1 Caesar Cipher

The Caesar cipher shifts all the letters in a piece of text by a certain number of places. The key for this cipher is a letter which represents the number of place for the shift. So, for example, a key D means “shift 3 places” and a key M means “shift 12 places”. Note that a key A means “do not shift” and a key Z can either mean “shift 25 places” or “shift one place backwards”.

For example, the word “CAESAR” with a shift P becomes “RPTHPG”.

Question 1.1.

(a) What does “CAESAR” become with a shift of F?

(b) What key do we need to make “CAESAR” become “MKOCKB”?

(c) What key do we need to make “CIPHER” become “SYFXUH”?

(d) Use the Caesar cipher to encrypt your first name

With any encryption method, we need to be able to decrypt our ciphertexts.

Question 1.2.

(a) Above we saw that “CAESAR” becomes “RPTHPG” using a key P. Can you find a key that will turn “RPTHPG” back into “CAESAR”?

(b) Use a key N to shift “CAESAR”. What key is need to shift back? What do you notice? Is this true for all texts?

(c) How can we find the decryption key from the encryption key

Caesar ciphers are very simple to create but are also quite easy to crack. One method we can use to crack ciphers is called **Frequency Analysis**. This is where we look at the frequency (*i.e.* the number of times) that each letter appears. The most common letters in the ciphertext are related to the most common letters in the plaintext. The most common letters in the plaintext are likely to be the most common letters in the language.

Question 1.3.

(a) What do you think are the most common letters in English?

(b) What do you think are the least common letters in English?

(c) Is this true for other languages?

Another way to crack ciphers is by looking at one and two letter words. If we see a single letter word in the ciphertext then it is likely to be A or I. Also we can look at repeated letters (such as "t" in "letter").

Question 1.4.

(a) What do you think are the commonest two letter words?

(b) What do you think are the most common repeated letters? What about the least common?

We can now use these methods to crack Caesar Ciphers.

Question 1.5.

(a) Crack the following plaintext

```
TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
```

What encryption key was used?

(b) Make you own ciphertext using the Caesar cipher. Can you crack other people's ciphertexts?

2 Substitution Cipher

To use a substitution cipher we replace (substitute) each letter of the plaintext with a different letter in the cipher text. To use this cipher we need a table of letter replacements. For example, look at the following table

Plain	**C**	**D**	**E**	**H**	**I**	**N**	**P**	**R**	**S**	**T**	**Y**
Cipher	X	J	L	A	Z	E	V	K	H	O	M

Using this substitution, the plaintext

```
THIS SENTENCE IS ENCRYPTED
```

is changed to this ciphertext

```
OAZH HLEOLEXL ZH LEXKMVOLJ
```

Question 2.1.

(a) Check that this substitution is correct

(b) Given this ciphertext `JLXKMVO OAZH` which has been created using the substitution above, can you find the plaintext?

(c) Encrypt some more words using this substitution.

Obviously to make this cipher useful we have to provide substitutions for the whole alphabet. As with the Caesar cipher, we can use frequency analysis to crack substitution ciphers.

Question 2.2. Crack the ciphertext given below

```
D LJELKOKJKOUV COSIYM OL IDMRYM KU CMDCZ KIDV
D CDYLDM COSIYM EJK GY CDV LKOXX JLY PMYQJYVCB
DVDXBLOL KU POVR KIY WULK CUWWUV XYKKYML.
O SMUWOLYR BUJ KIDK O GUJXR JLY DXX KGYVKB LOF
XYKKYML LU KIDK WYDVL KIDK O IDHY TUK KU DRR
YFKMD GUMRL LJCI DL NYXXB DVR AUU.
```

This text contains all 26 letters. To help you crack the cipher, use the table

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**

and the text spaces below

```
- ------------ ------ -- ------ -- ----- ----

- ------  ------ --- -- --- ----- --- ---------

-------- -- ---- --- ---- ------ -------.

- -------- --- ---- - ----- --- --- ------ ---

------- -- ---- ----- ---- - ---- --- -- ---

----- ----- ---- -- ----- --- ---.
```

You will find that the first few letters in the top row of the table spell out a word.

Question 2.3. Use the table below to make your own substitution ciphers. Can you crack other people's ciphers?

