Brian Huang
CS370
Programming assignment 1

1. I used sha1, sha224, sha256, sha384, and sha512. The output size of sha1 is 40 hexadecimal digits long, while the rest are 32 to 64 bit words long. I used python's hashlib library.
2. It takes about the same amount of time for both of the bloom filters to process one password.
3. There is no probability of a false negative, because that is the property of the bloom filter. The size of my bloom filters are 2^{22} so the probability for false positive is:

$$p = (1 - e^{\frac{-kn}{m}})^k$$

$$p = (1 - e^{\frac{-(5)(623{,}518)}{2^{22}}})^5$$

$$p = 0.039 \ = \ 3.9\%$$

$$p = (1 - e^{\frac{-kn}{m}})^k$$

$$p = (1 - e^{\frac{-(3)(623{,}518)}{2^{22}}})^3$$

$$p = 0.046 \ = \ 4.6\%$$

4. There are two ways to reduce the rate of false positives. The first is to increase the number of hash functions you use in the bloom filter, the second is to increase the size of your bloom filter.