

Prova di VHDL

Architettura dei Calcolatori (9 CFU) Macchine per l'elaborazione dell'informazione 03/07/2012

Sviluppare una macchina che effettua la cifratura/decifratura di uno stream di dati in ingresso.

La macchina possiede 3 ingressi da un bit:

- reset: fa partire la macchina dallo stato iniziale
- clock: ingresso
- x : dato
- c: se 1 cifra, se 0 decifra

Un ingresso p da 8 bit che rappresenta la password.

In uscita il messaggio criptato viene riportato sequenzialmente su un bit di uscita.

La funzione di cifratura consiste in:

- contare 8 bit
- effettuare una rotazione verso destra di un numero di posizioni indicate nei 2 bit meno significativi della password
- xor con la password
- xor con gli 8 bit precedentemente cifrati (tutti 0 nel caso del primo byte).

La decifrazione implementa le operazioni opposte.

Realizzare le funzioni di cifratura e decifratura come entity indipendenti da utilizzare attraverso un approccio composizionale.