Section 7 Lecture 43 – Hashing - Exercises

Q1)

(i) 8713 (mod 256) is 9, which is 00001001 in binary

(ii) Just swapping each pair, 01011101

(iii) Taking alternate bits gives 00000111, which reversed gives 11100000

(iv) Just 00000000

Q2)

(i)

(a) It could do – for example 9713 (changing one digit) would give 241 which is 11110001 which is totally different

(b) No – it could be anything equivalent (mod 256)

(c) Any two numbers equivalent (mod 256) will give the same hash, for example 1 and 257 give the same answer 00000001

(ii)

(a) No, changing e.g. one bit will only change bit in the answer

(b) Yes – just repeat the process

(c) No, each message gives a unique answer

(iii)

(a) No – e.g. changing one bit would give either no difference or a one bit difference

(b) No – eight bits have been lost

(c) Yes, anything with different "lost" bits, for example 0000000000111111 gives the same answer as 0101010000111011

(iv)

(a) No, the hash is the same, 00000000

(b) No – it could have been anything

(c) Yes – absolutely anything!

Q3)

Over to you! You should find that a minor change completely alters the hash.