Esercizio Esonero 2019/2020

Programmazione I con Laboratorio

Canali per le domande: ricevimento, email: francesco.santini@unipg.it, Telegram: @safran

1 Cifrario di Cesare

In crittografia il cifrario di Cesare è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.[1]

Come è noto, Giulio Cesare usava, nel corso delle varie guerre, comunicare attraverso dispacci cifrati. Il codice usato da Cesare era un semplice cifrario di sostituzione dove le lettere alfabetiche differivano di una costante (chiave k) dalle lettere codificate in chiaro. In Figura 1 un esempio con $k = 3$ (intendiamo sempre uno spostamento verso destra). Seguendo questo esempio, la stringa "ciao" viene cifrata in "fldr".

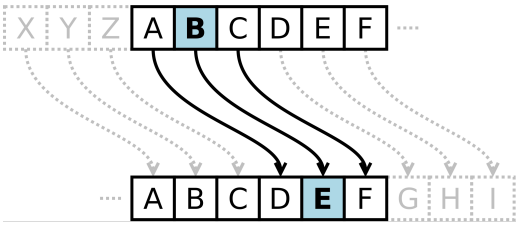

Figura 1. Cifrario di Cesare, spostando ogni lettera di 3 posizioni [Fonte Wikipedia].

2 Cifrario a Sostituzione (Alfabeto Mescolato)

La sostituzione operante su singole lettere, detta sostituzione semplice, si applica utilizzando un altro alfabeto scritto con le lettere disposte in un certo ordine detto alfabeto per la sostituzione. Questo può essere preparato ruotando od invertendo l'alfabeto (creando così, rispettivamente, il cifrario di Cesare in Sezione 1, ed il cifrario Atbash) oppure mescolando le lettere secondo un ordine prestabilito: in quest'ultimo caso si parla di *alfabeto mescolato* o *alfabeto squilibrato*. Tradizionalmente gli alfabeti mescolati sono creati scrivendo prima una parola chiave (la k in questo caso).[2]

[1] Più notizie disponibili su `https://it.wikipedia.org/wiki/Cifrario_di_Cesare`.

[2] Cifrari a sostituzione: `https://it.wikipedia.org/wiki/Cifrario_a_sostituzione`.

```
char stringa[256];
fgets(stringa, sizeof(stringa), stdin);
```

Figura 2. Esempio per definire la stringa da leggere e leggere la stringa da tastiera con *fgets*.

Per esempio, dato l'alfabeto del testo in chiaro "abcdefghijklmnopqrstuvwxyz" e l'alfabeto mescolato "ZEBRACDFGHIJKLMNOPQSTUVWXY", la stringa cifrata corrispondente a "Fuggire, siamo stati scoperti!" è "CTDDGPA, QGZKM QSZSG QBMNAPSG!", ottenuta sostituendo ogni lettera del messaggio in chiaro con la lettera corrispondente nell'alfabeto mescolato.

3 Esercizio

Scrivere un programma su un file singolo di nome *string_cripto.c* che per prima cosa prende in input da tastiera una stringa (in gergo *plaintext*); fare riferimento alla Figura 2 per la dimensione massima della stringa e come leggerla.

A questo punto all'utente deve essere chiesto se vuole cifrarla con (uno dei due a scelta):

- Il cifrario di Cesare;
- Il cifrario a sostituzione (alfabeto mescolato).

Se l'utente richiede il cifrario di Cesare, prendere in input da tastiera la chiave k, e poi restituire in output la stringa cifrata (*printf*). In gergo, il risultato della cifratura è chiamato *cyphertext*. Se l'utente richiede la cifratura a sostituzione, richiedere l'alfabeto mescolato all'utente, e poi successivamente restituire in output il cyphertext. Supporre in ciascuno dei due casi di utilizzare l'alfabeto inglese (26 lettere), e di utilizzare stringhe solo di lettere minuscole. I caratteri differenti da questi devono essere lasciati inalterati (per esempio il "!" o lo spazion nell'esempio in Sezione 2). Controllare che l'alfabeto mescolato passato dall'utente (secondo caso) contenga tutte e sole le 26 lettere dell'alfabeto.

4 Sottomissione

Si accettano solo sottomissioni attraverso GitHub all'indirizzo `https://classroom.github.com/a/0WhgfLv-`. È necessario creare un account GitHub quindi. Dato che l'utilizzo di GitHub fa parte dell'esercizio, lo studente deve essere in grado di verificare da solo se l'upload ha avuto successo o meno (non si accettano domande in questo senso). La scadenza per la sottomissione è **Domenica 17 Novembre** (23:59). Nel file README.md del repository aggiungere 1) nome, 2) cognome e 3) matricola (seguire le istruzioni sul file README). L'esonero sarà valutato con SÌ o NO. In caso di mancata sottomissione, o di risposta NO come risultato, in sede di esame orale saranno chieste una o più domande aggiuntive.