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

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

3 Vignère Cipher

For the Vignère cipher we use a word as the key. Suppose that we use the word “KEY” as the key and we want to encrypt the word “CRYPTOGRAPHY”. We repeat the key and line up the repeated key and the cipher text:

Key	*K*	*E*	*Y*	*K*	*E*	*Y*	*K*	*E*	*Y*	*K*	*E*	*Y*
Plaintext	C	R	Y	P	T	O	G	R	A	P	H	Y

Then we use each letter of the key as a shift for the Caesar cipher and encrypt each letter of the plaintext. So, to encrypt the letter ‘C’ in the plaintext we use ‘K’ (a shift of 10) from the key and we get ‘M’. Then, we continue along the text, so, for example, to encrypt ‘H’ in the plaintext we use ‘E’ (a shift of 4) from the key to get ‘L’. Here’s the completed ciphertext:

Key	*K*	*E*	*Y*	*K*	*E*	*Y*	*K*	*E*	*Y*	*K*	*E*	*Y*
Plaintext	C	R	Y	P	T	O	G	R	A	P	H	Y
Ciphertext	**M**	**V**	**W**	**Z**	**X**	**M**	**Q**	**V**	**Y**	**Z**	**L**	**W**

To make the encryption process easier we can have a table of letters to work out the ciphertext — see Table 1. Using this cipher, we do not encrypt spaces or punctuation marks so we often remove them.

Question 3.1.

(a) Use the key “CODE” to encrypt the sentence “TO BE OR NOT TO BE”. Some of the ciphertext is already completed for you:

Key	*C*	*O*	*D*	*E*	*C*	*O*	*D*	*E*	*C*	*O*	*D*	*E*	*C*
Plaintext	T	O	B	E	O	R	N	O	T	T	O	B	E
Ciphertext	**V**	_	_	_	_	**F**	_	_	_	_	**R**	_	_

(b) Use your own key and phrase and encrypt it using the Vignère cipher.

Question 3.2.

(a) With the Caesar and Substitution ciphers we can use frequency analysis to guess some of the letters in the ciphertext. Can we use frequency analysis with the Vignère cipher? Explain your answer using the some of the ciphertexts that you’ve created.

(b) [Harder] Is it possible to use the ciphertext to guess anything about the key? Explain your answer using some ciphertexts.

	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**
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Table 1: Table of letter keys for the Vignère cipher

Question 3.3.

(a) Earlier we used the key “KEY” to encrypt “CRYPTOGRAPHY” to get “MVWZXMQVYZLW”. What key word would turn the ciphertext back into the plaintext? Use Table 1 to help.

(b) Now work out the keys to reverse the other ciphertexts.

(c) [Very Hard!] Here is some text that has been encrypted:

```
OINCHHFIAFYASZGUIVJCRKIWLLKJ
```

The plaintext begins with the letters `WELLDONE`. Use this piece of text, called a **crib**, to work out the key and the whole of the plaintext. Can this technique still be used if the crib is not at the start of the text?

4 RSA Encryption

RSA encryption is much more complicated than the encryption methods we have seen so far. The RSA method encrypts numbers rather than pieces of text. Here is a description of what you must do to use RSA encryption

(a) Pick two large prime numbers p and q

(b) Work out the products $n = p \times q$ and $k = (p - 1) \times (q - 1)$

(c) Pick a public key e which does not have any factors in common (apart from 1 of course) with the number k

(d) Find a private key d so that $d \times e = 1 \pmod{k}$

(e) To encrypt a number m work out $m^e \pmod{n}$

(f) To decrypt a number c work out $c^d \pmod{n}$

You will see that there is lots of Maths involved to use this encryption. Let us have a look at the Maths behind this encryption method.

First, a reminder about factors. Let us look at the factors of 12. A number is a **factor** of 12 if it divides exactly into 12 with no remainder. So, the factors of 12 are 1,2,3,4,6 and 12. Two things to note: (a) 1 and the number itself are always factors and (b) factors usually occur in pairs.

Question 4.1.

(a) find the factors of 30

(b) find the factors of 100

(c) find the factors of 23

You should notice that 23 has exactly *two* factors. A number is **prime** if it has exactly *two* factors — so, for example, 2 and 3 are prime but 1 and 4 are not prime.

