Corso di Laurea in Sicurezza dei sistemi e delle reti informatiche

# Fondamenti di informatica per la sicurezza

anno accademico 2003–2004

docente: Stefano Ferrari

## Soluzione del primo compitino — 03.11.2003 — versione A

### Esercizio 1

Effettuare i seguenti cambi di base:

a) $(172)_8 = (???)_{10}$

b) $(83)_{10} = (???)_2$

c) $(B1)_{16} = (???)_2$

d) $(37)_8 = (???)_2$

e) $(61)_7 = (???)_2$

### Soluzione

a) $(172)_8 = 1 \cdot 8^2 + 7 \cdot 8^1 + 2 \cdot 8^0 = 64 + 56 + 2 = (122)_{10}$

b) $(83)_{10}$

| quoziente | resto |
|---|---|
| 83 | |
| 41 | 1 |
| 20 | 1 |
| 10 | 0 |
| 5 | 0 |
| 2 | 1 |
| 1 | 0 |
| 0 | 1 |

$(83)_{10} = (1010011)_2$

c) $(B1)_{16}$

| $B$ | 1 |
|---|---|
| 1011 | 0001 |

$(B1)_{16} = (10110001)_2$

d) $(37)_8$

| 3 | 7 |
|---|---|
| 011 | 111 |

$(37)_8 = (11111)_2$

e) $(61)_7 = 6 \cdot 7^1 + 1 \cdot 7^0 = 42 + 1 = (43)_{10}$

| quoziente | resto |
|---|---|
| 43 | |
| 21 | 1 |
| 10 | 1 |
| 5 | 0 |
| 2 | 1 |
| 1 | 0 |
| 0 | 1 |

$(61)_7 = (101011)_2$

### Esercizio 2

Una macchinina radiocomandata è personalizzabile assemblando diversi tipi di gomme, motore, e carrozzeria.

Le gomme sono disponibili in tre versioni (dure, medie e morbide), il motore in due (basso consumo, medio consumo) e la carrozzeria è disponibile in 17 colori diversi.

Si calcoli:

a) il numero di bit necessari per codificare ciascuno dei tre componenti (gomme, motore, carrozzeria);

b) il numero di bit necessari per codificare la configurazione di un macchinina.

### Soluzione

a)

| | |
|---|---|
| gomme | $\lceil \log_2(3) \rceil = 2$ |
| motore | $\lceil \log_2(2) \rceil = 1$ |
| carrozzeria | $\lceil \log_2(17) \rceil = 5$ |

b) $\lceil \log_2(3 \times 2 \times 17) \rceil = \lceil \log_2(102) \rceil = 7$

Nota: $\lceil x \rceil$ indica il numero intero uguale o immediatamente superiore a $x$.

### Esercizio 3

Dimostrare, tramite tavola di verità che le seguenti formule sono tautologie:

a) $((a \leftrightarrow ((b \to a) \land \neg c)) \land \neg(c \lor b)) \to a$

b) $(((b \leftrightarrow a) \to \neg(a \lor \neg c)) \land \neg(c \lor b)) \to a$

### Soluzione

a) La soluzione è riportata in fig. 1

b) La soluzione è riportata in fig. 2

### Esercizio 4

Dimostrare, che le seguenti inferenze sono valide:

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

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

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

### Soluzione

a) La soluzione è riportata in fig. 3.

b) La soluzione è riportata in fig. 4.

c) La soluzione è riportata in fig. 5.

### Esercizio 5

Formalizzare le seguenti proposizioni:

a) metto la camicia azzurra se e solo se metto il maglione rosso o quello blu

b) non metto il maglione blu, ma quello rosso

c) non metto il maglione blu

d) se metto la camicia azzurra, metto il maglione rosso

e) metto la camicia azzurra e il maglione blu

### Soluzione

Dati i seguenti simboli proposizionali:

$a$ metto la camicia azzurra

$b$ metto il maglione rosso

$c$ metto il maglione blu

le frasi dell'esercizio possono essere formalizzate come:

a) $a \leftrightarrow (b \vee c)$

b) $\neg c \wedge b$

c) $\neg c$

d) $a \rightarrow b$

e) $a \wedge c$

### Esercizio 6

Dimostrare che è valida l'inferenza ottenuta prendendo come ipotesi i punti a) e c) dell'esercizio 5 e come tesi il punto d).

