Scuola di Scienze Matematiche, Fisiche e Naturali Corso di Laurea in Informatica

Progetto Assembly RISC-V per il Corso di Architetture degli Elaboratori – A.A. 2021/2022

–

Messaggi in Codice

1. Informazioni sull'autore

- Autore: Vannacci Serena
- Indirizzo: serena.vannacci@stud.unifi.it
- Matricola: 7030223

- Data di consegna: 02/01/2023

2. Descrizione della soluzione adottata

Main:

Carico l'indirizzo di myplaintext e di mycypher rispettivamente nei registri a1 e s0, stampo myplaintext (caricando l'indirizzo di myplaintext anche in a0) e salvo i valori ASCII delle singole lettere (A, B, C, D, E) corrispondenti alle diverse modalità di cifratura nei registri da s1 a s5.

Svolgo un controllo sulla lunghezza di myplaintext e sul contenuto dei simboli di myplaintext il cui codice ASCII deve essere compreso tra 32 e 127 (estremi inclusi). Per tale compito utilizzo dei registri temporanei: t0 per il conteggio della lunghezza della stringa, t1 e t3 per confrontare i simboli della stringa con gli estremi dell'intervallo a cui devono appartenere, infine t2 per caricare il simbolo corrente della stringa salvata in a1.

Sulla base dei simboli contenuti in mycypher proseguo facendo una sequenza di confronti con i valori ASCII contenuti nei registri da s1 a s5 per selezionare quale cifratura utilizzare.

Lo stesso tipo di procedimento viene implementato per la selezione degli algoritmi di decifrazione (eseguito solo dopo aver terminato la lettura di mycypher), leggendo mycypher a partire dall'ultimo simbolo fino a quello iniziale.

In entrambi i casi utilizzo il registro temporaneo t0 per caricare il simbolo corrente di mycypher.

L'etichetta Stampa contrassegna la parte di codice che visualizza sulla console i risultati finali dell'esecuzione delle procedure di cifratura e decifrazione.

Cifrario a Sostitizione:

Se in mycypher è presente il codice ASCII di A, verrà scelta la procedura per la cifratura o la decifrazione, in base a che punto della lettura di

mycypher il programma si trova. Per tale finalità si utilizza il registro temporaneo t3, caricato con 0 per la cifratura e con 1 per la decifrazione.

Il codice è parzialmente identico per entrambe le scelte, viene inizialmente caricata la costante intera per effettuare la sostituzione in t1 (key_Sostituizione), salvato in t0 l'indirizzo iniziale della parte di memoria dove verrà salvato il risultato, e caricato in t4 il valore del modulo.

A seconda della presenza di un carattere minuscolo o maiuscolo verranno fatte delle operazioni diverse, come quelle illustrate nella comanda del progetto, per eseguire la trasformazione e poi sarà salvato il simbolo trasformato. Le operazioni vengono svolte utilizzando i registri temporanei (da t1 a t6).

Per la decifrazione vengono attuati dei piccoli cambiamenti durante le operazioni di trasformazione del simbolo per farlo tornare al valore pre-cifratura corretto.

Infine si procede alla stampa della stringa ottenuta.

Cifrario a Blocchi:

Se in mycypher è presente il codice ASCII di B, verrà scelta la procedura per la cifratura o la decifrazione, in base a che punto della lettura di mycypher il programma si trova. Per tale finalità si utilizza il registro temporaneo t3, caricato con 0 per la cifratura e con 1 per la decifrazione.

Il codice è parzialmente identico per entrambe le scelte, viene inizialmente caricata la stringa che rappresenta la chiave di codifica per i blocchi in a3, salvato in t0 l'indirizzo iniziale della parte di memoria dove verrà salvato il risultato, e inizializzato un contatore per la chiave in t1.

Per ogni simbolo vengono effettuate le stesse operazioni, come quelle illustrate nella comanda del progetto, per eseguirne la trasformazione e poi si procede salvando il simbolo trasformato. Le operazioni vengono svolte utilizzando i registri temporanei (da t1 a t6).

Per la decifrazione si fanno delle operazioni di trasformazione del simbolo per farlo tornare al valore pre-cifratura corretto.

Infine si procede alla stampa della stringa ottenuta.

Cifratura Occorrenze:

Se in mycypher è presente il codice ASCII di C, verrà scelta la procedura per la cifratura o la decifrazione, in base a che punto della lettura di mycypher il programma si trova.

Il codice è diverso per le due procedure.

Per la cifratura inizializzo in t0 il contatore per la posizione delle occorrenze, calcolo l'indirizzo dove salvare la stringa trasformata, e in a3 salvo l'indirizzo iniziale di tale parte di memoria. Inoltre mi salvo in t5 una costante negativa che mi rappresenta l'occorrenza già letta.

