segreta dello schema.
Nel gioco le 4 parole segrete sono la chiave, il testo in chiaro è il codice, il testo cifrato è rappresentato dagli indizi.

La cifratura viene effettuata dal codificatore che, per trasmettere in modo sicuro il codice ai suoi compagni, utilizza la chiave segreta (le 4 parole) per trasformare il messaggio in chiaro (il codice di 3 cifre) in messaggio cifrato (gli indizi)

La decifratura viene eseguita dai compagni di squadra che a partire dal testo cifrato (gli indizi) e dalla chiave (le 4 parole) scoprono il testo in chiaro (codice di 3 cifre).

La squadra avversaria riesce a captare il testo in chiaro (codice di 3 cifre) sentendolo dai compagni di squadra che effettuano la decifratura e sentono anche gli indizi dato a loro dal codificatore, ma non sono a conoscenza della chiave. Essendo però a conoscenza del testo in chiaro e il corrispettivo testo cifrato essi potrebbero fare delle ipotesi, delle assunzioni per indovinare la chiave segreta che, una volta ottenuta, permette di decifrare tutti i messaggi in modo corretto.

Per esempio, WhatsApp cifra e decifra i messaggi che voi inviate, i messaggi viaggiano su internet in modo cifrato. Immaginiamo che Bob vostro amico e membro della classe sia un hacker provetto e riesca a guardare tutti i messaggi su internet, in particolare vede il messaggio che Alice manda a Chiara anche se incomprensibile, se poi Bob, di nascosto, prende il telefono a Chiara, riesce a leggere il messaggio in chiaro, e sapendo anche quello cifrato, potrebbe iniziare ad ipotizzare una chiave di cifratura.