Discussion Question 3: In our example, the attacker tries to leak the values in the array secret_part2. In a real-world attack, people can use Spectre to leak arbitrary values in the victim's address space. Explain how the attacker can achieve this.

We need to know some kind of code on which the victim is working. For example, if the secret key value is 1, the victim will access a particular address based on the key and then the attacker can do timing side-channel attacks and decode the secret key value is 1. If the value is 0, the victim won't access any address and the attacker would decode that. That's how the attacker can achieve real world spectre attack. Also, in the real-world attack, the attacker needs to exploit speculative execution like mistrainging Branch Predictors or BTB.

Discussion Question 4: Try to tune the training parameters and answer this question: What is the fewest number of times you need to train the branch on line 9 in Listing 3 to make the attack work?

Training the Brach once works fine for the attack.