

CORSO di LAUREA in **INFORMATICA**  
Corso di  
**PROGRAMMAZIONE I e LABORATORIO PROGRAMMAZIONE I**  
(12 CFU)  
A.A. 2020-21

Docenti: Proff. Angelo Ciaramella e Giulio Giunta

Cognome: Spinosa  
Nome: Riccardo Andrea  
Matricola: 0124/2253

**PROGETTO D'ESAME DI LABORATORIO**

1. Cifratura-decifratura.

Sviluppare una coppia di algoritmi, implementati come function, per crittografare e decrittografare un messaggio. L'algoritmo si basa sulla cosiddetta cifratura polialfabetica, che consiste nel trasformare il messaggio in un testo di lunghezza uguale a quella del messaggio, detto il "testo cifrato", utilizzando un altro testo (prefissato), detto "il testo delle lettere chiave". Ogni lettera del messaggio viene trasformata in una lettera del testo cifrato nel seguente modo: la lettera del messaggio viene sostituita dalla lettera dell'alfabeto successiva, se la corrispondente lettera chiave (nel testo delle lettere chiave) è B, da quella due volte successiva se la lettera chiave è C, da quella 3 volte successiva se la lettera chiave è D e così via; se la lettera chiave è A, la lettera del messaggio non viene modificata. L'alfabeto deve essere considerato come circolare, nel senso che la lettera successiva alla lettera Z è la lettera A. Per esempio, se il messaggio è THEPRESIDENT allora se il testo delle parole chiave è CODECODECODE allora il messaggio cifrato è VVHTTSVMFSQX; si osservi che in generale il testo delle lettere chiave si ottiene a partire da una parola chiave ripetuta più volte (CODE nel caso in esame). La corrispondenza: lettera del messaggio - lettera del testo cifrato - lettera chiave è evidente scrivendo i tre testi nel seguente modo (alfabeto:ABCDEFGHIJKLMNOPQRSTUVWXYZ)

chiave	C	O	D	E	C	O	D	E	C	O	D	E
messaggio	T	H	E	P	R	E	S	I	D	E	N	T
testo cifrato	V	V	H	T	T	S	V	M	F	S	Q	X

Il main legge da tastiera il messaggio da crittografare (l'equivalente di THEPRESIDENT nell'esempio), legge da tastiera la parola chiave (l'equivalente di CODE nell'esempio; osservate che non è necessario leggere tutto il testo delle parole chiavi, perché questo può essere ottenuto a partire dalla parola chiave), chiama la function di cifratura (passando come parametro il messaggio e la parola chiave), che restituisce il testo cifrato, visualizza il testo cifrato, chiama la function di decifratura, passando come parametro il testo cifrato e la parola chiave, visualizza il messaggio decifrato, che deve coincidere con il messaggio di partenza. Usare solo lettere maiuscole e non usare la spaziatura. Usare le stringhe per rappresentare tutti i tipi di testo e le function in **string** (serve solo la **strlen**). E' utile sapere che in C, è possibile sommare "sommare i caratteri" sfruttando il fatto che il codice ASCII rappresenta i caratteri come interi e che a lettere consecutive corrispondono interi consecutivi (consiglio: determinate qual è la

rappresentazione ASCII di A e poi “sottraetela” dalla rappresentazione di ogni lettera per sapere qual è la “posizione” di ogni lettera nell’alfabeto.). Fare una versione alternativa del main, in cui la parola chiave è una 5-stringa generata a caso, usando la function **rand()**, il cui prototipo è in **<stdlib.h>**, per generare gli interi casuali. Si ricorda che, se **numero\_casuale** è dichiarata di tipo **int**, allora la chiamata **numero\_casuale=rand()%(n+1);** genera un numero casuale intero (distribuzione uniforme) nell’insieme (0,1,2,..n). Usare sempre la **srand()** per rendere automatica la scelta iniziale del *seed* della sequenza di numeri casuali. Nella Relazione si deve riportare l’analisi della complessità di tempo dell’algoritmo (operazione dominante: confronto)

## 2. Gestione archivio telefonico

Si vuole simulare l’archivio telefonico di un cellulare. Ogni nominativo è identificato dal *Cognome*, *Nome*, *numero telefonico*. Provvedere all’implementazione dell’algoritmo per la simulazione dell’archivio telefonico (massimo 30 nominativi). Permettere, inoltre, all’utente di

- Inserire o cancellare un nominativo
- Dato il Cognome e il Nome di un utente visualizzare il numero telefonico corrispondente (effettuare una ricerca binaria ricorsiva)
- Dato un numero telefonico vedere il numero totale di chiamate da e verso quel numero

L’archivio può anche essere inizializzato con informazioni casuali. Effettuare almeno due test per ognuna delle opzioni dell’utente.

### ATTENZIONE – LEGGERE ATTENTAMENTE

La prova d’esame di laboratorio richiede il progetto degli algoritmi e la loro implementazione come programmi C.

Tutti i programmi devono contenere

- un insieme di commenti iniziali che spiega brevemente le finalità del programma;
- un insieme di commenti all’inizio di ogni function che spiega le finalità della function e il significato dei parametri di input output (*specifiche* della function);
- commenti esplicativi dei principali blocchi di istruzioni;

e devono essere corredati da

- un insieme di almeno **3 esecuzioni** per testare il programma con diversi dati di input.

Lo studente deve consegnare al docente una **UNICA** relazione organizzata come **documento multimediale**. In particolare deve essere inviata per e-mail al docente una **UNICA** cartella (zippata) denominata **Relazione\_Cognome\_Nome.zip**.

La **cartella** deve contenere:

- un file **index.html** che è il documento multimediale;

- una cartella **images** che contiene le immagini del documento multimediale;
- una cartella **C** contenente i file sorgente del progetto (**.c**, **.h**);
- il testo della prova inviata dal docente in formato **.pdf** ;
- altre cartelle eventualmente generate per il documento.

La **relazione** deve contenere necessariamente almeno

- il testo della prova inviata dal docente;
- il testo dei programmi C (sorgente);
- l'output e la descrizione dei test di esecuzione.

I **test devono essere almeno tre per ogni programma**, devono essere salvati come *"print screen"* e come figure nel documento multimediale. Devono essere corredati da una descrizione per l'interpretazione dei risultati del test.

La relazione deve riportare chiaramente il nome e cognome dell'allievo e la sua matricola.

La relazione deve essere inviata al docente per e-mail (**angelo.ciaramella@uniparthenope.it**) entro la data di scadenza della prenotazione on-line dell'esame e deve essere inviata esclusivamente dall'indirizzo e-mail personale dello studente (**nome.cognome@studenti.uniparthenope.it**).

IL NOME DELLA CARTELLA CHE CONTIENE LA RELAZIONE DEVE ESSERE **Relazione\_cognomeallievo\_nomeallievo.zip**

**NON SARANNO ESAMINATI PROGETTI DIFFORMI DA QUANTO PRECISATO.**