1/1/2022

Group # 4

Group Members:

Muhammad Shahmir 21K-3563

Khizer Nadeem 21K-4768

Saad Hassan 21K-3605

Secure Supermarket Management System

NETWORKING AND CYBERSECURITY PROJECT

**Scenario:**

The scenario chosen by our group to implement was a Supermarket checkout/management software in which we implemented several security features. This software allows employees to add items which a person has brought to their bill and check out.

**Cybersecurity Concepts used:**

1. Encryption
2. User Authentication
3. Credit Card authentication
4. Validation
5. Verification

**Tasks Implemented by Members**:

1)Encryption/Decryption/Driver function: Shahmir (21K-3563)

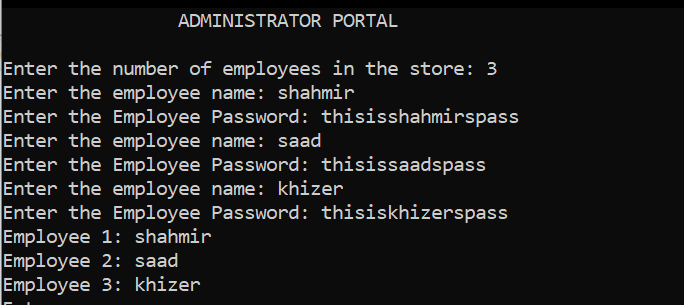
2)Credit Card Authentication: Khizer Nadeem(21K-4768)

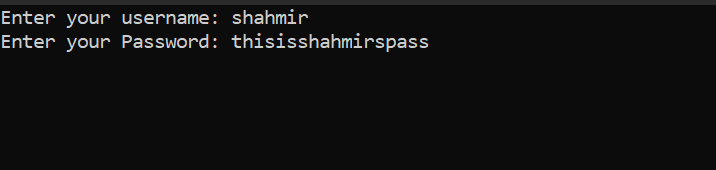
3)Validation/Verification: Saad Hassan(21K-3605)

To start off the program will ask for owner/administrator/root access so that the owner can set the usernames and passwords for each employee to ensure that unauthorized personnel cannot access the software.



Once the owner has added his password the program prompts him to add employees who will be working at the store. The owner will input the usernames and passwords of these employees which they can use later on to access the software.





**Encryption/Decryption:**

Here we implemented encryption using the shift cipher as all passwords are saved in the text file using the shift cypher. The owner can access these later in case one of the employees forget their passwords. The shift cypher is implemented with the key ‘8’.

How a shift cypher works:

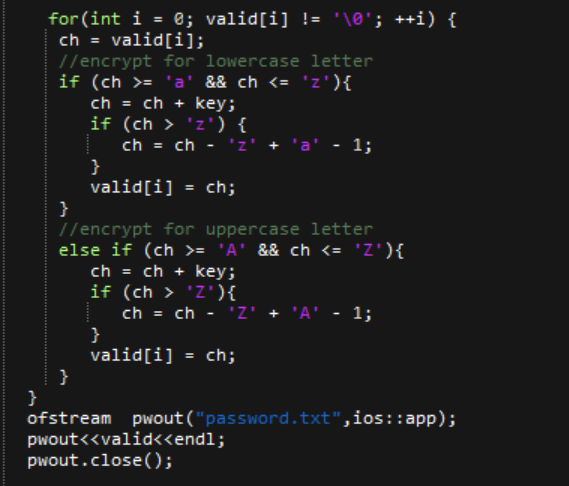
1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number X.  
( A=0, B=1, C=2, ..., Y=24, Z=25)

2. Calculate: Y = (X + K) mod 26 //mod is done to ensure it does not go out of range

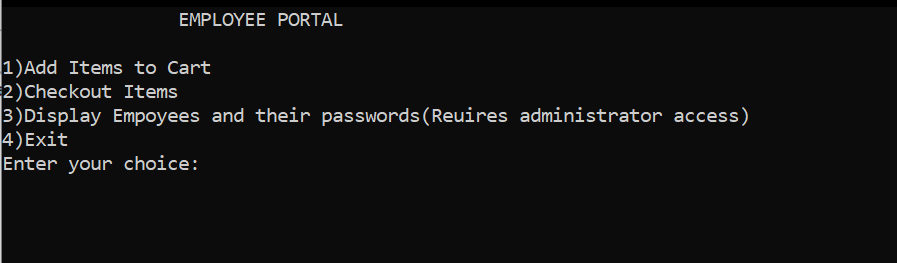
3. Convert the number Y into a letter that matches its order in the alphabet starting from 0.

Password Encryption:



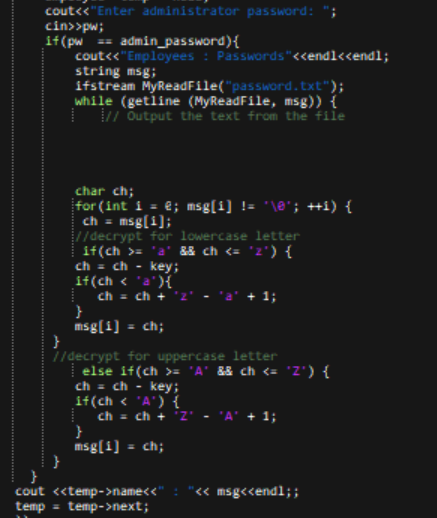


Once the employee enters their username and password they gain access to the employee portal where they can add to cart and checkout items for the customers



In Case one of the employees lost their password the Administrator can

Access the passwords as they have been saved in the text file. Here we have implemented the decryption algorithm for shift cypher.