Question 4.2.

(a) find all the prime numbers that are less than 20

(b) find a three digit prime number

(c) can we find prime numbers bigger than 1 million? bigger than 1 billion?

For RSA we need two big prime numbers. Currently to make the encryption secure we have to find prime numbers than have more than 600 digits!

You will have seen in the description of RSA expressions like this:

$$a \pmod{n}$$

The word "mod" stands for modulus which is another word for remainder. So, if we had

$$17 \pmod{5}$$

this means "give me the remainder when 17 is divided by 5" and so

$$17 \pmod{5} = 2$$

because

$$17 = (3 \times 5) + 2$$

Some more examples for you:

$$29 \pmod{6} = 5 \qquad 49 \pmod{10} = 9 \qquad 35 \pmod{7} = 0$$

Some calculators allow you to work out mod using the fractions button $\boxed{a\ b/c}$. So if you type

$$\boxed{2}\ \boxed{9}\ \boxed{a\ b/c}\ \boxed{6}\ \boxed{=}$$

you get an answer $\boxed{4\lrcorner 5\lrcorner 6}$ and the penultimate number 5 gives us the remainder. This does not always work though as sometimes the fraction is cancelled down.

Question 4.3. Fill in the missing numbers * below

$$25 \pmod{6} = * \qquad 31 \pmod{12} = *$$

$$18 \pmod{*} = 5 \qquad * \pmod{3} = 1$$

An example Let us now go through an example in which we use RSA encryption by following the steps we saw earlier.

(a) First we need to pick two primes, so let's take $p = 7$ and $q = 13$

(b) So now $n = 7 \times 13 = 91$ and $k = 6 \times 12 = 72$.

(c) For the public key, we will try $e = 5$ which does not have any factors in common with 72.

(d) Now the private d is 29 — if we work out $d \times e$ we get $5 \times 29 = 145$. Now $145 = 2 \times 72 + 1$ and so $d \times e = 1 \pmod{72}$. So d is a suitable private key.

(e) Let's encrypt 23 so we need to work out $23^5 \pmod{91}$. If we work out 23^5 then we get 6436343 — it quite hard then to work out what the remainder would be when we divide this by 91. Instead we can work the power in stages and find the remainder at each stage. So first do

$$23^2 = 529 = 5 \times 91 + 74 = 74 \pmod{91}$$

Now we can do the other powers

$$23^3 = 23^2 \times 23 = 74 \times 23 \pmod{91} = 1702 = 64 \pmod{91}$$

$$23^4 = 23^3 \times 23 = 64 \times 23 \pmod{91} = 1472 = 16 \pmod{91}$$

$$23^5 = 23^4 \times 23 = 16 \times 23 \pmod{91} = 368 = 4 \pmod{91}$$

So when we encrypt 23 using the key 5 we get an answer of 4.

(f) Let's now undo this encryption, so when we use the private key to work $4^{29} \pmod{91}$ we should get our original number of 23. To work 4^{29} we could use the same method as before but this would take 28 steps. However we can do it fewer steps. Since $29 = 1 + 4 + 8 + 16$ we can write:

$$4^{29} \pmod{91} = 4^1 \times 4^4 \times 4^8 \times 4^{16} \pmod{91}$$

So

$$4^4 = 256 = 74 \pmod{91}$$

$$4^8 = 4^4 \times 4^4 = 74 \times 74 \pmod{91} = 5476 = 16 \pmod{91}$$

$$4^{16} = 4^8 \times 4^8 = 16 \times 16 \pmod{91} = 256 = 74 \pmod{91}$$

So,

$$4^{29} = 4 \times 74 \times 16 \times 74 \pmod{91}$$

We can do this in stages

$$\begin{aligned}
4^{29} &= 296 \times 16 \times 74 \pmod{91} \\
&= 23 \times 16 \times 74 \pmod{91} \\
&= 368 \times 74 \pmod{91} \\
&= 4 \times 74 \pmod{91} \\
&= 296 \pmod{91} \\
&= 23 \pmod{91}
\end{aligned}$$

So we get our original number back.

Question 4.4.

(a) Using the same public key 5 encrypt the number 5 using RSA

(b) Using the private key 29, undo the encrpytion

Question 4.5. Now, let us take $p = 5$ and $q = 11$. So $n = 55$ and $k = 40$.

