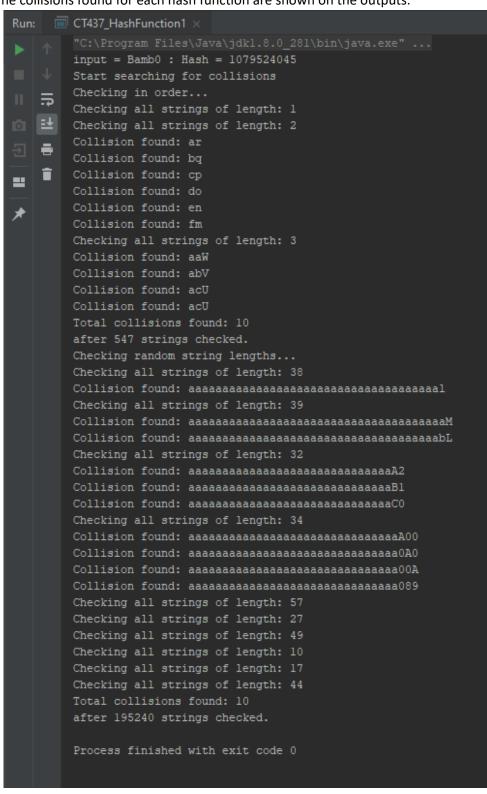
CT437 Assignment 3 – Breaking Hash Functions

Problem 1 - Searching for collisions

- The screenshot below is from running the code using hashF1 (i.e. usingNewFunction set to false in the checkAllStringsOfCertainLength function), using 2 methods: incrementing string lengths and random string lengths.
- The collisions found for each hash function are shown on the outputs.



Problem 2 - New hash function

- The screenshot below is from the code running in the same way as problem 1, but using the new hash function.
 - Using incrementing string lengths, it took 547 checks to find 10 collisions for hashF1, but 230345 for hashF2.
 - Using random string lengths, it took 195240 checks to find 10 collisions for hashF1, but 1000122 for hashF2.
- This suggests that hashF2 is more resistant to collisions

```
Run: Transplace CT437_HashFunction1
       input = Bamb0 : Hash = 1079524045

↓ Start searching for collisions

      Checking in order...
       Checking all strings of length: 1
       Checking all strings of length: 2
       Collision found: A4
     Collision found: B3
       Collision found: C2
       Collision found: D1
       Collision found: E0
       Collision found: 0E
       Checking all strings of length: 3
       Checking all strings of length: 4
       Collision found: aabP
       Total collisions found: 10
       Checking random string lengths...
       Checking all strings of length: 53
       Checking all strings of length: 56
       Checking all strings of length: 9
       Checking all strings of length: 33
       Collision found: aaaaaaaaaaaaaaaaaaaaaaaaabH
       Collision found: aaaaaaaaaaaaaaaaaaaaaaaaaaaGG
       Collision found: aaaaaaaaaaaaaaaaaaaaaaaaaaa
       Checking all strings of length: 44
       Checking all strings of length: 30
       Checking all strings of length: 49
       Checking all strings of length: 3
       Checking all strings of length: 9
       Checking all strings of length: 43
       Total collisions found: 10
       after 1000122 strings checked.
       Process finished with exit code 0
```