Section 7 Lecture 43 – Hashing

Q1)

For each of the following hashing algorithms which give an 8-bit answer, give the hash of the given message.

(i) Take a number (mod 256) and write it as an 8-bit binary number, given input 8713

(ii) Take an 8-bit binary number and swap each pair of bits (so swapping the first and second bits, then the third and fourth bits, and so on), given input 10101110

(iii) Take a 16-bit binary number and take every alternating bit (first, third, fifth etc) and then reverse the answer, given input 0101010000111011

(iv) Return 00000000, given input 10111011101110010011010111101011

Q2)

For each hashing algorithm in Q1:

(a) Does a small change in the input give a totally different hash?

(b) Can you recover the original message given a hash?

(c) Can you create two messages that give the same hash?

Q3)

Find an online SHA and/or MD5 calculator. Experiment with different messages – try just changing one letter (e.g. “MEET ME IN THE CAR” and “MEET ME IN THE BAR”). Are the hashes completely different even with a minor change?