Progetto Assembly RISC-V

Corso di Architetture degli Elaboratori

a.a 2021/2022

Messaggi in Codice

Autore:

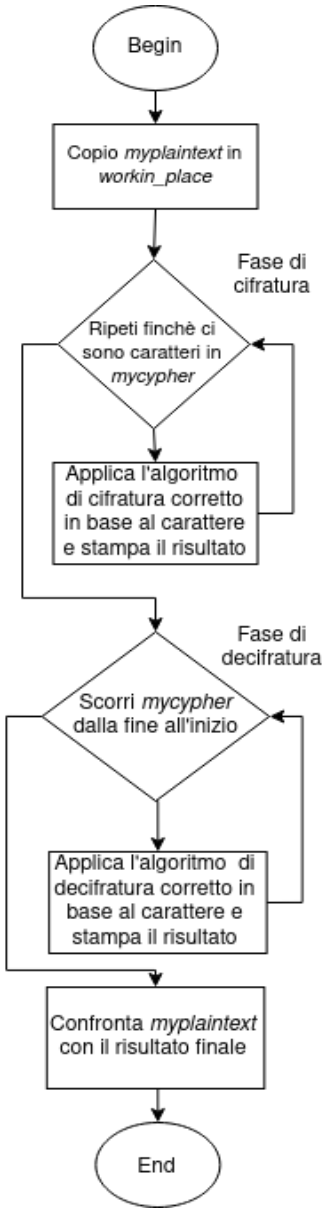
Lorenzo Bartolini
Matricola: **7073016**
Mail: *lorenzo.bartolini8@stud.unifi.it*

Consegnato in data

Abstract

Il progetto richiede di scrivere un programma in Assembly RISC-V che applichi in cascata una sequenza di algoritmi di cifratura ad una stringa fornita come parametro.
In input vengono fornite due stringhe: la stringa da cifrare (myplaintext) e la sequenza di algoritmi da usare (mycypher).
Una volta cifrato il messaggio è richiesto di decifrarlo per tornare alla stringa in chiaro da cui è stato inizializzato il programma.
Ho organizzato il programma con una procedura separata per ogni algoritmo e, dove necessario, ho separato la fase di cifratura da quella di decifratura. Ho unito il tutto all'interno della procedura Main che funge anche da entrypoint del programma.

Main



Inizialmente copio il contenuto di *myplaintext* in una nuova posizione di memoria, puntata dalla variabile *working_place*. Questo per dei problemi legati alla dimensione della stringa durante l'esecuzione dell'algoritmo ad Occorrenze, infatti in tutti gli altri casi la dimensione della stringa rimane invariata e non crea problemi ma in caso la dimensione varia e rischia di sovrascrivere porzioni di memoria contenenti altre informazioni. Non sovrascrivere *myplaintext s*erve anche come reference alla fine degli algoritmi per verificare il corretto funzionamento del programma.
Procedo scorrendo la stringa *mycypher* e applico, su *working_place*, per ogni carattere della stringa l'algoritmo che gli corrisponde. Dopo ogni algoritmo stampo a video il risultato parziale che ho appena calcolato.
Una volta terminato di scorrere la stringa significa che ho cifrato la stringa usando tutti gli algoritmi richiesti in cascata.
A questo punto scorro *mycypher* al contrario, tramite l'indice che ho usato precedentemente, e per ogni carattere applico la versione per la decifratura dell'algoritmo corrispondente. Come per la fase di cifratura stampo a video il risultato parziale.
Una volta terminata l'esecuzione stampo la stringa originale, ovvero il *myplaintext* intatto, e quella che ha subito gli algoritmi di cifratura e decifratura.

esempio di esecuzione usando due diversi algoritmi

```
Cifrato usando: Algoritmo di Cesare (A)
Uftu_Sfmbajpof_BEF_2021_2022

Cifrato usando: Algoritmo a Blocchi (B)
dry$kXuygpvu~rdQQKn>5A=dA<7A

Decifrato usando: Algoritmo a Blocchi (B)
Uftu_Sfmbajpof_BEF_2021_2022

Decifrato usando: Algoritmo di Cesare (A)
Test_Relazione_ADE_2021_2022



Decifrato: Test_Relazione_ADE_2021_2022
Originale: Test_Relazione_ADE_2021_2022
```