2018-05-07 Crittografia (cifrari monoalfabetici)

***Cifrario di Cesare***

Svetonio nella Vita dei Cesari racconta che Giulio Cesare usava per le sue corrispondenze riservate un cifrario monoalfabetico molto semplice: ogni lettera viene sostituita dalla lettera che la segue di tre posti nell'alfabeto:

* la lettera A è sostituita dalla D
* la B dalla E
* per le ultime lettere si procede circolarmente ricominciando dalla A

Chiaro ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cifrato DEFGHIJKLMNOPQRSTUVWXYZABC

1. Scrivere l’applicazione (***pasw00901a.cpp***) che dato il file di testo **testoInChiaro.txt** genera il file di testo **testoCifrato.txt** applicando il metodo di cifratura di Cesare ai soli caratteri alfabetici minuscoli e maiuscoli lasciando inalterati gli altri caratteri.
2. Scrivere l’applicazione (***pasw00901b.cpp***) che decodifica il file di testo **testoCifrato.txt** ottenuto applicando l’applicazione precedente e genera il file **testoInChiaro.txt**
3. Scrivere l’applicazione (***pasw00901c.cpp***) che dato il file di testo **testoInChiaro.txt** genera il file di testo **testoCifrato.txt** applicando un metodo di cifratura analogo a quello di Cesare ai soli caratteri alfabetici minuscoli e maiuscoli. Il metodo di cifratura richiede in input un valore intero **n** (***2≤n≤25***) che rappresenta lo “spostamento” circolare di ogni lettera nell’alfabeto.
4. Scrivere l’applicazione (***pasw00901d.cpp***) che tenta di decodificare il file **testoCifrato.txt** crittato con l’applicazione precedente senza conoscere il valore di **n**.  
   La decodifica avviene per tentativi assegnando in successione valori a **n** e visualizzando le prime 10 righe del testo decrittato in questo modo fino a quando l’utente segnala che il valore di n è corretto per la decodifica che prosegue salvando l’intero file decrittato **testoInChiaro.txt**.
5. Modificare l’applicazione precedente (***pasw00901e.cpp***) calcolando la frequenza massima delle lettere del file crittato e calcolando un possibile valore di n utilizzando la tabella di frequenza qui riportata.

|  |  |  |  |
| --- | --- | --- | --- |
| **Italiano** | | **Inglese** | |
| E | 11,79 | E | 12,31 |
| A | 11,74 | T | 9,59 |
| I | 11,28 | A | 8,05 |
| O | 9,83 | O | 7,94 |
| N | 6,88 | N | 7,19 |