Introduction to Programming: Lab Session 11 – Exercises

1 Ciphers (from ETH)

One of the classical cryptographic techniques for enciphering text is known as the Vigenère cipher. It derives from the Caesar cipher, in which each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E and so on. The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values.

To implement the Vigenère cipher the letters of the alphabet A, B, ..., Z are associated with the numbers 0, 1, ..., 25. The plain text message can then be viewed as a sequence of numbers: $P = [P_1, P_2, \ldots, P_n]$ where $P_i \in \{0, 1, \ldots, 25\}$ for any $i \in \{1, 2, \ldots, n\}$. To encrypt the plain text, the algorithm generates a key of the same length as the plain text by repeating a secret pass phrase.

The key can also be viewed as a sequence of numbers between $0, 1, \ldots, 25$: $K = [K_1, K_2, \ldots, K_n]$ where $K_i \in \{0, 1, \ldots, 25\}$ for any $i \in \{1, 2, \ldots, n\}$. The message is encrypted by adding the key item by item to the plain text modulo 26: $C = [C_1, C_2, \ldots, C_n]$ where $C_i = (P_i + K_i) \bmod 26$ for any $i \in \{1, 2, \ldots, n\}$. This code is then presented to the user as a sequence of letters again. To make things easier, only uppercase alphabetic letters should be encrypted and all other characters (such as digits, spaces, commas, etc.) are not encrypted. The following example illustrates this using the pass phrase "TIGER":

Plain text:	STUDENTS, SOLVE THE ASSIGNMENT WELL AND FAST!
Key:	TIGERTIG, ERTIG ERT IGERTIGERT IGER TIG ERTI!
Code:	LBAHVGBY, WFEDK XYX IYWZZVSIEM EKPC TVJ JRLB!

To increase the security of the cipher, we add a second cryptographic technique called spiral cipher. The encrypted message from above will be passed as plain text to this new cipher. The spiral cipher takes the text and writes it row by row into a quadratic matrix. It then generates the encrypted message by reading it out in a clockwise spiral

pattern starting in the right top corner of the matrix. The size of the matrix should be large enough to store the entire text, but not larger than needed. If the text is smaller than the number of cells in the matrix, the remaining cells are filled with spaces. Note that this cipher does not require a user-defined key.

L	B	A	H	V	G	B
Y	,		W	F	E	D
K		X	Y	X		I
Y	W	Z	Z	V	S	I
E	M		E	K	P	C
	T	V	J		J	R
L	B	!				

Plain text: LBAHVGBY, WFEDK XYX IYWZZVSIEM EKPC TVJ JRLB!
Code: BDIICR !BL EYKYLBAHVGE SPJ JVTMW , WFXVKE ZXYZ

1.1 To do

1. Create a new project in EiffelStudion.

2. Implement a **deferred class** *CIPHER* that has two deferred features: *encrypt* and *decrypt*. Then implement a class *VIGENERE_CIPHER* that uses the cryptographic technique of the Vigenère cipher described above to encrypt and decrypt messages. Also implement a class *SPIRAL_CIPHER* that implements the spiral cipher technique from above. Both classes should inherit from *CIPHER* and effect its deferred features.

3. Write an effective class *COMBINED_CIPHER* inheriting from *CIPHER*. A combined cipher stores a list of ciphers (descendants of *CIPHER*). Its *encrypt* feature takes the message given as argument and encrypts it using the first cipher of the list. Then it uses the outcome of this encryption as input to the second cipher, and so on. The *decrypt* feature reverses this process.

4. Create an instance of *COMBINED_CIPHER* and add an instance of *VIGENERE_CIPHER* as its first cipher and an instance of *SPIRAL_CIPHER* as second cipher. Encrypt the message "MYLASTASSIGNMENT" using the pass phrase "BUSY" with your combined cipher and write the encrypted message into the line called "Pass phrase" of Step 5:
   Pass phrase: BUSY
   Message: MYLASTASSIGNMENT

5. Use the encrypted message from Step 4 as pass phrase to decrypt the code below. Note that the code is available on the Internet to help you copy paste it into your application `https://drive.google.com/open?id=0B1GMHm59JFjqeEhYVEpZY2dnajA`