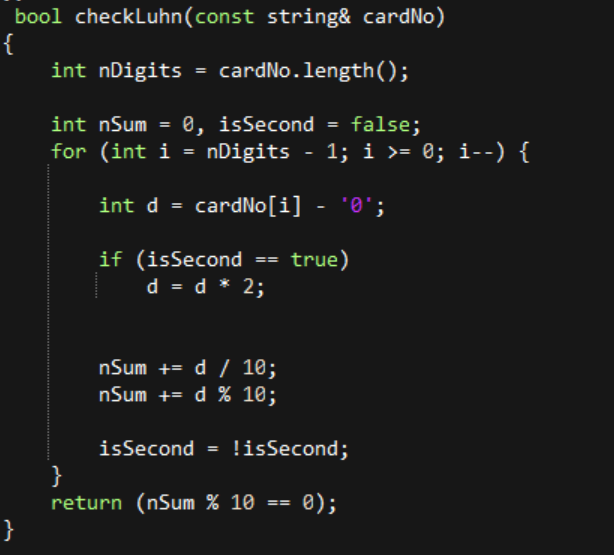


**Credit Card Authentication:**

Once the employee checks out all the items and the person’s bill is generated, the program asks whether the person would like to pay via cash or credit card. If the person asks to pay through credit card the program asks for the persons credit card number and validates it using the Luhn algorithm. The Luhn algorithm, also known as the modulus 10 or mod 10 algorithm, is a simple checksum formula used to validate a variety of identification numbers, such as credit card numbers, IMEI numbers, Canadian Social Insurance Numbers.

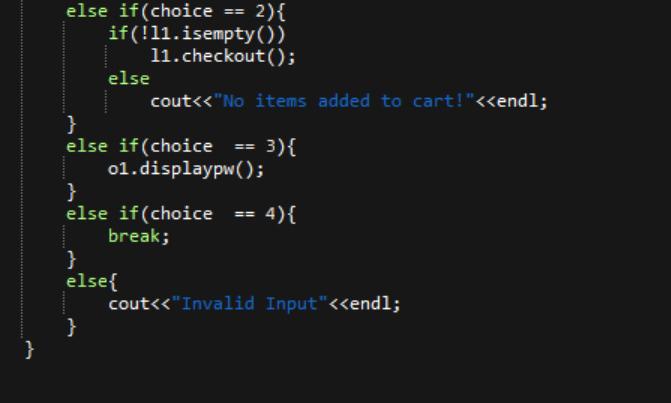
Here are the steps applied by the algorithm to check credit cards :

* Drop the last digit from the card number. The last digit (16th position) is called Luhn key.
* Evaluate each digit from right to left. When the digit is in odd positions, we multiply it by 2. If, in addition, the digit is superior or equal to 5, we simply substract 9 from the previous multiplication (only applicable for odd ranks).
* Add all the numbers together
* Compute the Luhn Key. This (last) digit is the amount that you would need to add to the previous total (computed above in step 3) to get a multiple of 10 (Modulo 10). This Luhn key has to be equal to the last digit which has been removed in step 1.



**Validation/Verification:**

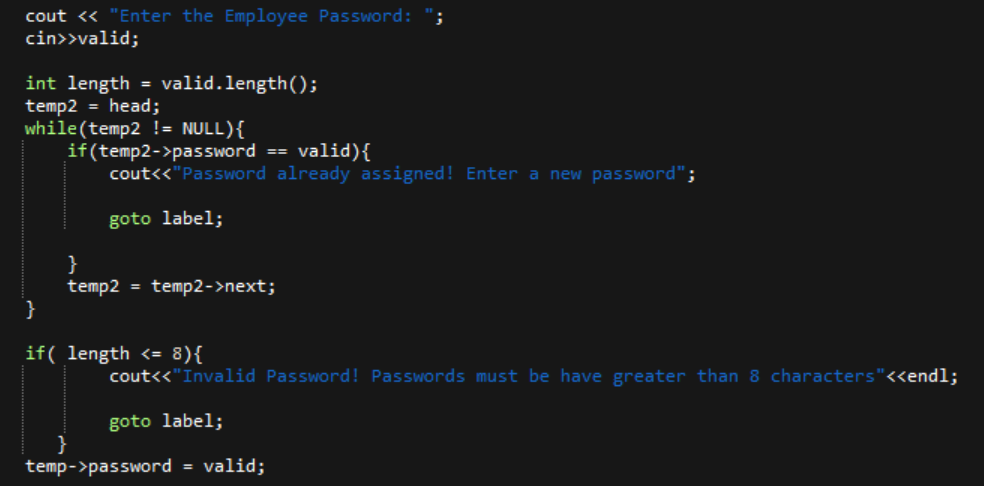
Most of the inputs in the program have been verified and error prompts have been set to ensure rectification in case of an erroneous input. Functions like isEmpty() were made to ensure that employees donot accidently check out an empty cart in which nothing is added.



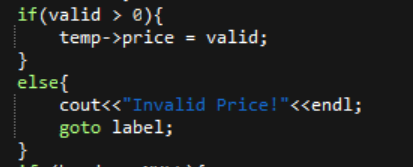
Furthermore Constraints were set on passwords to make them more secure:

Password Constraints:

1. No 2 employees can have the same passwords
2. Passwords must be greater than 8 characters to ensure they are not cracked easily.



To make sure price is not negative:



In case wrong choices are input by employee, error prompts have been added

