

Abdelhakman Adel
17012296

Assignment 6

PAGE
DATE

Theoretical questions

① The first 4 values are the values found in MD4 & MD5 & SHA 1 is a successor & They are called Nothing Up My Sleeve numbers with a hamming weight of 0.5 for all numbers. They are taken using the square root of some numbers.

② Strong Collision resistance is:

given hashing function $H()$ & inputs X & Y there is an absolute minimum chance of $H(X) = H(Y)$

(2)