

Password Encryption Assignment

10A 8T

In this digital world, it is very important to have “strong” passwords in order to protect our personal data. The difficulty is creating passwords that we can remember and yet are hard to guess from possible attackers. In this assignment we will analyze “what needs to be considered” when creating a “strong” password.

Consider four passwords used for bank cards, websites, and so on. DO NOT write them down.

a. What are the rules for creating each password? [3A]

	1.Online banking -research if needed	2.Email	3.Social media sites	4. OES School login
Minimum length				
What must be included				
What must not be included				

b. Think of the minimum requirements for passwords in each scenario [5A]

➤ **for example:** 4 characters, must include uppercase and numbers

How many possible passwords can be created using the minimum requirements in each scenario below? Show all calculations using proper notation.

i. Online banking:

ii. Email:

iii. Social websites:

iv. School login :

- c. At 90 000 codes per second, how long, on average, would it take for a good password cracking program to break each of your passwords? [2T]

Online banking:

Email:

Social websites:

School login:

- d. Some passwords require at least one digit and at least one capital letter. Why? Provide calculations to support your answer. [3T]

- e. Develop a set of guidelines to identify a good, poor, or average password. Back it up with examples and calculations. [3T]