Introduction to Cryptography Assignment 4

Implementation of hash function SHA-1

Environment

Linux 2.6.34-gentoo-r6 x86_64 with UTF-8 locale

g++ version 4.4.3 (Gentoo 4.4.3-r2 p1.2)

Vim 7.2

Questions

Question 1(20%)

Input message is empty string (length 0)

| |
| |

Answer1

| da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709 |

Question 2(20%)

Input message

| You know you dont have to act with me, Steve. You dont have to say anything, and you dont have to do anything. Not a thing. Oh, maybe just whistle. You know how to whistle, dont you, Steve? You just put your lips together and... blow. |

Answer2

| bd6b2294 fb86b57c 97f32064 f5f94304 5f5615f1 |

Question 3(20%)

Input message

| The world aint all sunshine and rainbows. Its a very mean and nasty place and I dont care how tough you are it will beat you to your knees and keep you there permanently if you let it. You, me, or nobody is gonna hit as hard as life. But it aint about how hard ya hit. Its about how hard you can get it and keep moving forward. How much you can take and keep moving forward. Thats how winning is done! |

Answer3

| abc49a21 e5a6d8ee 3441410a 8ab71e17 3f15e12e |