Εργαστήριο 6ο

1. Καταρχάς, ο MD5 είναι γνωστό πως έχει σπάσει και μπορούμε γρήγορα από το hash να βρούμε το αρχικό κείμενο. Όσον αφορά τον SHA, τόσο ο SHA1 όσο και ο SHA256 έχουν μεγαλύτερο μέγεθος εξόδου, 160bit και 256bit αντίστοιχα, συγκριτικά με τα 128bit του MD5. Οπότε, ο αλγόριθμος SHA είναι πιο ασφαλής.
2. Λόγω ότι ο MD5 επεξεργάζεται τα δεδομένα εισόδου(κείμενο, αρχείο, εικόνα, κ.λπ.) ανά μπλοκ των 64bytes και παράγει ένα μικρό hash(128bit), ο αλγόριθμος είναι ευαίσθητος στις επιθέσεις λεξικού. Έτσι με την χρήση ενός μεγάλου σε πλήθος λέξεων λεξικού, όπου η κάθε μια έχει γνωστή και τη τιμή hash της αντίστοιχα, μπορεί να γίνει πολύ γρήγορα η αντιστοίχιση και να βρεθεί η αρχική είσοδος.