Bluegrass Community and Technical College

Programming Requirements Document

Learning an Easy Cipher

BACKGROUND INFORMATION

This semester we will study several cybersecurity topics (secure code and cryptography). This assignment will begin our study of cryptography. There are few important terms to know:

- Cryptography – a technique of protecting information and communications using codes so that only those for whom the information is intended can read and use it.
- Encryption - the process of translating information/data that is easily read by individuals (called plaintext) into a new format that appears to be random, meaningless, and not easily understood (called ciphertext).
- Decryption - the process of converting ciphertext back to plaintext.

This assignment will focus on a very basic (and easy to break) encryption cipher:

The Caesar Cipher.

Read and watch the following video and website on the Caesar Cipher:

https://learncryptography.com/classical-encryption/caesar-cipher
https://www.youtube.com/watch?v=pIt4Q68J00A

The Caesar Cipher is simply a "shift" algorithm. You can use Caesar ciphers with alphabetic letters and with integer values. Many examples you read illustrate the Caesar Cipher with letters, but you can also use it for numeric data. We will use it to encrypt integers.

For integers, you simply apply the shift value to an existing number to achieve an "encrypted" number.

Examples:

Plaintext integer: 107
Shift: 15
Encrypted value: 122 (107+15)

Ciphertext integer 122
Shift: 15
Decrypted value: 107 (122-15)

Plaintext integer: 1000
Shift: 145
Encrypted value: 1145

Ciphertext integer 1111
Shift: 10
Decrypted value: 1101

NARRATIVE DESCRIPTION

Your local bank uses 5-digit personal identification number (PIN) for debit card and ATM transactions. They allow customers to change their PIN using the last 4 digits of their social security number (SSN) as a verification. They want the PIN and last 4 digits of the SSN encrypted when stored.

You have been asked to use a Caesar cipher to encrypt a customer's PIN and last 4 digits of an SSN. Write a program that will test this.

To do this, create a Java program that will **input** the following:

- A customer's first name
- A customer's last name
- The customer's PIN
- The customer's last 4 digits of their SSN
- A shift value for the Caesar cipher

The program should perform the following **processing**:

- Encrypt the PIN and SSN using the shift value. Output these values

The program should perform the following **output**:

- To test encryption using a Caesar cipher on the customer's PIN and SSN, output the customer's name, PIN, last 4-digits of the the SSN, the Caesar Shift, the encrypted PIN and the encrypted SSN in the following format:

```
Customer:          Olivia Jenkins
PIN:               11507
Last 4 of SSN:     7008
Caesar Shift:      123
Encrypted PIN:     11630
Encrypted SSN:     7131
```

- Once this is completed and tested, add coding to decrypt the encrypted PIN and SSN. <u>Do not simply display the input provided by the customer but calculate the decryptions using the shift value.</u> Your final output should be similar to:

```
Customer:          Olivia Jenkins
PIN:               11507
Last 4 of SSN:     7008
Caesar Shift:      123
Encrypted PIN:     11630
Encrypted SSN:     7131
Decrypted PIN:     11507
Decrypted SSN:     7008
```

NOTE: Since we have not learned about selection statement yet, we will not perform error-checking on the user input. This will be coming soon.

New Concepts Assessed and Illustrated (in addition to any previously learned)

- Cryptography and the Caesar cipher
- Formatting output in a pleasing manner
- Integer arithmetic

Software Requirements (Use a checklist for all features)

- ☐ Select the correct data type for each variable and constant.
- ☐ Input required values from the user (one at a time).
- ☐ Encrypt the PIN.
- ☐ Encrypt the SSN.
- ☐ Decrypt the encrypted PIN.
- ☐ Decrypt the encrypted SSN.
- ☐ All input prompts should be clear to the user as to what they are to key.
- ☐ All output should be clear to the user as to what they are viewing as the results. You must format the output as shown on the previous page.
- ☐ Do not use any features/topics we have not learned in class. THIS WILL NOT INCLUDED IN FUTURE ASSIGNMENTS BUT ALWAYS REQUIRED.
- ☐ Include a comment block at the top of your program to include (1) Your name (2) Date (3) Instructor (4) Class and (5) Purpose of this program. THIS WILL NOT INCLUDED IN FUTURE ASSIGNMENTS BUT ALWAYS REQUIRED.
- ☐ Use the Programming Standards document from Module 1 to apply documentation standards correctly. Document each section of code. THIS WILL NOT INCLUDED IN FUTURE ASSIGNMENTS BUT ALWAYS REQUIRED.

Security Considerations

Selecting incorrect data types can have security implications, which we will soon learn about. It is very important that you select the correct data type (and size) for each variable and constant you use. We do not want to waste memory and yet we must insure the data type is large enough to hold the data to be stored in memory. Cryptography allow us to secure sensitive data.