

# Caravaggio's puzzle

Prova di crittografia mediante codici testuali e grafici



L'obiettivo di questa sfida è quello di scoprire chi si cela dietro l'immagine in JPG che è stata assegnata ad ogni gruppo. Il file a disposizione è il risultato di una crittografia RSA applicata alla matrice di colori dell'immagine originale.

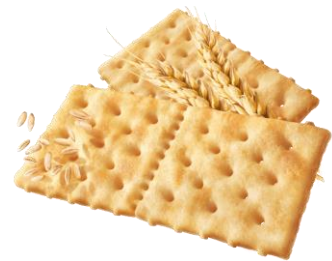
Per poter tornare a visualizzare l'immagine di partenza dobbiamo riuscire a decodificare secondo la stessa tecnica. Possiamo farci aiutare dall'informatica attraverso i due programmi (che vi sono stati forniti) che traducono in algoritmo i metodi di crittografia:

1 – decritto.nb

2 – decoVigenere.exe

Ma saranno sufficienti i software, se non conosciamo le chiavi?

Dovete diventare dei veri cracker!!!



Vediamo insieme i passaggi per scoprire la foto misteriosa!!

1- All'interno del file decritto.nb dobbiamo inserire il percorso del file dell'immagine criptata assegnata al vostro gruppo e le chiavi *ekeyset*, *dkeyset*, *enneset*... ma non le conosciamo!!

```
(*Inseriamo le chiavi pubbliche*)  
ekeyset = ;  
dkeyset = ;  
enneset = ;
```

```
n le domande dal primo elemento di ogni pixel*)  
nte\\Desktop\\PLS2023-2024\\5M\\_____ .png"[]];
```

← Percorso per file

2- Per poter individuare le prime 2 dobbiamo rispondere a delle domande... ma non le conosciamo!! Come possiamo scoprire le domande per trovare *ekeyset* e *dkeyset*???

3- Per far comparire le domande in chiaro è necessario eseguire il programma variando il parametro *keycif* da 1 a 9 fin quando non avete la decrittazione del testo di due domande.

```
(*Programma di decrittazione*)
(*Primo passo, recuperiamo il testo con le domande dal primo elemento di ogni pixel*)
tbin = ImageData[Import["C:\\Users\\Utente\\Desktop\\PLS2023-2024\\5M\\img5M.png"]];

dims = Dimensions[tbin];
(*Key numerica per la criptazione del messaggio di testo*)
keycif = {"3"};
keynum = ToExpression[Characters[keycif][[1]]];

(*Funzione per il prolungamento dei file di testo nel formato dell'immagine*)
perex[tab_, n_, m_] := Table[tab[[1 + Mod[k + h, Length[tab]]]], {k, 0, n}, {h, 0, m}];
```

N.B.: in questa fase, prima di eseguire il programma al variare di *keycif*, è necessario commentare la parte di codice sotto la riga indicata inserendo i caratteri (\*

```
mtab = Table[Round[255 * tbin[[k, h, 1]] + imgkey[[
FromCharCode[mtab[[1]]]
(*
(*Inseriamo le chiavi pubbliche e private e l'
ekeyset=1319;
dkeyset=1559;
enneset=1769;
```

A questo punto la risposta alla prima domanda è il valore

numerico da assegnare a *ekeyset*, mentre la risposta alla seconda è il valore per *dkeyset*! Adesso manca soltanto *enneset*!!

4- Per trovare *enneset* dovete decodificare con *VigenereDecode.exe* la stringa che trovate dentro il file di testo "*domandaNset.txt*" utilizzando come chiavi possibili i nomi dei componenti del gruppo. Solo con uno dei nomi viene riprodotta una domanda, la risposta alla quale è il valore numerico da impostare su *enneset*. A questo punto avendo le tre chiavi possiamo far girare l'intero programma (togliete i caratteri (\* inseriti al punto 3) sull'immagine criptata ed ottenere così la figura cercata.

5- Inviare il file, decrittato secondo i precedenti passaggi, all'indirizzo [michele.brizi@liceorecanati.org](mailto:michele.brizi@liceorecanati.org)