Corso di Laurea in Ingegneria Informatica

Calcolatori — a.a. 2022–2023

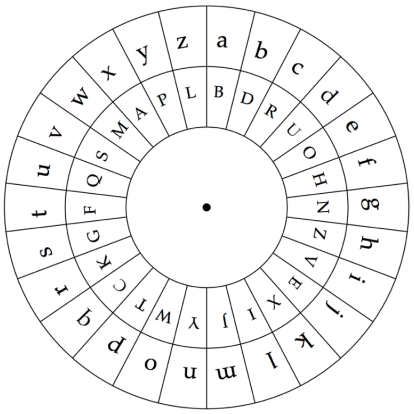
Scritto A del 10 febbraio 2023

(completamento della prova in itinere del 5/11/2022)

Cognome e Nome dello studente: _____

Alberti dischi (dal 1467)

Nel 1467 Leon Battista Alberti descrisse nel trattato De componendis cifris *uno dei primi sistemi di cifratura polialfabetica. Il sistema (vedi figura) è composto da una coppia di dischi concentrici, dei quali quello interno può ruotare rispetto a quello esterno, fisso.*



Il disco esterno riporta le 26 lettere minuscole in ordine alfabetico, quello interno le maiuscole in ordine casuale. Il cifratore e il destinatario devono utilizzare la stessa coppia di dischi, e condividere una chiave $\ell\mathcal{S}$*, dove* ℓ *è una lettera dell'alfabeto interno detta* lettera indice*, e* $\mathcal{S} = s_1 s_2 \dots s_n$ *è una parola di* n *interi detta* parola degli scorrimenti*. Supponiamo di voler cifrare il testo "Incontriamoci alle tre", di avere scelto la chiave D1020043, e posizionato i dischi come in figura. Allora la prima lettera del messaggio cifrato sarà quella che sul disco esterno corrisponde alla lettera indice D, cioè* **b**.

Tale lettera consentirà al destinatario di posizionare opportunamente i due dischi uno rispetto all'altro prima di cominciare la decifrazione. La seconda lettera cifrata sarà **V**, *corrispondente alla prima lettera del testo ('I'* $\to$ *'i'). Per la cifratura della lettera successiva,* $s_1 = 1$ *nella parola degli scorrimenti indica che dobbiamo ruotare il disco interno di una posizione in senso orario: dunque alla 'n' del testo corrisponde* **J**. *La lettera cifrata successiva,* **D** $\leftrightarrow$ *'c', è ottenuta con i dischi nella stessa posizione della lettera precedente (*$s_2 = 0$ *significa infatti nessuna rotazione). Proseguendo in questo modo, e ricominciando da* s_1 *ogni volta che si raggiunge la fine di* $\mathcal{S}$*, si arriva alla cifratura completa del messaggio (si omettono gli spazi per renderlo ancora più criptico):*

bVJDIXCXPTDDTSEKCEMQZ .

♢ Scrivere un programma assembler 8086 che, lavorando con le stringhe, consenta di cifrare con il sistema di Alberti il testo "Leibniz Boole Turing" adoperando la chiave K4300615120. Il programma deve includere almeno una procedura, con passaggio dei parametri attraverso lo stack. Simulare su carta il funzionamento del programma, mostrando il contenuto della stringa cifrata ad ogni iterazione, e fornendo esempi del contenuto dei principali registri utilizzati e dello stato dello stack.

Corso di Laurea in Ingegneria Informatica

Calcolatori — a.a. 2022–2023

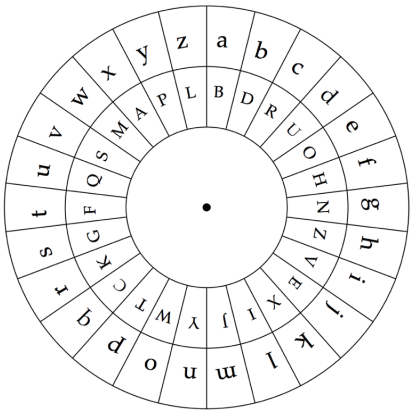
Scritto B del 10 febbraio 2023

(completamento della prova in itinere del 5/11/2022)

Cognome e Nome dello studente: _____

Alberti dischi (dal 1467)

Nel 1467 Leon Battista Alberti descrisse nel trattato De componendis cifris *uno dei primi sistemi di cifratura polialfabetica. Il sistema (vedi figura) è composto da una coppia di dischi concentrici, dei quali quello interno può ruotare rispetto a quello esterno, fisso.*



Il disco esterno riporta le 26 lettere minuscole in ordine alfabetico, quello interno le maiuscole in ordine casuale. Il cifratore e il destinatario devono utilizzare la stessa coppia di dischi, e condividere una chiave $\ell\mathcal{S}$*, dove* ℓ *è una lettera dell'alfabeto interno detta* lettera indice*, e* $\mathcal{S} = s_1 s_2 \dots s_n$ *è una parola di* n *interi detta* parola degli scorrimenti*. Supponiamo di voler cifrare il testo "Incontriamoci alle tre", di avere scelto la chiave D1020043, e posizionato i dischi come in figura. Allora la prima lettera del messaggio cifrato sarà quella che sul disco esterno corrisponde alla lettera indice D, cioè* **b**.

Tale lettera consentirà al destinatario di posizionare opportunamente i due dischi uno rispetto all'altro prima di cominciare la decifrazione. La seconda lettera cifrata sarà **V**, *corrispondente alla prima lettera del testo ('I'* $\to$ *'i'). Per la cifratura della lettera successiva,* $s_1 = 1$ *nella parola degli scorrimenti indica che dobbiamo ruotare il disco interno di una posizione in senso orario: dunque alla 'n' del testo corrisponde* **J**. *La lettera cifrata successiva,* **D** $\leftrightarrow$ *'c', è ottenuta con i dischi nella stessa posizione della lettera precedente (*$s_2 = 0$ *significa infatti nessuna rotazione). Proseguendo in questo modo, e ricominciando da* s_1 *ogni volta che si raggiunge la fine di* $\mathcal{S}$*, si arriva alla cifratura completa del messaggio (si omettono gli spazi per renderlo ancora più criptico):*

bVJDIXCXPTDDTSEKCEMQZ .

♢ Scrivere un programma assembler 8086 che, lavorando con le stringhe, consenta di decifrare con il sistema di Alberti il messaggio **rYBYHFBLLYOKYIXRKMKGS** adoperando la chiave K4300615120. Il programma deve includere almeno una procedura, con passaggio dei parametri attraverso lo stack. Simulare su carta il funzionamento del programma, mostrando il contenuto della stringa decifrata ad ogni iterazione, e fornendo esempi del contenuto dei principali registri utilizzati e dello stato dello stack.