1) CRITTOGRAFIA.

a)

TRUE

(b) Numero di trasposizioni applicabili su string da 4 bit

$4! = 4 \cdot 3 \cdot 2 = 24$

(b) Numero di sostituzioni applicabili su string da 4 bit

$2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$

2) DIGITAL SIGNATURE and DIGITAL CERTIFICATE

a)

(1) Il PC invia il codice hash al lettore di smartcard.

(2) Il lettore di smartcard può richiedere un pin all'utente

(3) La smartcard calcola e restituisce al PC la codifica del codice hash ricevuto dal PC.

b)

Decifro X con la mia chiave privata e prendo il risultato come chiave di sessione condivisa con il cliente.

4) ACCESS CONTROL

-rw-r----	mario	cooks	order.txt
--s--x---	mario	waiters	enqueue
--s--x---	mario	cooks	dequeue