Utilizzo lo stack per salvare il valore calcolato fino a quel momento di t0 e l'indirizzo del simbolo successivo, contenuto in a0, per poi recuperarlo dopo aver terminato di scandagliare la stringa alla ricerca delle occorrenze.

Se il simbolo in t2 è uguale a quello contenuto in t5 vado avanti al simbolo successivo, altrimenti lo salvo, seguito dal simbolo ASCII del trattino (-) e dalle sue occorrenze trasformate opportunamente in codice ASCII, lasciando uno spazio tra il simbolo attualmente in t2 e il successivo.

Ogni occorrenza trovata nella stringa in input viene modificata in una costante negativa (-1).

Salvo in t0 l'indirizzo iniziale di a2, ed infine si procede alla stampa.

Per la decifrazione calcolo l'indirizzo dove salvare la stringa trasformata, e in t0 salvo l'indirizzo iniziale di tale parte di memoria.

Leggo il simbolo e lo salvo in t4 se non corrisponde al codice ASCII del trattino (-). Essendoci anche la possibilità di un trattino nella stringa iniziale, faccio un controllo e se ne trovo due di fila, allora lo salvo in t4 e procedo a calcolare le posizioni in cui si trovano le occorrenze.

Infine si procede alla stampa della stringa ottenuta.

Dizionario:

Se in mycypher è presente il codice ASCII di D, verrà scelta la procedura per la cifratura o la decifrazione, in base a che punto della lettura di mycypher il programma si trova.

Il codice è identico per entrambe le scelte, viene inizialmente salvato in t0 l'indirizzo iniziale della parte di memoria dove verrà salvato il risultato.

In base alla tipologia di simbolo, ovvero lettere minuscole, maiuscole o numeri, vengono eseguite operazioni diverse, come quelle illustrate nella comanda del progetto, per ottenerne la trasformazione e poi si continua con il salvataggio del simbolo trasformato. Le operazioni vengono svolte utilizzando i registri temporanei (da t2 a t6).

Infine si procede alla stampa della stringa ottenuta.

Inversione:

Se in mycypher è presente il codice ASCII di E, verrà scelta la procedura per la cifratura o la decifrazione, in base a che punto della lettura di mycypher il programma si trova.

Il codice è identico per entrambe le procedure, viene inizialmente calcolato l'indirizzo iniziale della parte di memoria dove verrà salvato il risultato e caricato in a2.

Per ottenere la stringa invertita si salvano all'inverso i simboli di a0 in a2, dopodiché prima della stampa viene salvato in t0 l'indirizzo corretto della stringa trasformata.

Infine si procede alla stampa della stringa ottenuta.

Fine:

Parte di codice che segnala la terminazione del programma stampando sulla console la stringa "Termine programma".

