

# Esame di Laboratorio di Architettura

19/1/2009

## Istruzioni:

Per consegnare il compito usate il form al sito <http://www.dsi.unive.it/~lab-arch/esami/consegna.php>. La soluzione dell'esame deve essere in un file ASCII e deve essere un programma accettato da SPIM. ATTENZIONE: se la pagina di consegna vi da un errore informandovi che la consegna è permessa solo dai laboratori, assicuratevi che il browser non usi il proxy per la sottorete "dsi.unive.it".

## Compito n.1

### Potenza modulo m

Calcolare velocemente espressioni del tipo  $a^n \bmod m$ , cioè il resto della divisione delle potenza n-esima di un numero a per un intero m, è alla base dei moderni algoritmi di crittografia e quindi fondamentale per eseguire transazioni sicure in rete.

La potenza modulare può essere ottenuta per divisioni successive di n:

1. se n è pari ( $n=2b$ ),  $a^n \bmod m$  si può scrivere come

$$a^{2b} \bmod m = (a*a)^b \bmod m = (a*a \bmod m)^b \bmod m$$

se n è dispari ( $n=2b+1$ ),  $a^n \bmod m$  si può scrivere come

$$a^{2b+1} \bmod m = (a*a)^b * a \bmod m = ((a*a \bmod m)^b \bmod m) * a \bmod m$$

dove l'operazione  $x \bmod y$  mi dà il resto della divisione di x per y.

Si scriva una procedura ricorsiva MIPS che calcoli la potenza n-esima di un numero a modulo m usando la scomposizione data e si scriva un programma che chieda in input a, n e m e scriva in output il valore di  $a^n \bmod m$ .

### Domande opzionali

- Come posso usare XOR per invertire il valore di due registri senza usare altra memoria se non i due registri stessi.
- Dimostrare la correttezza dell'approccio usando le proprietà di XOR (suggerimento: XOR è associativa, commutativa e  $a \text{ XOR } b \text{ XOR } b = a$ ).