Exercises: Breaking Vigenère

1. Here is a text, in blocks of ten letters, sent using the Vigenère cipher.

```
TVIMRFXLLN  SRXXKPRTXU  KPRJZYJWSV  KCMMGJKCMM  JNBWYTNELC  CMAZTHUBVJ
ROELRXMBVQ  AQRMBGGNXP  VZLRTMKXYG  VYPWHCHOCL  RDIYTBNYMI  EQFNBHXBUO
GAJBBNTJGM  ANTLIGCUMN  VZEUEFVLBB  XLZVFOWYYQ  FHEUESRZLQ  ZBUUNNNIXO
GALXBTXMDI  YRAUELPRHM  VLBTMBVTRZ  MYIJRYBXVP  VSTHUPRYEY  GBBTGIKSAU
PCEOUKPUJA  CKVCRTAUME  EWJOGAYMJG  LZRUBALHFB  XTHQZVTNXQ  FCYJUYNWXK
GCEISKPBFC  EYMCDMOEFL  JLHXLFVGFY  VLVIZGLMYM  BVXHVLGNXZ  IWAZWIFZGU
IOKWHZMBVU  VRDVFBGRXM  EWEZAUKPRC  HOCLFVXHUB  UKGYOBSKPQ  VMXYUYZVTV
KIULRJTHUX  VTVBVLOEAC  JKBALCELHJ  EYPPRIHOCL  AZDHFEGNTN  RBGNBMMMEE
FIDMAZIYFX  YKFYVBVTZC  EARIKYKIYR  HPVZGNXWFC  AZKSNMEKAI  CLVTZOGBUK
BLXTNYLYJI  AJLUPQAMBH  YCFNXXMWVI  XMKWUGKLPX  BZMYIBUKUI  PEUUECMMQ
```

Using the Kasiski test, give any repetitions of three or more letters that you find, and hence any possible key lengths.

KPR 6, 369; KCMM 6; CMM 558; MAZ 432; HUB 342; RXM 313; GNX 270; GNX 435; CHOCL 294; DIY 87; OGA 60, 84, 141; EUE 20; VLB 54; IYR 318; MBV 135 6 is a common divisor of many of these gaps, so the keyword may have length 2, 3 or 6.

2. The text is 599 letters long. Below is the number of occurrences of each letter in the ciphertext. Calculate the index of coincidence.

	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
occurances	22	36	24	6	27	20	24	20	24	18	25	32	36	22	14	18	10	25	8	23	31	35	13	30	32	24

$$IC = \left(\frac{22}{599}\right)^2 + \left(\frac{36}{599}\right)^2 + \left(\frac{24}{599}\right)^2 + \left(\frac{6}{599}\right)^2 + \left(\frac{27}{599}\right)^2 + \left(\frac{20}{599}\right)^2 + \left(\frac{24}{599}\right)^2 + \left(\frac{20}{599}\right)^2 + \left(\frac{24}{599}\right)^2 + \left(\frac{18}{599}\right)^2 + \left(\frac{25}{599}\right)^2 + \left(\frac{32}{599}\right)^2 + \left(\frac{36}{599}\right)^2 + \left(\frac{22}{599}\right)^2 + \left(\frac{14}{599}\right)^2 + \left(\frac{18}{599}\right)^2 + \left(\frac{10}{599}\right)^2 + \left(\frac{25}{599}\right)^2 + \left(\frac{8}{599}\right)^2 + \left(\frac{23}{599}\right)^2 + \left(\frac{31}{599}\right)^2 + \left(\frac{35}{599}\right)^2 + \left(\frac{13}{599}\right)^2 + \left(\frac{30}{599}\right)^2 + \left(\frac{32}{599}\right)^2 + \left(\frac{24}{599}\right)^2 = 0.0432523878$$

3. Using the Friedman test, approximate the length of the keyword.

$$l = \frac{0.027}{(IC - 0.038)} = \frac{0.027}{(0.04325 - 0.038)} = 5.64$$

4. If possible, determine the keyword and decrypt the ciphertext (*You may simply name the book*).

   'KPR', 'GNX' and 'MBV' are all the trigram 'the'. 'CHOCL' is the word 'would', while 'MAZ' is 'ent', 'OGA' is 'ing' and 'IYR' is 'all'. The most common divisor of the repetitions is 6. Working back you may determine the keyword is **TURING** and the text is;

   'A breeze ruffled the neat hedges of Privet Drive, which lay silent and tidy under the inky sky, the very last place you would expect astonishing things to happen. Harry Potter rolled over inside his blankets without waking up. One small hand closed on the letter beside him and he slept on, not knowing he was special, not knowing he was famous, not knowing he would be woken in a few hours' time by Mrs. Dursley's scream as she opened the front door to put out the milk bottles, nor that he would spend the next few weeks being prodded and pinched by his cousin Dudley... He couldn't know that at this very moment, people meeting in secret all over the country were holding up their glasses and saying in hushed voices: "To Harry Potter – the boy who lived!".'