(a) Suppose that we take the public key $e = 3$. Check that $d = 27$ is a suitable private key.

(b) Encrypt 18 using the public key 3. You should find that your final answer is 2.

(c) What should be the answer to $2^{27} \pmod{55}$? Check that this is true.

As a final note about RSA encryption, up to now we have looked at numbers rather than letters. We can change letters into a single number in lots of different ways. For instance, we can take A=1, Z=26 and "Space" to be 27. Then we can think of a sequence of letters as a number in Base 28. Just as 245 is really $(2 \times 10^2) + (4 \times 10^1) + (5 \times 10^0)$ then we can take "BCD" to be

$$(2 \times 28^2) + (3 \times 28^1) + (4 \times 28^0) = 1568 + 84 + 4 = 1656$$

Commands for the Haskell program

You must type in the commands exactly as they are written. Be sure to include spaces and use lower and upper case letters correctly. A useful command is `$$` which repeats the last result. For example,

```
Main> 35 + 78
113
Main> 4 * $$
452
```

The last calculation works out $4 \times (35 + 78)$.

Some example sentences

```
Main> qwe
"THE QUICK BROWN FOX JUMPED OVER THE LAZY SLEEPING DOG"
Main> shake
"TO BE OR NOT TO BE THAT IS THE QUESTION"
```

The first one contains all 26 letters and the second has some short words.

Caesar cipher

To shift the word “HELLO” using a key ’R’, type

```
Main> caesar ’R’ "HELLO"
"YVCCF"
```

To undo the Caesar cipher, we use the function `uncaesar`:

```
Main> uncaesar ’R’ "YVCCF"
"HELLO"
```

We can do a frequency analysis using the function `analyse`:

```
Main> analyse qwe
[(1,’A’),(1,’B’),(1,’C’),(2,’D’),(6,’E’),(1,’F’),(2,’G’),
(2,’H’),(2,’I’),(1,’J’),(1,’K’),(2,’L’),(1,’M’),(2,’N’),
(4,’O’),(2,’P’),(1,’Q’),(2,’R’),(1,’S’),(2,’T’),(2,’U’),
(1,’V’),(1,’W’),(1,’X’),(1,’Y’),(1,’Z’)]
```

This gives us a list of pairs (frequency, letter). It is not always easy to see the results so we can use the function `printPairs` to print the results:

```
Main> printPairs analyse qwe
'A': 1
'B': 1
...
```

To show the top 4 frequencies:

```
Main> topFreq 4 (analyse qwe)
'E': 6
'O': 4
'U': 2
'T': 2
```

(We can change 4 to another number between 1 and 26.) Remember that we can replace `qwe` by any text string in the commands above.

To find the most frequent letter in a string, we can type:

```
Main> freqLet "HELLO WORLD"
'L'
```

The function `crackCaesar` tries to guess the plaintext from a ciphertext:

```
Main> crackCaesar "YMJ HFY XFY TS YMJ RFY"
"THE CAT SAT ON THE MAT"
```

and just to confirm:

```
Main> caesar 'F' "THE CAT SAT ON THE MAT"
"YMJ HFY XFY TS YMJ RFY"
```

Substitution Cipher

We can check a string is suitable as a key by using `checkKey`:

```
Main> checkKey "KJHGTYRUIOPQWSAZMFCVBDELNX"
True
Main> checkKey "KJHGTYRUIOPQWSAZMFCVBDELN"
False
Main> checkKey "KJHGTYRUIOPQWSAZMFCVBDELNXG"
False
```

The first key is suitable, the second has two few letters and the third has G twice.

We can create a substitution key by giving the first few letters:

```
Main> createKey "CIPHER"
"CIPHERABDFGJKLMNOQSTUVWXYZ"
Main> createKey "CRYPTOGRAPHY"
"CRYPTOGAHBDEFIJKLMNQSUVWXZ"
```

Here are some examples for using the substitution cipher:

```
Main> subst "KJHGTYRUIOPQWSAZMFCVBDELNX" "HELLO WORLD"
"UTQQA EAFQG"
Main> subst (createKey "CIPHER") "HELLO WORLD"
"BEJJM WMQJH"
Main> subst "KJHGTYRUIOPQWSAZMFCVBDELNX" qwe
"VUT MBIHP JFAES YAL OBWZTG ADTF VUT QKXN CQTTZISR GAR"
```

Here's a function that undoes the cipher:

```
Main> unsubst (createKey "CIPHER") "BEJJM WMQJH"
"HELLO WORLD"
```

Vignère

To use the Vignère with key “KEY” and plaintext “HELLO WORLD”:

```
Main> vig "KEY" "HELLO WORLD"
"RIJVSUYVJN"
```

Note that the space has been removed.

