Security Lab 2

1. When using MD5, the final output is a 32 character hash

When using SHA1, the final output is a 40 character hash

When using SHA256, the final output is a 64 character hash

All of the hashes are the size of the key being used in each divided by 4

1. You do not have to use a key of a specific size. Every output is the same length when using the same algorithm. This is due to the compression that takes place inside each algorithm, making it that much harder for a hacker to get ahold of the key being used.
2. 9bfa74ffa9e321697a3bb9efaeb60945 – md5 original

7987558b32473f94e3e65ebffccacca0 – md5 flipped bit

2abd5e0d79bd2c531e8c8a92d69d33f1e278139aab3c191af28de94130ce1d21 – sha256 original

16b87874a3613b5500d57bb30f979488b7c36cfd421c92594b1eef6ca31e09d6 – sha256 flipped

I do not really see much for similarities between the values. There is a “ff” in in both of the md5 cases, but that is about all I can find.