

**Fondamenti di informatica per la sicurezza****29.11.2008 — Primo compitino — versione C**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) $k = (612)_7, n = 10$
- b) $k = (39)_{10}, n = 2$
- c) $k = (4E)_{16}, n = 2$
- d) $k = (701)_8, n = 2$
- e) $k = (304)_5, n = 2$
- f) $k = (1100101)_2, n = 16$

Esercizio 2

Dati $a = -17, b = 10$ 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 produce caramelle utilizzando i seguenti componenti:

- gusto: pera, menta, fragola, mela, limone;
- forma: sferica, cilindrica, anello;
- ripieno: cremoso, effervescente.

Ogni caramella viene confezionato utilizzando un componente di ogni categoria.

Inoltre, viene proposta anche una supercaramella, di forma sferica, multistrato formata con 3 gusti e un ripieno.

Si calcoli:

- a) il numero di bit necessari per codificare le caratteristiche dei componenti (gusto, forma, ripieno);

- b) il numero di bit necessari per codificare le possibili caramelle;
- c) il numero di bit necessari per codificare le possibili supercaramelle.

Esercizio 4

Sia data la seguente formula, F :

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

- 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 apprezza, compri, e viceversa):

- a) sia Carlo, sia Bice comprano;
- b) Antonio compra se e solo se Bice e Carlo non apprezzano;
- c) Antonio apprezza solo se apprezza anche Bice;
- d) quando Antonio non compra, Bice e Carlo apprezzano;
- e) Carlo compra, Bice o Antonio no.

Esercizio 6

Dimostrare la validità delle seguenti inferenze:

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