### Soluzione

**Ip1** $a \leftrightarrow (b \vee c)$

**Ip2** $\neg c$

**Tesi** $a \rightarrow b$

La dimostrazione è riportata in fig. 6

| $a$ | $b$ | $c$ | $b \to a$ | $\neg c$ | $(b \to a) \wedge \neg c$ | $a \leftrightarrow \alpha$ | $(c \vee b)$ | $\neg(c \vee b)$ | $\beta \wedge \gamma$ | $(\beta \wedge \gamma) \to a$ |
|---|---|---|---|---|---|---|---|---|---|---|
| F | F | F | V | V | V | F | F | V | F | V |
| F | F | V | V | F | F | V | V | F | F | V |
| F | V | F | F | V | F | V | V | F | F | V |
| F | V | V | F | F | F | V | V | F | F | V |
| V | F | F | V | V | V | V | F | V | V | V |
| V | F | V | V | F | F | F | V | F | F | V |
| V | V | F | V | V | V | V | V | F | F | V |
| V | V | V | V | F | F | F | V | F | F | V |
| | | | | | $\alpha$ | $\beta$ | | $\gamma$ | | |

Figura 1: Soluzione dell'esercizio 3a.

| $a$ | $b$ | $c$ | $b \leftrightarrow a$ | $\neg c$ | $a \vee \neg c$ | $\neg(a \vee \neg c)$ | $\alpha \to \beta$ | $c \vee b$ | $\neg(c \vee b)$ | $\gamma \wedge \delta$ | $(\gamma \wedge \delta) \to \alpha$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| F | F | F | V | V | V | F | F | F | V | F | V |
| F | F | V | V | F | F | V | V | V | F | F | V |
| F | V | F | F | V | V | F | V | V | F | F | V |
| F | V | V | F | F | F | V | V | V | F | F | V |
| V | F | F | F | V | V | F | V | F | V | V | V |
| V | F | V | F | F | V | F | V | V | F | F | V |
| V | V | F | V | V | V | F | F | V | F | F | V |
| V | V | V | V | F | V | F | F | V | F | F | V |
| | | | $\alpha$ | | | $\beta$ | $\gamma$ | | $\delta$ | | |

Figura 2: Soluzione dell'esercizio 3b.

| | | |
|---|---|---|
| (1) | $c \to (a \wedge b)$ | equivalenza logica a Ip1 |
| (2) | $(c \to a) \wedge (c \to b)$ | equivalenza logica a (1) |
| (3) | $c \to b$ | elemento di cong. di (2) |
| (4) | $\neg b \to \neg c$ | contrapposizione di (3) |
| (5) | $\neg c$ | *modus ponens* da Ip2 e (4) |

Figura 3: Soluzione dell'esercizio 4a.

| | | |
|---|---|---|
| (1) | $(b \to a) \wedge (b \to c)$ | equivalenza logica a Ip1 |
| (2) | $b \to a$ | elemento di cong. di (1) |
| (3) | $\neg a \to \neg b$ | contrapposizione di (2) |
| (4) | $\neg b$ | *modus ponens* da Ip2 e (3) |

Figura 4: Soluzione dell'esercizio 4b.

| | | |
|---|---|---|
| (1) | $\neg(a \vee c) \vee \neg b$ | equivalenza logica a Ip1 |
| (2) | $\neg b \vee (\neg a \vee \neg c)$ | equivalenza logica a (1) |
| (3) | $b \to (\neg a \vee \neg c)$ | equivalenza logica a (2) |
| (4) | $(b \to \neg a) \vee (b \to \neg c)$ | equivalenza logica a (3) |
| (5) | $b \to \neg a$ | elemento di cong. di (4) |
| (6) | $(b \to \neg a) \wedge (\neg b \to \neg a)$ | congiunzione di (5) e Ip2 |
| (7) | $(b \to \neg a) \wedge (\neg b \to \neg a) \to \neg a$ | dimostrazione per casi |
| (8) | $\neg a$ | *modus ponens* da (6) e (7) |

Figura 5: Soluzione dell'esercizio 4c.

| | | |
|---|---|---|
| (1) | $(a \to (b \vee c)) \wedge ((b \vee c) \to a)$ | equivalenza logica a Ip1 |
| (2) | $(a \to (b \vee c)))$ | elemento di cong. (1) |
| (3) | $\neg a \vee (b \vee c)$ | equivalenza logica a (2) |
| (4) | $c \vee (\neg a \vee b)$ | equivalenza logica a (3) |
| (5) | $\neg c \to (a \to b)$ | equivalenza logica a (4) |
| (6) | $a \to b$ | *modus pones* da Ip2 e (5) |

Figura 6: Soluzione dell'esercizio 6.