

Tu quoque, Brute!

Istituto Comprensivo “Antonio Sant’Elia” – Villaguardia (CO)

Classe: 2°A

Insegnante di riferimento: Giuseppa Michelangela Rizzo

Ricercatore: Marta Diacci

Ragazzi partecipanti: Matteo Aggio, Gianluca Baglieri, Moatez Ben Salha, Sofia Bollini, Davide Bonsignore, Federica Briccola, Stefania Costante, Marika Faggionato, Matteo Frezzato, Alessia Gini, Francesca Giurina, Elisa Lamedica, Giulia Langone, Matteo Laurito, Simone Lo schiavo, Francesco Montorfano, Carlotta Montori, Igor Moscatelli, Elettra Martina Peverelli, Gaetano Pinto, Margherita Rini, Nicole Robustelli, Matteo Sirco, Sara Sonzogni, Alessio Sorgiovanni, Pietro Olmo Turconi, Stefano Veronelli

Siamo a Roma nel I secolo a.C.

Per via della sua favorevole posizione di retrovia, Mediolanum si sta rivelando di importanza notevole per le campagne di Giulio Cesare alla conquista della Gallia. Ora Cesare deve mandare ai suoi generali di stanza proprio a Mediolanum alcune indicazioni su come arruolare nuove legioni di soldati e su come prepararsi a raggiungerlo. Sono questioni delicate e quindi c'è bisogno di trovare un metodo di comunicazione TOP SECRET (si sa che non c'è da fidarsi dei messaggeri!).

Cesare inventa per l'occasione un cifrario a cui gli altri daranno poi il suo nome, ma c'è un problema serio: il suo quartier generale è infestato da spie mandate dai Galli e da spie mandate dai suoi avversari nel Senato romano (molto più pericolose).

IL CIFRARIO DI CESARE

Il metodo ideato da Cesare per crittografare (cioè rendere incomprensibili ai nemici) i suoi messaggi consiste nello spostare tutto l'alfabeto di un determinato numero di lettere e a quel punto nel sostituire ogni lettera con quella corrispondente nell'alfabeto cifrato:

| | | | | | | | | | | | | | | | | | | | | | |
|------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alfabeto | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z |
| Alfabeto cifrato | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T |

Di quante lettere è stato spostato l'alfabeto della tabella precedente per ottenere quello cifrato? A quale lettera corrisponde la A cifrata?

Questa lettera si chiama chiave ed è l'elemento essenziale da conoscere per poter cifrare e decifrare un messaggio con il metodo di Cesare.

Se l'imperatore avesse voluto cifrare il suo nome GIULIO CESARE con la chiave D come sarebbe diventato?

- Come possono fare Cesare e i suoi per scambiarsi la chiave senza rischiare di essere scoperti da un traditore?

- Se un messaggero volesse provare a decifrare il messaggio senza conoscere la chiave come potrebbe fare? Pensate che ci riuscirebbe?

Come possono fare Cesare e i suoi per scambiarsi la chiave senza rischiare di essere scoperti da un traditore?

- Mettere il messaggio in uno scrigno con varie serrature solo una è quella giusta, se si sbaglia si sprigiona una sostanza che rende illeggibile il messaggio
- Inviare le coordinate delle lettere del messaggio al Generale, che possiede la tabella con le lettere scritte casualmente
- Mandare diversi messaggeri per strade differenti ognuno con una parte del messaggio

I codici potrebbero essere :

- Il messaggio inizia con la lettera che indica la chiave (es. 9=i)
- Il messaggio è formato da parole fuorvianti fra cui la chiave (es. trova un fiore con tre petali: chiave 3)
- Utilizzare gli ideogrammi

