Max Franz

Write-Up for Project 2

1. I chose to use MD5, SHA224, SHA256, SHA384, and SHA512 which are all unkeyed cryptographic hash functions. The output range for SHA224 is [0 - ((2^256) - 1)], for SHA256 the output range is [0 - ((2^256) - 1)], for SHA384 the output range is [0 - ((2^384) - 1)], for SHA512 the output range is [0 - ((2^512) - 1)], and for MD5 the output range is [0 - ((2^128) - 1)]. I hardcoded the size of the bloom filters, the size of the 3 hash function bloom filter is 4,000,000 and the size of the 5 hash function bloom filter is 6,000,000.
2. The 3 hash function bloom filter takes 0.0174939632416 seconds and the 5 hash function bloom filter takes 0.0178260803223 seconds. The 3 hash function bloom filter performs better because there are less calculations that have to be done.
3. The probability of false positive is 5% or 0.05. There are no false negatives when using a bloom filter.
4. You can reduce the false positive rate by either increasing the number of hash functions, increasing the size of the bitarray, or adding less elements to be checked.