To undo the cipher

```
Main> unvig "KEY" "RIJVSUYVJN"
"HELLOWORLD"
```

There is also a function called `revKey` which finds the key with which we can undo a Vignère cipher:

```
Main> revKey "KEY"
"QWC"
```

and thus

```
Main> vig "QWC" "RIJVSUYVJN"
"HELLOWORLD"
```

If we know some of the plaintext then it possible to guess the key by using the command `crackVig`. So if we had

```
Main> vig "KEY" "THISISENCRYPTED"
"DLGCMQORABCNDIB"
```

then `crackVig` prints out a list of possible keys.

```
Main> crackVig "ENCRYPT" "DLGCMQORABCNDIB"
["KEY"]
```

Sometimes it is not possible to guess a key

```
Main> crackVig "THIS" "DLGCMQORABCNDIB"
[]
```

RSA Encryption

To do RSA encryption we need to work out an expression such as:

$$13^8 \pmod{55}$$

To work out this, we can do:

```
Main> 13^8
815730721
```

and then

```
Main> mod $$ 55
36
```

Since we need to do this calculation many times, there is a function `power` which work this out:

```
Main> power 13 8 55
36
```

Example Let's work through an example of RSA encryption. We take $p = 7$ and $q = 13$ so $n = 7 \times 13 = 91$ and $k = 6 \times 12 = 72$. We now need to pick a public key e which does not have any factors in common with 72. Using e we need a private key d such that $d \times e = 1 \pmod{72}$. Suppose we take $e = 5$ and to work out the private key we do

```
Main> private 5 7 13
29
```

The function `private` needs three things: the first is our public key and the last two are our prime numbers. We can check that $d = 29$ is a suitable key:

```
Main> mod (29*5) 72
1
```

If we do not pick a good public key e then we will get an error message

```
Main> private 6 7 13
Program error: Not coprime
```

Now let's encrypt the number 23 using the public key $e = 5$. We want to work out $23^5 \pmod{91}$ so we type

```
Main> power 23 5 91
4
```

Now to decrypt using the private key $d = 29$:

```
Main> power 4 29 91
23
```

We can apply RSA to letters by changing the letters into numbers. So using the primes 7 and 13 and public key 23.

```
Main> rsa "WELL" 5 (7*13)
[4,31,38,38]
```

Note that "W", which is changed to 23, is encrypted to 4, as above. To change this back, we use the private key 29:

```
Main> unrsa [4,31,38,38] 29 (7*13)
"WELL"
```

There are some sample keys which can be used. Typing in `p1` and `q1` will give you two prime numbers and their product is defined to `n1`. A suitable public key is `e1` and the corresponding private key is `d1`.

```
Main> p1
241679
Main> q1
8123471
Main> n1
1963272347809
Main> p1 * q1
```

```
1963272347809
Main> e1
3
Main> d1
1308842655107
Main> private e1 p1 q1
1308842655107
```

So we can try

```
Main> rsa qwe e1 n1
[1244282649599,1568503221394,684458173516,1772351482757,
346990991405,1861579902643,538356473688]
```

Then to decode

```
Main> unrsa [1244282649599,1568503221394,
684458173516,1772351482757,
346990991405,1861579902643,538356473688] d1 n1
"THE QUICK BROWN FOX JUMPED OVER THE LAZY SLEEPING DOG"
```

There's some larger primes `p2` and `q2` with public key `e2` and private key `d2`. An example using the larger primes and `shake`:

```
Main> rsa shake e2 n2
[944552924503602346111,24180811974541611992954,
19885192145733533765925]

Main> unrsa $$ d2 n2
"TO BE OR NOT TO BE THAT IS THE QUESTION"
```

(where `$$` means the last calculation).