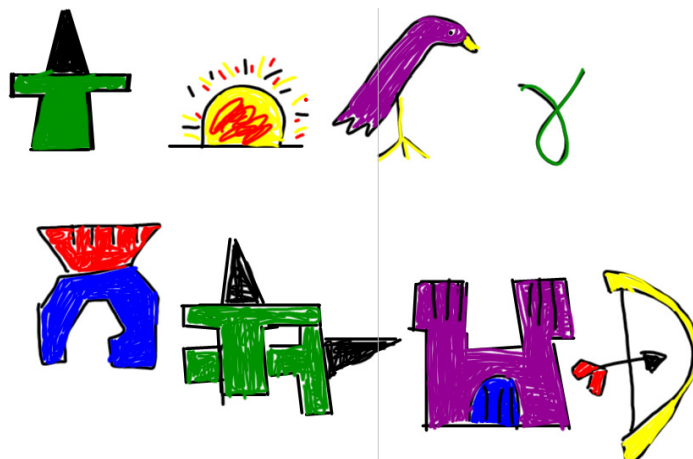


Fig. 1 – Soluzione: battaglia all'alba mandare 3 legioni saccheggiare città nemiche

- Utilizzare uno spartito musicale



Fig. 2 – Soluzione: l'originalità è il nostro forte

-Inventare un nuovo linguaggio

Fig. 3 – Soluzione: spade finite, abbiamo bisogno di nuove armi

-Scrivere le parole in modo speculare

LLA ERINURBMI
 IVETEGIRID OSREV
 AVONEG NOC
 ICEID IRRAC

Fig. 4 – Soluzione: all'imbrunire dirigetevi verso Genova con dieci carri

- La chiave è il numero corrispondente dell'ultima lettera del messaggio
- Invertire le sillabe delle parole Es.: Viain nau patrur = invia una truppa
- Far corrispondere la lettera ad un numero

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

CIFRATO:

| | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 2 | 4 | 6 | 8 | 10 | 7 | 9 | 11 | 13 | 15 | 12 | 14 | 16 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 18 | 20 | 17 | 19 | 21 | 23 | 25 | 22 | 24 | 26 | 13 | 5 | |

ES:

| | |
|---------------|----------------|
| A = 1 + 1 = 2 | F = 6 + 1 = 7 |
| B = 2 + 2 = 4 | G = 7 + 2 = 9 |
| C = 3 + 3 = 6 | H = 8 + 3 = 11 |

FRECCE E LANCE

6 | 18 | 5 | 3 | 3 | 5 5 12 | 1 | 14 | 3 | 5

7 | 21 | 10 | 6 | 6 | 10 10 14 | 2 | 18 | 6 | 10

Fig. 5 - .Quest'ultimo si ottiene sommando il numero corrispondente alla posizione della lettera nell'alfabeto un numero da 1 a 5 in ordine crescente. Una volta giunti a 5 si ricomincerà da 1

-Fare il codice tramite un rebus



Fig. 6.- Soluzioni rebus: urgente bisogno di riforma fiscale;
 adoro saccheggiare; siamo in battaglia navale

Se un messaggero volesse provare a decifrare il messaggio senza conoscere la chiave come potrebbe fare? Pensate che ci riuscirebbe?

-Potrebbe provare con tutte le chiavi.

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z |
| Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V |
| V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U |
| U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T |
| T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S |
| S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R |
| R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q |
| Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O | P |
| P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N | O |
| O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M | N |
| N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L | M |
| M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I | L |
| L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H | I |
| I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G | H |
| H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F | G |
| G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E | F |
| F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D | E |
| E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C | D |
| D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B | C |
| C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A | B |
| B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z | A |
| A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | Z |

-Come utilizzare la tabella:

ciao= **dons** BENE (CHIAVE) alfredo=**bpsvfhb** BENE BEN cappello =**ihiegzu**
GUSTAVOG casa=**oafd** MANDARINO

Doppie : tabella VIGENERE

Chiave lunga come messaggio: nessun problema

Chiave più corta del messaggio: ripetere la chiave fino ad arrivare alla lunghezza del messaggio

Chiave con doppia coincidente alla doppia del messaggio cambio di chiave

Chiave più lunga: considerare solo il pezzo utile