Algoritmi Genetici per la decrittazione di testi

Questo pacchetto software permette la decrittazione di testi in lingua inglese, codificati usando un cifrario monoalfabetico a permutazione o un cifrario polialfabetico di Vigenère, mediante l'uso di algoritmi genetici. É composta da 4 diversi moduli scritti in Python3, ciascuno dotato di un *main* e quindi eseguibile singolarmente, più un file di dati contenete le percentuali di apparizione di bigrammi, necessario il calcolo della funzione di fitness (tratto da https://blogs.sas.com/content/iml/files/2014/09/bigrams.txt).
L'esecuzione di uno qualsiasi dei moduli richiede come input il nome del file con il testo criptato e restituisce un nuovo file con il testo decrittato.

genalgo_keyfixed.py

Questo script permette di decifrare un testo criptato con la codifica polialfabetica, conoscendo la lunghezza della chiave usata (una parola).
Il programma accetta i seguenti argomenti (quelli indicati con $'--'$ sono opzionali):

- *filename*: nome del file con il testo criptato
- *popsize*: numero di individui della popolazione
- *keysize*: numero di lettere nella chiave
- *ngen*: numero di generazioni
- $--$*pelite*: frazione della popolazione salvata per elitismo
- $--$*pxover*: probabilità di eseguire il crossover
- $--$*mutprob*: probabilità di mutazione
- $--$*randseed*: seme per il generatore di numeri casuali
- $--$*cores*: numero di cores su cui viene lanciato il programma

genalgo_permutation.py

Questo script permette di decifrare un testo criptato con un cifrario monoalfabetico a permutazione, utilizzando un alfabeto composto solo dalle 26 lettere minuscole e senza il carattere *spazio*.
Il programma accetta i seguenti argomenti (quelli indicati con $'--'$ sono opzionali):

- *filename*: nome del file con il testo criptato
- *popsize*: numero di individui della popolazione
- *ngen*: numero di generazioni
- $--$*pelite*: frazione della popolazione salvata per elitismo
- $--$*pxover*: probabilità di eseguire il crossover
- $--$*mutprob*: probabilità di mutazione
- $--$*randseed*: seme per il generatore di numeri casuali
- $--$*cores*: numero di cores su cui viene lanciato il programma

genalgo_key.py

Questo script permette di decifrare un testo criptato con la codifica polialfabetica senza inserirela lunghezza esatta della chiave, che cercata in un range (specificabile dall'utente). Il programma accetta i seguenti argomenti (quelli indicati con $'--'$ sono opzionali):

- *filename*: nome del file con il testo criptato
- *popsize*: numero di individui iniziali per ciascuna sotto-popolazione
- *ngen*: numero di generazioni
- $--$*pelite*: frazione della popolazione salvata per elitismo
- $--$*pxover*: probabilità di eseguire il crossover
- $--$*mutprob*: probabilità di mutazione
- $--$*randseed*: seme per il generatore di numeri casuali
- $--$*klmin*: minima lunghezza di chiave utilizzata
- $--$*klmax*: massima lunghezza di chiave utilizzata
- $--$*cores*: numero di cores su cui viene lanciato il programma

genalgo_all.py

Questo script è pensato come l'unione dei due precedenti, in quanto permette di decrittare un testo in cui non sia noto il tipo di crittografia utilizzato (Vigenere/permutazione). Il programma permette di trattare in modo diverso la popolazione usata per la parte polialfabetica e quella per la parte monoalfabetica, che altrimenti sono inizializzate con gli stessi parametri, e accetta i seguenti argomenti (quelli indicati con $'--'$ sono opzionali

- *filename*: nome del file con il testo criptato
- *popsize*: numero di individui per ciascuna sotto-popolazione
- *ngen*: numero di generazioni
- $--$*popsize_perm*: numero di individui per la popolazione monoalfabetica
- $--$*pelite*: frazione della popolazione salvata per elitismo
- $--$*pxover*: probabilità di eseguire il crossover
- $--$*mutprob*: probabilità di mutazione
- $--$*mutprob_perm*: probabilità di mutazione (popolazione monoalfabetica)
- $--$*randseed*: seme per il generatore di numeri casuali
- $--$*klmin*: minima lunghezza di chiave utilizzata
- $--$*klmax*: massima lunghezza di chiave utilizzata
- $--$*cores*: numero di cores su cui viene lanciato il programma