Università degli Studi di Milano

Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

Fondamenti di informatica per la sicurezza

anno accademico 2008–2009 docente: Stefano Ferrari

29.11.2008 — Primo compitino — versione D

valutazioni **1** (5) _____ **2** (5) _____ **3** (5) _____ **4** (4) _____ **5** (4) _____ **6** (9) _____

Cognome _____ **Nome** _____

Matricola _____ **Firma** _____

Esercizio 1

Per ogni numero k, calcolare il corrispondente numerale nella base n indicata:

a) $k = (523)_7$, $n = 10$

b) $k = (57)_{10}$, $n = 2$

c) $k = (7\mathrm{C})_{16}$, $n = 2$

d) $k = (512)_8$, $n = 2$

e) $k = (410)_5$, $n = 2$

f) $k = (1000111)_2$, $n = 16$

Esercizio 2

Dati $a = 18$, $b = -6$ e $n = 5$, calcolare in complemento a 2 a n bit, specificando sempre se si verifica un overflow:

1. le stringhe binarie s_a e s_b che codificano rispettivamente a e b;
2. la somma delle stringhe binarie s_a e s_b;
3. la differenza delle stringhe binarie s_a e s_b.

Esercizio 3

Una azienda editoriale produce adesivi con le seguenti caratteristiche:

- serie: calcio, spazio, orsetti, dinosauri;
- tipo: normale, metallizzato, olografico;
- dimensione: normale, mini.

L'azienda vende gli adesivi in pacchetti da cinque adesivi.

Si calcoli:

a) il numero di bit necessari per codificare ciascuna caratteristica (serie, tipo, dimensione);

b) il numero di bit necessari per codificare i possibili adesivi;

c) il numero di bit necessari per codificare i possibili pacchetti.

Esercizio 4

Sia data la seguente formula, F:

$$F = ((\neg p \vee q) \leftrightarrow (q \rightarrow \neg r)) \wedge \neg p$$

a) Costruire la tavola di verità di F.

b) F è una tautologia? Motivare la risposta.

Esercizio 5

Formalizzare le seguenti proposizioni (ipotizzando che chi non colora, disegni, e viceversa):

a) Antonio colora solo se colora anche Bice;

b) quando Antonio disegna, Bice e Carlo non colorano;

c) sia Carlo, sia Bice disegnano;

d) Bice disegna se e solo se Antonio e Carlo colorano;

e) Carlo non colora, Bice o Antonio sì.

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

a) **Ip1** $\neg(a \rightarrow \neg b)$
Ip2 $a \rightarrow \neg c$
Tesi $\neg c$

b) **Ip1** $\neg((a \leftrightarrow c) \vee (\neg a \wedge b))$
Ip2 c
Tesi $\neg b$

c) **Ip1** $a \vee b$
Ip2 $\neg(c \rightarrow b)$
Tesi a

Tautologie

- $a \wedge b \Rightarrow a$ (Eliminazione di congiunzione)
- $a \Rightarrow a \vee b$ (Introduzione di disgiunzione)
- $\neg(a \leftrightarrow b) \Leftrightarrow \neg a \leftrightarrow b$ (Negazione della biimplicazione)
- $(a \vee b) \wedge \neg b \Rightarrow a$ (Sillogismo disgiuntivo)
- $\neg a \Rightarrow (a \rightarrow b)$ (*Ex falso sequitur quodlibet*)
- $a \Rightarrow (b \rightarrow a)$ (*Verum sequitur a quodlibet*)
- $a \vee \neg a$ (Terzo escluso)
- $\neg(a \wedge \neg a)$ (Non contraddizione)
- $(a \rightarrow b) \wedge (\neg a \rightarrow b) \Rightarrow b$ (Dimostrazione per casi)
- $(\neg b \rightarrow a) \wedge \neg a \Rightarrow b$ (Dimostrazione per assurdo)
- – $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$ (De Morgan)
  – $\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$
- $(a \rightarrow b) \wedge (b \rightarrow c) \Rightarrow a \rightarrow c$ (Sillogismo ipotetico)
- $a \rightarrow b \Rightarrow (b \rightarrow c) \rightarrow (a \rightarrow c)$ (Transitività dell'implicazione)
- $a \rightarrow b \Leftrightarrow \neg b \rightarrow \neg a$ (Contrapposizione)
- $a \rightarrow (b \wedge c) \Leftrightarrow (a \rightarrow b) \wedge (a \rightarrow c)$ (Distributività delle conseguenze)
- $(a \wedge b) \rightarrow c \Leftrightarrow a \rightarrow (b \rightarrow c)$ (Esportazione/importazione delle premesse)
- $\neg\neg a \Leftrightarrow a$ (Doppia negazione)
- $a \rightarrow b \Leftrightarrow \neg a \vee b$ (Definizione di implicazione)
- – $a \leftrightarrow b \Leftrightarrow (a \rightarrow b) \wedge (b \rightarrow a)$ (Definizione di biimplicazione)
  – $a \leftrightarrow b \Leftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b)$
- $((a \rightarrow b) \wedge a) \Rightarrow b$ (*Modus ponens*)
- $((a \rightarrow b) \wedge \neg b) \Rightarrow \neg a$ (*Modus tollens*)
- – $(a \vee a) \Leftrightarrow a$ (Idempotenza)
  – $(a \wedge a) \Leftrightarrow a$
- – $a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c)$ (Distributività)
  – $a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$
- – $(a \vee b) \Leftrightarrow (b \vee a)$ (Commutatività)
  – $(a \wedge b) \Leftrightarrow (b \wedge a)$
- – $a \vee (b \vee c) \Leftrightarrow (a \vee b) \vee c \Leftrightarrow a \vee b \vee c$ (Associatività)
  – $a \wedge (b \wedge c) \Leftrightarrow (a \wedge b) \wedge c \Leftrightarrow a \wedge b \wedge c$