

## 4.18

This program has two parts, determined by the command line argument passed in. If the user passes in 'a', it will perform parts a-d of 4.18. It will end with a table of large mutual indices of coincidence and shift relations ask the user to solve the system of equations.

Since it is not included in the program I will include the system of equations solution here. The result of part 'a' includes the estimate key length of 7 and:

$B_i$	$B_j$	$Shift$
1	2	17
1	3	24
1	6	17
2	3	7
2	4	2
2	5	24
2	6	0
3	4	21
3	6	19

We can solve from this and get:

$$\begin{aligned}
 B_2 &= B_1 + 9 \\
 B_3 &= B_1 + 2 \\
 B_4 &= B_1 + 7 \\
 B_5 &= B_1 + 22 \\
 B_6 &= B_1 + 9 \\
 B_7 &= B_1 + 25
 \end{aligned}$$

The second part will be triggered if the user passes in 'b [keyLengthFromPartA] [letterShift1] [letterShift2] ...'. Using the results from above, we can enter in 'java Vigenere b 7 9 2 7 22 9 25', and see that our result is the 5th row down, with the keyword 'england' and the decrypted text: "it is to be questioned whether in the whole length and breadth of the world there is a more admirable spot for a man in love to pass a day or two than the typical english village it combines the comforts of civilization with the restfulness of

solitude in a manner equalled by no other spot except the new york public library”