

Birthday paradox and Hash collision

Description

- The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value.
- In this quiz, you will need to implement a program that takes a 16-byte number as input and find a different number with the same 16 MSB of the MD5 value.(hint: hashlib is your best friend)

Spec

- Input:
 - A 16-byte hexadecimal number
- Output:
 - The 16 MSB of the MD5 in hexadecimal and a 16-byte hexadecimal number separated by a whitespace
- For example:

Input:

c606196ea460a3a53ac3e81c614b990b

Output:

9cc7 0228e3b50cd30ee5084bf7340fd5a2d