Sample texts

In the program, there are a few sample texts that you can use to try things out. As well as `qwe` and `shake` there is the opening paragraph from a Poirot story by Agatha Christie:

```
Main> poirot
"Pure chance led my friend Hercule Poirot, formerly chief of
the Belgian force, to be connected with the Styles case. His
success brought him notoriety, and he decided to devote
```

```
himself to the solving of problems in crime. Having been
wounded in the Somme and invalided out of the Army, I finally
took up my quarters with him in London. Since I have a
first-hand knowledge of most of his cases, it has been
suggested to me that I select some of the most interesting and
place them on record. In doing so, I feel that I cannot do
better than begin with that strange tangle which aroused such
widespread public interest at the time. I refer to the affair
at the Victory Ball. "
```

Also, there is the text for Question 2.2:

```
Main> substExample
"D LJELKOKJKOUV COSIYM OL IDMRYM KU CMDCZ KIDV D CDYLDM
COSIYM EJK GY CDV LKOXX JLY PMYQJYVCB DVDXBLOL KU POVR
KIY WULK CUWWUV XYKKYML. O SMUWOLYR BUJ KIDK O GUJXR JLY
DXX KGYVKB LOF XYKKYML LU KIDK WYDVL KIDK O IDHY TUK KU
DRR YFKMD GUMRL LJCI DL NYXXB DVR AUU."
```

You may want to do a frequency analysis on this:

```
Main> analyse substExample
[(1,'A'),(5,'B'),(9,'C'),(20,'D'),(2,'E'),(2,'F'),(4,'G'),
(1,'H'),(10,'I'),(9,'J'),(25,'K'),(19,'L'),(12,'M'),(1,'N'),
(13,'O'),(2,'P'),(1,'Q'),(8,'R'),(3,'S'),(1,'T'),(15,'U'),
(10,'V'),(5,'W'),(10,'X'),(20,'Y'),(1,'Z')]
```

and the top five frequencies are:

```
Main> topFreq 5 (analyse substExample)
'K': 25
'Y': 20
'D': 20
'L': 19
'U': 15
```

You may also want to find all the three letter words in the text:

```
Main> sizeWord 3 substExample
["EJK","CDV","JLY","KIY","BUJ","JLY","DXX","LOF",
"TUK","DRR","DVR"]
```

There are some texts which have encrypted using the Vignère cipher. The texts `poirotVig1` and `poirotVig2` are encrypted versions of the `poirot` using two different keys. For example,

```
Main> poirotVig1
"WUJXKUGFJEDXLZEXYIWGLUKJJUDXXBOJVTXHZZKJSYUAQRLGMTZXJRRYPAFYW
EIWAOTXKBTFLCLXLJOLOTZXAGEDLSUTARNAZSMVKRYKIRGNOUZZPMFHBBXALTQ
TVQNWKEUBLRJLVDWOWGKZPMKXTSZGAHWLWYBAUGGYXEUTSEELQAIJPMWAIIOFN
BWXVJUMUDWWQAZZLSGFURGFKIFOIYOVLDGNBBLLOESKULOXPNSETLZGVKMIULW
MHRLXZFCAAHZBUVTDVNVHVFOFJEAAIIKSMIJLBUGFKKFHEYKVNEGYUBYLVFZBA
PGKLSAMPNYTLEFLCTMWZTWWBBSWAHSMQFKDLCLLWZKGMTZXUBYLPNLXZRYLPNY
TVQVDHCWMPRSGURWVWEJAUDGBVTYGPFWXTGNSAIUTVAULKOTXBGKJAHSGJRMAU
WAMPGNSASLKIAMWAAFZTRCZPCZTZBAKLDKNKUCAKEKIZRGVWUTEQPOFAEJXAGG
LAHWMQZKAYEXXZGULOESYNNOJHTLAMIOUAOJRJNRD"
```

See if you can work out what the keys are.

