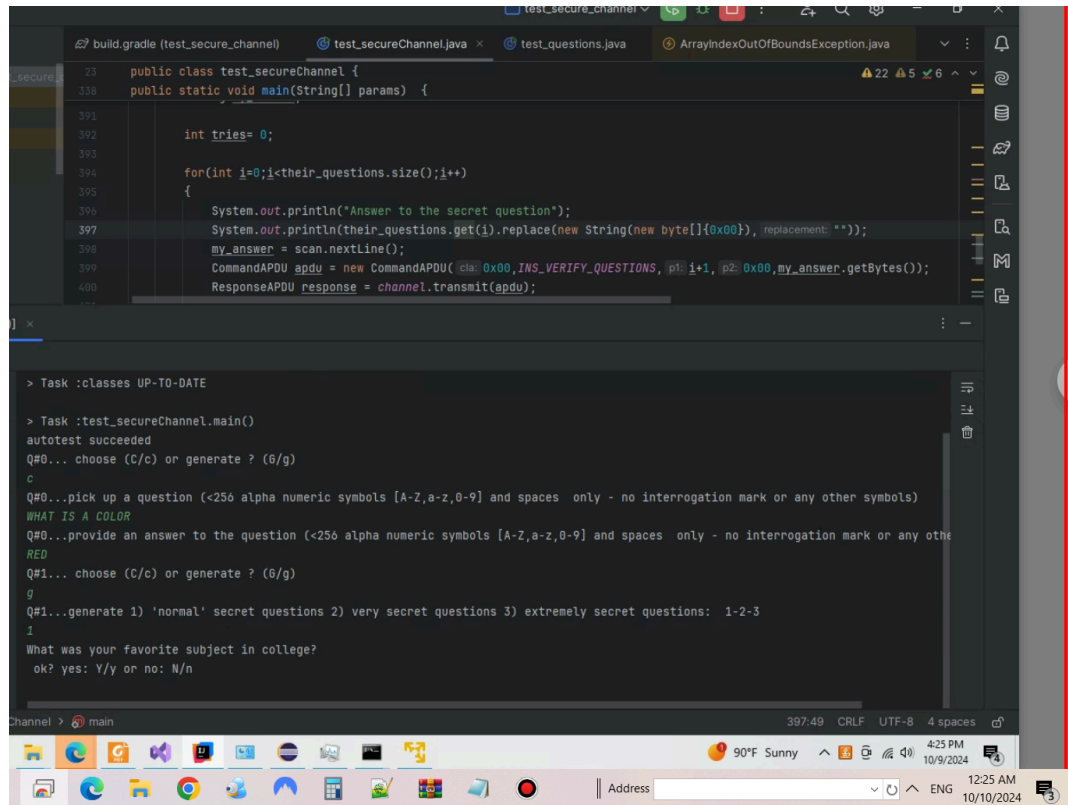


M72

- 1) Users can create 5 questions /answers on a desktop interface. Questions can be freely chosen or suggested by AI (GPT)



The screenshot shows an IDE with two windows. The top window displays Java code for a class named `test_secureChannel`. The code includes a `main` method that iterates over a list of questions, prints them, and processes user input. The bottom window shows the output of running the code, which includes prompts for choosing between generating questions or providing answers, and the resulting question and answer pairs.

```
public class test_secureChannel {
    public static void main(String[] params) {
        int tries= 0;
        for(int i=0;i<their_questions.size();i++)
        {
            System.out.println("Answer to the secret question");
            System.out.println(their_questions.get(i).replace(new String(new byte[]{0x00}), replacement: ""));
            my_answer = scan.nextLine();
            CommandAPDU apdu = new CommandAPDU(0x00,INS_VERIFY_QUESTIONS, p1: i+1, p2: 0x00,my_answer.getBytes());
            ResponseAPDU response = channel.transmit(apdu);
        }
    }
}
```

```
> Task :classes UP-TO-DATE
> Task :test_secureChannel.main()
autotest succeeded
Q#0... choose (C/c) or generate ? (G/g)
c
Q#0...pick up a question (<256 alpha numeric symbols [A-Z,a-z,0-9] and spaces only - no interrogation mark or any other symbols)
WHAT IS A COLOR
Q#0...provide an answer to the question (<256 alpha numeric symbols [A-Z,a-z,0-9] and spaces only - no interrogation mark or any other symbols)
RED
Q#1... choose (C/c) or generate ? (G/g)
g
Q#1...generate 1) 'normal' secret questions 2) very secret questions 3) extremely secret questions: 1-2-3
1
What was your favorite subject in college?
ok? yes: Y/y or no: N/n
```

- 2) The 5 user/questions are sent to card

YOUR CHOICES

Q:WHAT IS A COLOR

A:RED

Q:WHAT WAS YOUR FAVORITE SUBJECT IN COLLEGE?

A:TOPOLOGY

Q:Q1

A:A1

Q:Q1

A:A1

Q:Q1

A:A1

List of card readers: [PC/SC terminal Identive SCR33xx v2.0 USB SC Reader 0, PC/SC terminal JAVACOS Virtual Contact Reader 0, PC/SC terminal JAVACOS Virtual Contactless Reader 1]

Card reader: PC/SC terminal Identive SCR33xx v2.0 USB SC Reader 0

00A4040009010203040506070800

0x9000

Applet selected

000D01000F57484154204953204120434F4C4F52

000D02002A574841542057415320594F5552204641564F52495445205355424A45435420494E20434F4C4C4547453F

000D0300025131

000D0400025131

000D0500025131

000D010103524544

000D020108544F504F4C4F4759

000D0301024131

000D0401024131

000D0501024131

start recovery when ready - press RETURN

- 3) Then user can retrieve the list of questions and start answering them

```
WHAT WAS YOUR FAVORITE SUBJECT IN COLLEGE?  
TOPOLOGY  
Correct Answer!  
SECRET =LESECRET  
Answer to the secret question  
Q1  
A1  
Correct Answer!  
SECRET =LESECRET  
Answer to the secret question  
Q1  
A1  
Correct Answer!  
SECRET =LESECRET  
Answer to the secret question  
Q1
```

- 4) Each time a user answers any new question correctly , its score increases. Once this score reaches a quorum the secret is unlocked and can be retrieved.
- 5) After applet is deselected (eg typically card is removed from reader) , getting a secret is again locked and questions must be answered again
- 6) Trying to reach a secret without answering the questions will return an error