1) $C \rightarrow S : 20$

$S \rightarrow C : 20^d \bmod n$

$S_{PUB} = (13, 77)$ → e, n

a) Supponiamo che ($n = p \cdot q$) $n = 11 \cdot 7$ → perché n deve essere composta da primi.

b) $\phi(n) = (p-1)(q-1) = (11-1) \cdot (7-1) = 60$

c) $(d \cdot e) \bmod \phi(n) = 1 \rightarrow (d \cdot 13) \bmod 60 = 1$

$GCD(60,13) = 1$

$60 = 4 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 60 \cdot x + 13 \cdot y$

$1 = 3 - 2 = 60 \cdot x + 13 \cdot y$

$1 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 60 \cdot x + 13 \cdot y$

$1 = 2 \cdot (8 - 5) - 5 =$

$1 = -3 \cdot 5 + 2 \cdot 8 =$

$1 = -3 \cdot (13 - 8) + 2 \cdot 8 = 5 \cdot 8 - 3 \cdot 13$

$1 = 5 \cdot (60 - (4 \cdot 13)) - 3 \cdot 13 =$

$1 = 5 \cdot 60 - 23 \cdot 13$

$1 = 5 \cdot 60 - 23 \cdot 13$

$1 \bmod 60 = 5 \cdot 60 \bmod 60 - 23 \cdot 13 \bmod 60$

$= 0 - 23 \cdot 13 \bmod 60$

$= 37 \cdot 13 \bmod 60$ $\qquad d = 37$

$20^{37} \bmod 77 =$

1) $C \rightarrow S : 20$

$S \rightarrow C : 20^d \bmod n$

$S_{PUB} = (13, 77)$ → e, → n

a) Sappiamo che ($n = p \cdot q$) $n = 11 \cdot 7$ → perché n deve essere composto da primi.

b) Sappiamo che se $N = 4$ allora $N^d \bmod n = 60$ quindi $4^d \bmod 77 = 60$ (lo deduciamo dal testo)

c) Quindi cerchiamo d: per brute force scopriamo che $d = 7$

$4^7 \bmod 77 = 60$

d) Sostituiamo con $N = 20$ come richiesto nel testo $20^7 \bmod 77 = 48$

2)

(a) A - E

(b) B - F

4) Cs - esercizi - esami.pdf

read $\rightarrow X_S \geq X_O \rightarrow X_O \leq X_S$

write $\rightarrow X_O \geq X_S \rightarrow X_S \leq X_O$

In questo esercizio $X_S = (\text{confidential}, \{\text{red}, \text{blue}\})$

1) read FALSE TRUE FALSE NO READ

$(TS \leq C) \wedge (r \subset r,b)$

write TRUE FALSE FALSE NO WRITE

$(C \leq TS) \wedge (r,b \subset r)$

2) read FALSE TRUE FALSE NO READ

$(S \leq C) \wedge (r,b \subset r,b)$

write TRUE TRUE TRUE WRITE

$(C \leq S) \wedge (r,b \subset r,b)$

3) read FALSE FALSE FALSE NO READ

$(S \leq C) \wedge (r,h \subset r,b)$

write

$(C \leq S) \wedge (r,b \subset r,h)$ FALSE NO WRITE

4) $W \nsubseteq r,b \quad r,b \nsubseteq W$ NO WRITE NO READ

...

5) read

$$\underset{\text{TRUE}}{(C \subseteq C)} \wedge \underset{\text{FALSE}}{(r,b,g \subseteq r,b)} \quad \underset{\text{NO READ}}{\text{FALSE}}$$

write

$$\underset{\text{TRUE}}{(C \subseteq C)} \wedge \underset{\text{TRUE}}{(r,b \subseteq r,b,g)} \quad \underset{\text{WRITE}}{\text{TRUE}}$$

6) read

$$\underset{\text{TRUE}}{(C \subseteq C)} \wedge \underset{\text{TRUE}}{(b \subseteq r,b)} \quad \underset{\text{READ}}{\text{TRUE}}$$

false

$$\underset{\text{TRUE}}{(C \subseteq C)} \wedge \underset{\text{FALSE}}{(r,b \subseteq b)} \quad \underset{\text{NO WRITE}}{\text{FALSE}}$$

7) read

$$\underset{\text{FALSE}}{(TS \subseteq C)} \wedge \underset{\text{FALSE}}{(r,g,b,h \subseteq r,b)} \quad \underset{\text{NO READ}}{\text{FALSE}}$$

false

$$\underset{\text{TRUE}}{(C \subseteq TS)} \wedge (r,b \subseteq r,g,b,h) \quad \underset{\text{WRITE}}{\text{TRUE}}$$