It is possible to work out the length of the key of a Vignère by working out the lengths between matching characters. For example,

```
Main> keyLengths poirotVig1
[(24,1),(18,2),(23,3),(25,4),(20,5),(23,6),(20,7),
(30,8),(13,9),(14,10),(18,11),(14,12),(20,13),(25,14),
(21,15),(45,16),(18,17),(20,18),(15,19),(19,20),(28,21),
(18,22),(17,23),(29,24),(26,25),(15,26),(19,27),(18,28),
(18,29),(13,30)]
```

Looking at the top 3 frequencies:

```
Main> topFreq 3 (keyLengths poirotVig1)
16:  45
8:   30
24:  29
```

This means that the key is likely to have length 8, 16 or 24. Since 8 is a factor of both 16 and 24 then the most likely key length is 8. You may also try to find the keys by using a crib.

There is another Vignère encrypted text:

```
Main> vigExample
"OVPWAAAVGVDAHEDSUHPHZIRAKYXMSLIIIMRKYGLSEDHZGOVPQEDFFPHCZQPUH
CTISQRVMGVVJBOWLQMJMJCOTYUHVLOWWOAMBULYWCHGFSUTOSLFLAHYXMGNKIE
HJMCSYUIOCXGDGTQKQOTAJHSHVFVVRNHZZIPHYXDFHDRPGSXISLWLFVVBMQWRE
WGRGYGEDVFSUPVZVLRSPIBNYWBMZHYXNOXHHUFVVOWZQ"
```

Can you decrypt this?

Answers

Caesar Cipher

Question 1.1

(a) HFJXFW

(b) The key is ‘K’

(c) The key is ‘Q’

Question 1.2

(a) We need a shift of ‘L’

(b) After a shift of ‘N’, “CAESAR” becomes “PNRFNE”. The same key ‘N’ shifts the ciphertext back to “CAESAR”. This is true for all texts. It is also true for the key ‘A’

(c) The encryption and decryption keys occur in pairs (apart from ‘A’ and ‘N’). The pairs are (‘B’,‘Z’), (‘C’,‘Y’) and so until (‘M’,‘O’).

Question 1.3

(a) The most common letters are E,T,A and I.

(b) The least common letters are Z, X, J and Q.

(c) This is not true for all languages.

Question 1.4

(a) Words such as “of”, “to”, “he”, “we”, “it” and “is” are common in English.

(b) Letters such as ‘T’, ‘P’, ‘S’, ‘L’, ‘E’ and ‘O’ are commonly repeated letters. But letters such as ‘Q’, ‘J’ and ”W” are not commonly repeated in English words.

Question 1.5

(a) The plaintext decrypts to “CAESAR CIPHERS ARE QUITE EASY TO CRACK” and the key was ‘R’. Note that ‘V’ and ‘R’ are the most common letters in the ciphertext: ‘V’ corresponds to ‘E’ and ‘R’ corresponds to ‘A’.

Substitution Cipher

Question 2.1

(b) DECRYPT THIS

Question 2.2 The plaintext is

A SUBSTITUTION CIPHER IS HARDER TO CRACK THAN A CAESAR CIPHER BUT WE CAN STILL USE FREQUENCY ANALYSIS TO FIND THE MOST COMMON LETTERS. I PROMISED YOU THAT I WOULD USE ALL TWENTY SIX LETTERS SO THAT MEANS THAT I HAVE GOT TO ADD EXTRA WORDS SUCH AS JELLY AND ZOO.

Here's the key:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
D	E	C	R	Y	P	T	I	O	N	Z	X	W
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
V	U	S	Q	M	L	K	J	H	G	F	B	A

It was created by using the word "DECRYPTION" and the rest of the alphabet in reverse order.

Vignère Cipher

Question 3.1

(a) VCEIQFQSVHRFG

Question 3.2

(a) We cannot use frequency analysis for this cipher. Look at the encryption of TOBEORNOTTOBE in the previous question. The letter O is encrypted to the letters C, Q, S and R. While in the ciphertext, we have two Qs which come from the letters O and N.

(b) We can sometimes guess the length of the key by looking at letters which are repeated in the ciphertext and finding the length of the repeat. In the CRYPTOGRAPHY example earlier, R is encrypted to V twice — with a repeat length of 6 — Y is encrypted to W twice — with a repeat length of 9. So since 3 is a factor of 6 and 9 we could guess that the key length is 3 (which it is!).

We have to be careful with this method as sometimes we can get false matches — for example, there are two letter Ms in the ciphertext (with a repeat length of 5) but these come from different letters in the plaintext.

