CSCI 3675 – Principles of Programming Languages
Fall 2021
Homework 3 – Vigenère Cipher with Haskell[1]
Due Wednesday, October 13, at 11:59 PM

1 Background

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence. This cipher is an example of **monoalphabetic substitution cipher** because it uses only one cipher alphabet per message.

To confuse potential cryptanalysts, Leon Battista Alberti (born in 1404) proposed using two or more cipher alphabets and switching between them during encryption (see Figure 1). To understand how the Leon Battista Alberti cipher works, let us encipher the message **hello**. Encrypt the first letter **h** with the first cipher alphabet, the second letter **e** with the second cipher alphabet, the third letter **l** with the first cipher alphabet, the fourth letter **l** with the second cipher alphabet, and so on. Using this approach the plain text **hello** is enciphered as **AFPAD**.

Plain alphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Cipher alphabet 1	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Cipher alphabet 2	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

Figure 1: Multiple cipher alphabets

Blaise de Vigenère (born 1523) refined Alberti's idea and turned it into a new cipher – **Vigenère cipher** – which uses twenty-six distinct cipher alphabets to encrypt a message (see Figure 2). Each cipher alphabet in the square is shifted by one letter with respect to the previous alphabet. Row 1 represents a cipher alphabet with a Caesar shift of 1, row 2 represents a cipher alphabet with a Caesar shift of 2, and so on.

In the Vigenère cipher, a different row of the square (a different cipher alphabet) is used to encrypt different letters of the message. To decrypt the message, the intended receiver needs to know which row of the square has been used to decipher each letter. This calls for an agreed system of switching between rows, which is achieved by using a *key phrase*. We illustrate this process with an example.

Let us encrypt the message **divert troops to east ridge**, using the key phrase **WHITE**. Position the key phrase (aka keyword) and the plaintext as shown in Figure 3. Each letter in the plaintext is associated with a letter from the keyword. To encrypt the first letter **d**, identify the key letter above it (which is **W**). This letter in turn defines a particular row in the Vigenère square. The row beginning with **W** (i.e., 22) is the cipher alphabet that will be used to find the substitute letter for the plaintext letter **d**. The substitute letter for **d** is **Z**. This process is repeated for the remaining letters in the plaintext. Longer keywords bring more rows into the encryption process and increase the complexity of the cipher. The great advantage of the Vigenère cipher is that it is not vulnerable to the frequency analysis, whereas the Caesar cipher is.

2 Problem Description

Write a program using the Haskell programming language that implements the Vigenère cipher. Your program should:

1. Read a key phrase from keyboard.

[1]This assignment is based on The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, by Simon Singh.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figure 2: Vigenère square used by the Vigenère cipher. The Vigenère cipher is an example of a **polyalphabetic cipher** because it employs several cipher alphabets per message.

Keyword	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I	T	E	W	H	I			
Plaintext	d	i	v	e	r	t	t	r	o	o	p	s	t	o	e	a	s	t	r	i	d	g	e			
Ciphertext	Z	P	D	X	V	P	A	Z	H	S	L	Z	B	H	I	W	Z	B	K	M	Z	N	M			

Figure 3: Vigenère cipher example

2. Read a message from keyboard.
3. Encrypt the message using the key phrase.
4. Print the encrypted message.
5. Decrypt the encrypted message using the key phrase.
6. Print the decrypted message. This should be same as the message read from the keyboard.

Neither the key phrase nor the message should not be hardcoded into your solution. Instead, your program should work with any valid key phrase and message.

Submission

Submit your work as one file containing all your code, via Canvas. The name of the file should be `hw3.hs` and it should compile with GHCi.