VBC Vigenere and Belasso's Cryptography

Intent of this exercise.

This exercise is a direct continuation of the exercise

CC - Cesar's Cryptography

Historic Background

This method was made more efficient in 1553 by Giovan Battista Bellaso. It was reintroduce by Blaise de Vigenére in 1586. Today it is named after the latter. Both are described in www.wikipedia.org.

Figure 1 Blaise de Viginére

Belasso & Viginére's method has a matrix of the English alphabet of 26 letters (see p. 5) and a secret keyword. The keyword must have unique letters, i.e. "will " is not good, but "whisky" is.

We repeat the key as many times as necessary

```
whiskywhiskywhiskywhiskywhisky          KEYWORD
vigineresshouldbebelasso                MESSAGE
```

Now we look up every single letter in the line, which begins with the keyword letter.

KEYWORD LETTER w v → **r**,

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
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

KEYWORD LETTER h i → **p**

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
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

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

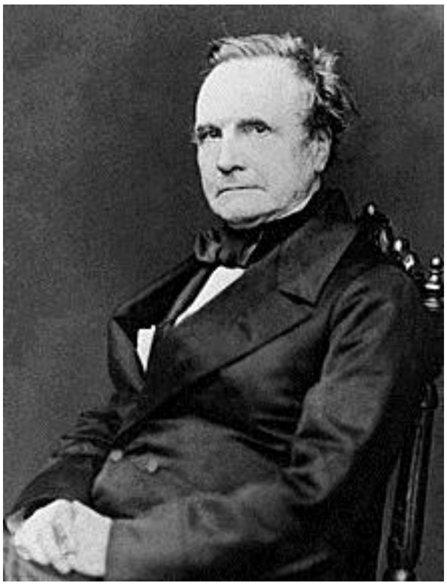
FIGURE 2 VIGINÉRE'S CODE MATRIX

The coded message is then :

`whiskywhiskywhiskywhisk`	Keyword
`viginereshouldbebelasso`	Message
`rpoaxcnlazyshhjwlchhaky`	Coded message (I hope and think ;-)

It took 300 years before this method was broken. Friedrich Kasiski was the first to publish a solution in 1863.

After the death of Charles Babbage (the inventor of a steam based computer, called The Difference Engine) it was found, that he did it as early as 1846. There is a vivid description in the bottom of the wiki page :



https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Remember to use JUnit 5 in your development.

Remember to break the problem down to smaller problems.

VBC EXERCISE:

1. Implement the above crypto algorithm
2. Use a chosen key to encrypt Alice in Wonderland or Moby Dick (*.txt files from www.gutenberg.org on Fronter).
3. Extra :
   a. Are you as smart as Babbage and Kasiski ?
   b. Can you decrypt f.ex. Alice in Wonderland presuming, that you do not know the keyword ?
   c. PS : this is not easy, just for the fun of it.

d. PPS : IT IS EASIER IF YOU CAN FIND THE LENGTH OF THE KEYWORD

Hints:

https://en.wikipedia.org/wiki/Kasiski_examination

HAS A GOOD DESCRIPTION OF KASISKI'S ATTACK ON THE PROBLEM.