Question 3.3

(a) The reverse key for "KEY" is "QWC". Using the table, for each letter of the key you look along the row of the table for that letter. When you find the letter A, you look at what column you are in. So looking at the row for 'K', you will see that 'A' is in column 'Q'.

(b) For example, the reverse key for "CODE" is "YMXW"

(c) You know that the first letter in the plaintext is W, the letter in the cipher text is O, so using the table, looking along row 'W' you find 'O' in column 'S'. So the first letter of the key is 'S'.

Now look at row 'E' until you find 'I' - this happens in column 'E' — so the second letter of the key is 'E'. Continuing this process gets you the characters "SECRETSE" — so it looks like the key is "SECRET". Using this key, the plaintext is "WELLDONEYOUHAVEDECRYPT-EDTHIS".

This technique can be used with any crib. What you do is to try the crib at each position of the ciphertext and work out what the key would be. If the key starts to repeat then we are likely to have found the correct key.

RSA encryption

Question 4.1

(a) 1,2,3,5,6,10,15,30

(b) 1,2,4,5,10,20,25,50,100

(c) 1,23

Question 4.2

(a) 2,3,5,7,11,13,17,19

(b) 101 is the smallest and 997 is the biggest

(c) There are primes numbers that are bigger than any number you can think of as there are infinitely many primes. Whether you can actually find such a prime is a different matter. Many computer scientist regularly try to find the next biggest prime number.

Question 4.3

$$25 \pmod 6 = 1 \qquad 31 \pmod{12} = 7 \qquad 18 \pmod{13} = 5$$

For the last one, there are many different possible answers: 1,4,7,11 etc.

Question 4.4

(a) We need to work out $5^5 \pmod{91}$ So

$$5^3 = 5 \times 5 \times 5 = 125 = 34 \pmod{91}$$

$$5^4 = 5^3 \times 5 = 34 \times 5 = 170 = 79 \pmod{91}$$

$$5^5 = 5^4 \times 5 = 79 \times 5 = 395 = 31 \pmod{91}$$

(b) We need to work out $31^{29} \pmod{91}$.

$$\begin{array}{l} 31^2 = 31 \times 31 = 961 = 51 \pmod{91} \\ 31^4 = 31^2 \times 31^2 = 51 \times 51 \pmod{91} = 2601 = 53 \pmod{91} \\ 31^8 = 31^4 \times 31^4 = 53 \times 53 \pmod{91} 2809 = 79 \pmod{91} \\ 31^{16} = 31^8 \times 31^8 = 79 \times 79 = 6241 = 53 \pmod{91} \end{array}$$

So

$$\begin{aligned}
31^{29} &= 31^1 \times 31^4 \times 31^8 \times 31^{16} \pmod{91} \\
&= 31 \times 53 \times 79 \times 53 \pmod{91} \\
&= 1643 \times 4187 \pmod{91} \\
&= 5 \times 1 \pmod{91} \\
&= 5
\end{aligned}$$

which is our original number.

Question 4.5

(a) We need $3 \times 27 = 1 \pmod{40}$ and

$$3 \times 27 = 81 = 2 \times 40 + 1 = 1 \pmod{40}$$

(b)

$$\begin{aligned}
18^3 \pmod{55} &= 18^2 \times 18 \pmod{55} \\
&= 324 \times 18 \pmod{55} \\
&= 49 \times 18 \pmod{55} \\
&= 882\ (= 16 \times 55 + 2) \\
&= 2 \pmod{55}
\end{aligned}$$

(c) The answer to $2^{27} \pmod{55}$ should be 18.

$$\begin{aligned}
2^{27} \pmod{55} &= 2^6 \times 2^6 \times 2^6 \times 2^6 \times 2^3 \pmod{55} \\
&= 64 \times 64 \times 64 \times 64 \times 8 \pmod{55} \\
&= 9 \times 9 \times 9 \times 9 \times 8 \pmod{55} \\
&= 81 \times 81 \times 8 \pmod{55} \\
&= 26 \times 26 \times 8 \pmod{55} \\
&= 26 \times 208 \pmod{55} \\
&= 26 \times 43 \pmod{55} \\
&= 1118 \pmod{55} \\
&= 18 \pmod{55}
\end{aligned}$$

There are many other ways to work out this answer.