Θέμα 3ο = Φεβρουάριος 2011

A) α) Το SSH παρέχει authentication (ταυτοποίηση των 2 άκρων), confidentiality (εμπιστευτικότητα) μέσω συμμετρικής κρυπτογράφησης και integrity (ακεραιότητα) των δεδομένων.

β) Δεν μας εξασφαλίζει την αυθεντικότητα του public key του server με τον οποίο συνδέθηκε. Είναι ευθύνη του χρήστη η αποδοχή, ή μη, του κλειδιού αυτού. Γι' αυτό το λόγο η μέθοδος είναι επιρρεπής σε επιθέσεις τύπου man-in-the-middle. Ο SSH client δεν κάνει αυτόματα αποδεκτό το public key του server γιατί δεν είναι πιστοποιημένο από κάποια τρίτη εμπιστη οντότητα που αυτός γνωρίζει εκ των προτέρων.

γ) Ο μηχανισμός αυτός χρησιμοποιεί την κρυπτογραφία δημόσιου κλειδιού, σε συνδυασμό με ψηφιακά πιστοποιητικά και πιστοποιεί την αυθεντικότητα του δημόσιου κλειδιού του server.

B) Βλέπε λύσεις Οκτώβρη 2011