CS 4476 – Assignment 3

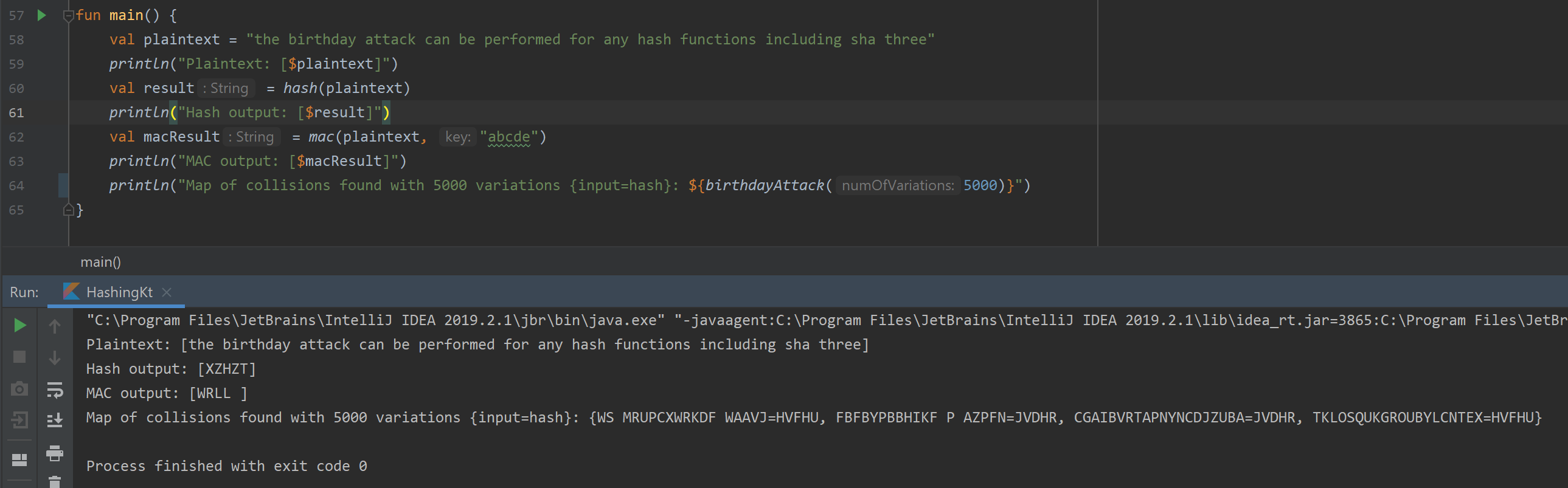
These programs have been developed using the language Kotlin, targeting JVM. This was completed using IntelliJ Idea.

Hashing.kt is the source code file, containing the solutions to all 3 problems in the assignment. Three functions were implemented in this program, one as a solution for each problem:

**fun hash(str: String): String** – implements the 3 specified rounds for hashing plaintexts.

**fun mac(str: String, key: String): String** – calls the hash function as per MACK(x) = h(K||h(K||x)), with K as a 5 character key and x as the plaintext.

**fun birthdayAttack(numOfVariations: Int): String** – hashes a number (numOfVariations) of random 20-character strings, then finds and returns any duplicate hashes and their inputs from those variations.

Outputs are shown in the screenshot below: