Si vuole progettare e realizzare un programma che consente di criptare e decriptare un testo. I metodi di criptazione posso essere di vari tipi: per trasposizione, per sostituzione…
Ogni utente deve poter:

- scegliere se criptare o decriptare
- inserire una stringa
- scegliere il metodo
- settare le impostazioni o la chiave desiderata
- ottenere in output la stringa desiderata

Il programma deve inoltre avere una parte dedicata alla storia e alla spiegazione dei metodi usati, si desidera quindi la possibilità di:

- selezionare il metodo
- ottenere in output la storia e la spiegazione del funzionamento

Deve essere presente anche un'introduzione generale alla criptologia in questa porzione di programma.

Il metodo per spostamento in generale trasforma un carattere in un altro traslandolo di “n” posizioni. Questo metodo è esteso da vari altri metodi come per esempio il Codice Cesare che traspone di una posizione tutte le lettere e non traspone gli altri caratteri, si basa sull'algebra modulare.

Il metodo per sostituzione in generale trasforma un carattere in un qualsiasi simbolo scelto a discrezione dall'utente. Questo metodo è specificato meglio in vari altri metodi come per esempio il codice Morse.

Il programma deve anche prevedere l'aggiunta di molti altri metodi di criptazione.
Lo scopo principale del programma è di essere utile a chi vuole introdursi al mondo della criptologia che sia in ambito storico o in ambito matematico-tecnico e iniziarne gli studi, può trovare anche un ampio utilizzo per chi per gioco vuole criptare o decriptare alcuni semplici messaggi.