2. Test di corretto funzionamento

mycypher: "ABCCDE"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
Vyj",V"~m"-D<>5A?
V-1-6 y-2 j-3 "-4-7-10 ,-5 ~-8 m-9 --11 D-12 <-13 >-14 5-15 A-16 ?-17
V-1 --2-4-8-12-16-18-20-25-29-33-36-37-42-47-52-57-62-67 1-3-21-38-39-43-48-53-58-63-68 6-5-64  -6-10-14-23-27-31-35-40-45-50-55-60-65-70 y-7 2-9-44 j-11 3-13-49 "-15 4-17-54
7-19-69 0-22 ,-24 5-26-56-59 ~-28 8-30 m-32 9-34 D-41 <-46 >-51 A-61 ?-66
e-8 --7-5-1-87-83-81-79-74-70-66-63-62-57-52-47-42-37-32 8-6-78-61-60-56-51-46-41-36-31 3-4-35  -3-89-85-76-72-68-64-59-54-49-44-39-34-29 B-2 7-0-55 Q-88 6-86-50 "-84 5-82-45
2-80-30 9-77 ,-75 4-73-43-40 ~-71 1-69 N-67 0-65 w-58 <-53 >-48 z-38 ?-33
 33-? 83-z 84-> 35-< 85-w 56-0 76-N 96-1 17-~ 04-34-37-4 57-, 77-9 03-08-2 54-28-5 48-" 05-68-6 88-Q 55-0-7 2-B 92-43-93-44-94-45-95-46-86-27-67-58-98-3-  53-4-3
13-63-14-64-15-65-06-16-87-6-8 23-73-24-74-25-75-26-36-66-07-47-97-18-38-78-1-5-7-- 8-e
e-8 --7-5-1-87-83-81-79-74-70-66-63-62-57-52-47-42-37-32 8-6-78-61-60-56-51-46-41-36-31 3-4-35  -3-89-85-76-72-68-64-59-54-49-44-39-34-29 B-2 7-0-55 Q-88 6-86-50 "-84 5-82-45
2-80-30 9-77 ,-75 4-73-43-40 ~-71 1-69 N-67 0-65 w-58 <-53 >-48 z-38 ?-33
V-1 --2-4-8-12-16-18-20-25-29-33-36-37-42-47-52-57-62-67 1-3-21-38-39-43-48-53-58-63-68 6-5-64  -6-10-14-23-27-31-35-40-45-50-55-60-65-70 y-7 2-9-44 j-11 3-13-49 "-15 4-17-54
7-19-69 0-22 ,-24 5-26-56-59 ~-28 8-30 m-32 9-34 D-41 <-46 >-51 A-61 ?-66
V-1-6 y-2 j-3 "-4-7-10 ,-5 ~-8 m-9 --11 D-12 <-13 >-14 5-15 A-16 ?-17
Vyj",V"~m"-D<>5A?
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: "ABCDE"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
Vyj",V"~m"-D<>5A?
V-1-6 y-2 j-3 "-4-7-10 ,-5 ~-8 m-9 --11 D-12 <-13 >-14 5-15 A-16 ?-17
e-8-3 B-7 Q-6 "-5-2-89 ,-4 ~-1 N-0 --88 w-87 <-86 >-85 4-84 z-83 ?-82
 28-? 38-z 48-4 58-> 68-< 78-w 88-- 0-N 1-~ 4-, 98-2-5-" 6-Q 7-B 3-8-e
e-8-3 B-7 Q-6 "-5-2-89 ,-4 ~-1 N-0 --88 w-87 <-86 >-85 4-84 z-83 ?-82
V-1-6 y-2 j-3 "-4-7-10 ,-5 ~-8 m-9 --11 D-12 <-13 >-14 5-15 A-16 ?-17
Vyj",V"~m"-D<>5A?
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: "ADE"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
tNVH jHISH!?-7976
6797-?!HSIHj HVNt
tNVH jHISH!?-7976
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: "ADEADE"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
tNVH jHISH!?-7976
6797-?!HSIHj HVNt
6797-?!LWMLn LZRx
3202-?!odnoM oaiC
Ciao Mondo!?-2023
3202-?!odnoM oaiC
6797-?!LWMLn LZRx
6797-?!HSIHj HVNt
tNVH jHISH!?-7976
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: "C"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
C-1 i-2 a-3 o-4-7-10  -5 M-6 n-8 d-9 !-11 ?-12 --13 2-14-16 0-15 3-17
Ciao Mondo!?-2023
Termine programma
```

mycypher: "DEDD"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
xRZL nLMWL!?-7976
6797-?!LWMLn LZRx
3202-?!odnoM oaiC
6797-?!LWMLn LZRx
3202-?!odnoM oaiC
6797-?!LWMLn LZRx
xRZL nLMWL!?-7976
Ciao Mondo!?-2023
Termine programma
```

mycypher: "ABC"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
Vyj",V"~m"-D<>5A?
V-1-6 y-2 j-3 "-4-7-10 ,-5 ~-8 m-9 --11 D-12 <-13 >-14 5-15 A-16 ?-17
Vyj",V"~m"-D<>5A?
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: "AEC"
myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
Gmes Qsrhs!?-2023
3202-?!shrsQ semG
3-1 2-2-4 0-3 --5 ?-6 !-7 s-8-11-14 h-9 r-10 Q-12  -13 e-15 m-16 G-17
3202-?!shrsQ semG
Gmes Qsrhs!?-2023
Ciao Mondo!?-2023
Termine programma
```

mycypher: " ECDE"

myplaintext: "Ciao Mondo!?-2023"

```
Ciao Mondo!?-2023
3202-?!odnoM oaiC
3-1 2-2-4 0-3 --5 ?-6 !-7 o-8-11-14 d-9 n-10 M-12  -13 a-15 i-16 C-17
6-8 7-7-5 9-6 --4 ?-3 !-2 L-1-88-85 W-0 M-89 n-87  -86 Z-84 R-83 x-82
 28-x 38-R 48-Z 68-  78-n 98-M 0-W 58-88-1-L 2-! 3-? 4-- 6-9 5-7-7 8-6
6-8 7-7-5 9-6 --4 ?-3 !-2 L-1-88-85 W-0 M-89 n-87  -86 Z-84 R-83 x-82
3-1 2-2-4 0-3 --5 ?-6 !-7 o-8-11-14 d-9 n-10 M-12  -13 a-15 i-16 C-17
3202-?!odnoM oaiC
Ciao Mondo!?-2023
Termine programma
```