PasswordGenerator

Specifications:

1. The password must be 8 to 12 characters. The password should have an equal probability of being any length within the acceptable range of lengths.
2. The first character must be alphabetic (upper or lower case). Each of the 52 possible characters should have an equal probability of being selected.
3. All other characters may be alphanumeric. Each of the 62 possible characters should have an equal probability of being selected.
4. The password must contain:

* at least one upper case letter
* at least one lower case letter
* at least one numeric

1. At a randomly selected internal position (not the first or last character), the password must include one of the following:
   1. "\_" (underscore)
   2. "-" (hyphen)
   3. "$"
   4. "%"
   5. "#"
   6. "@"

There should be an equal probability of selecting any of these six characters. Only one character in the password should be non-alphanumeric.

Extra Credit:

Store all generated passwords in a text file in your project.

The text file name should be named **storedPasswords.txt**

Before accepting a password, the program needs to check that the password has not been previously generated. Therefore the password should not in the text file of previously generated passwords.

**Hint**: Read all the passwords from **storedPasswords.txt** into an **ArrayList<String>** instance variable.