Corso di Laurea in Ingegneria Informatica

Calcolatori Elettronici I — a.a. 2004–2005 (corso a.a. 2003–2004)

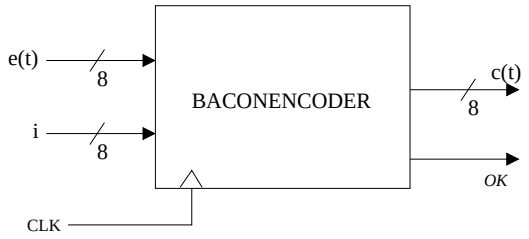
Compito # 1 del 9 febbraio 2005

Cognome e Nome dello studente: _____

Nel suo De dignitate et augmentis scientiarum *(1623), Francesco Bacone narra di avere inventato, da giovane, un metodo per celare un messaggio segreto in un testo qualsiasi. Il metodo consiste nel codificare il "testo esterno" utilizzando le lettere di due diversi alfabeti, scelte in funzione delle lettere che compongono il "testo interno". Più precisamente, a ciascun quintetto di lettere del testo bi-alfabetico codificato corrisponde univocamente una lettera del testo segreto. Ne risulta che il testo esterno deve contenere un numero di lettere almeno quintuplo di quello del testo interno (i segni di interpunzione ed altri simboli speciali, come quelli numerici, vengono ignorati in fase di codifica). La codifica proposta da Bacone per ciascuna lettera del testo segreto con lettere di due diversi alfabeti α e β è la seguente:*

'A'/'a' $\leftrightarrow \alpha\alpha\alpha\alpha\alpha$; *'B'/'b'* $\leftrightarrow \alpha\alpha\alpha\alpha\beta$; *'C'/'c'* $\leftrightarrow \alpha\alpha\alpha\beta\alpha$; ... *'Z'/'z'* $\leftrightarrow \beta\beta\alpha\alpha\beta$.

Si vuole realizzare una versione automatica del metodo di cifratura di Bacone adoperando come alfabeti α e β rispettivamente gli alfabeti ASCII minuscolo e maiuscolo.



La figura mostra una macchina sequenziale che consente di cifrare una singola lettera i del testo interno. A tale scopo, la macchina scandisce uno alla volta i caratteri $e(t)$, $t = 0, 1, \ldots$ del testo esterno, fornendo in uscita il testo cifrato $c(t)$ e terminando con un segnale di OK alto a operazione completata. Esempio: i='m' (tredicesima lettera dell'alfabeto inglese), $\{e(t)\}$ ="F. Baco" ($e(0)$ ='F') $\longmapsto$ $\{c(t)\}$="f. bACo".

1/ Disegnare parte operativa e controllo per la macchina sequenziale di figura, indicando i componenti utilizzati e riportando tutti i segnali di controllo.

2/ Scrivere un programma Assembly 8086 che, realizzando via software e generalizzando il controllo di cui al punto 1, consenta di cifrare il testo interno `"Pinocchio"` facendo uso del testo esterno `"C'era una volta... - Un re! - diranno subito i miei piccoli lettori."`. La stringa cifrata andrà a sovrascrivere il testo esterno. Che modifiche bisogna apportare al metodo di cifratura e al software relativo per poter gestire, oltre che messaggi puramente alfabetici, anche testi interni che contengano le 10 cifre numeriche e un set di n caratteri speciali, ad es. {`' '`,`','`,`'.'`,`';'`,`':'`,`'!'`,`'-'`}?

Corso di Laurea in Ingegneria Informatica

Calcolatori Elettronici I — a.a. 2004–2005 (corso a.a. 2003–2004)

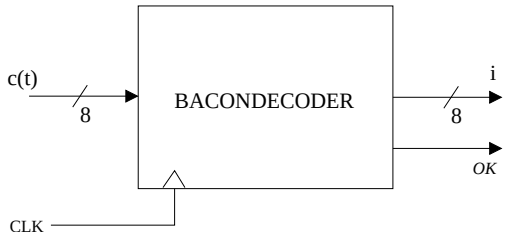
Compito # 2 del 9 febbraio 2005

Cognome e Nome dello studente: _____

Nel suo De dignitate et augmentis scientiarum *(1623), Francesco Bacone narra di avere inventato, da giovane, un metodo per celare un messaggio segreto in un testo qualsiasi. Il metodo consiste nel codificare il "testo esterno" utilizzando le lettere di due diversi alfabeti, scelte in funzione delle lettere che compongono il "testo interno". Più precisamente, a ciascun quintetto di lettere del testo bi-alfabetico codificato corrisponde univocamente una lettera del testo segreto. Ne risulta che il testo esterno deve contenere un numero di lettere almeno quintuplo di quello del testo interno (i segni di interpunzione ed altri simboli speciali, come quelli numerici, vengono ignorati in fase di codifica). La codifica proposta da Bacone per ciascuna lettera del testo segreto con lettere di due diversi alfabeti α e β è la seguente:*

'A'/'a' $\leftrightarrow \alpha\alpha\alpha\alpha\alpha$; *'B'/'b'* $\leftrightarrow \alpha\alpha\alpha\alpha\beta$; *'C'/'c'* $\leftrightarrow \alpha\alpha\alpha\beta\alpha$; ... *'Z'/'z'* $\leftrightarrow \beta\beta\alpha\alpha\beta$.

Si vuole decifrare in modo automatico un testo in formato digitale, cifrato col metodo di Bacone adoperando come alfabeti α e β rispettivamente gli alfabeti ASCII minuscolo e maiuscolo.



La figura mostra una macchina sequenziale che consente di decifrare una singola lettera i del testo interno. A tale scopo, la macchina scandisce uno alla volta i caratteri $c(t)$, $t = 0, 1, \ldots$ del testo cifrato, terminando con un segnale di OK alto a operazione completata. Esempio: $\{c(t)\}$="f. bACo" ($c(0)$ ='f') $\longmapsto$ i='m' (tredicesima lettera dell'alfabeto inglese).

1/ Disegnare parte operativa e controllo per la macchina sequenziale di figura, indicando i componenti utilizzati e riportando tutti i segnali di controllo.

2/ Scrivere un programma Assembly 8086 che, realizzando via software e generalizzando il controllo di cui al punto 1, consenta di decifrare il testo `"c'ERa una VolTA... - UN rE! - DIRannO suBIto I MIei PiCCOli lettori."`. La stringa decifrata andrà a sovrascrivere in memoria il testo cifrato. Che modifiche bisogna apportare al metodo di cifratura e al software di decifrazione per poter gestire, oltre che messaggi puramente alfabetici, anche testi interni che contengano le 10 cifre numeriche e un set di n caratteri speciali, ad es. {' ',',','.',';',':','!','-'}?