Solving Quagmire 3 by using symmetry.

The Quagmire 3 cipher. Quagmire 3 is a polyalphabetic cipher with strong symmetries that can be used to solve the cipher. The symmetries arise because all the mixed alphabets are the same. It is usual for the number of enciphering alphabets to be between 5 and 12. A matrix is built in which plaintext is represented by the mixed alphabet, and then the enciphering alphabets are slid relative to the plain by varying amounts. Below is an example with 6 enciphering alphabets (a period of 6):

```
Plain     strongcipheabdfjklmquvwxyz
Cipher 1  JKLMQUVWXYZSTRONGCIPHEABDF
Cipher 2  ZSTRONGCIPHEABDFJKLMQUVWXY
Cipher 3  STRONGCIPHEABDFJKLMQUVWXYZ
Cipher 4  LMQUVWXYZSTRONGCIPHEABDFJK
Cipher 5  VWXYZSTRONGCIPHEABDFJKLMQU
Cipher 6  YZSTRONGCIPHEABDFJKLMQUVWX
```

The cipher alphabets have been shifted left by 15,25,0,18,6 and 9 placed respectively.

To encipher the word 'beneath', one enciphers 'b' with the first cipher alphabet, 'e' with the second, and so on, using the first cipher alphabet again for the 7th letter 'h': the ciphertext is thus THNTCZY.

If you pick any four letters at the corners of a rectangle in the matrix you will find that any two letters in the same column or the same row are equally apart. For example I have highlighted sJnQ between the plain and cipher 1 rows. The distance SJ in all mixed alphabets is 15 places, which is also the distance between N and Q , because cipher 1 has been slid 15 places to the right of the plain alphabet. This property is invaluable in solving an unknown Quagmire 3 as I will demonstrate later.

Extended symmetries. In the rectangle SJNQ (above) there are seven other symmetries between letters in the same row or column:

SJ=NQ JS=QN QN=JS NQ=SJ SN=JQ NS=QJ
QJ=NS JQ=SN

The above can be easily verified from any of the mixed alphabets, for example:

```
          1111111111222222
0.2.4.6.8.0.2.4.6.8.0.2.4.
JKLMQUVWXYZSTRONGCIPHEABDF
```

Using symmetry to solve. A Quagmire 3 puzzle usually comprises the ciphertext and a 'probable' phrase or crib. Here is and example:

```
KPELQ KIHTQ RPJRF RFMSN MYXPK PAMCC XHAPW TMQRH GRKEL YWWST EGCYY
COVGA ACTST TQZIN GSSAL TTHLH AVPUY ETRWB WTSMC CXHAQ VZMAE RTTIL
OVBGK SLTTG XPEQR YLHAP BWSOE PCEMT AMGHO DAYXZ YHRTV ZYHKT QUMTD
RZAKP EZGSW RDRZA KPECY JCXLY WZCHC QRESO DMNPV RMHYR SKPSC EZSIV
FMSNM YXPKP RTG.
```

```
crib: "there's the keyword and the period"
```

The first step is to find the period by measuring the index of coincidence of each column over the expected range from period 5 to period 12. The IC will approach the English norm of 0.066 at the correct period, which turns out to be 6 in this case. Then the crib is placed by seeking repeated letters in the same column at period 6:

```
 Crib      ciphertext
there s     ZYHRTV
thekey      ZYHKTQ
wordan      UMTDRZ
dthepe      AKPEZG
riod        SWRD
```

Now using the crib and the equivalent ciphertext a partial matrix can be formed:

```
plain     abcdefghijklmnopqrstuvwxyz
cipher 1  .......YW.....M....K......
cipher 2  ....H..P......R..T........
cipher 3  ...DE.....K......R........
cipher 4  R...T..........Z..........
cipher 5  ....G........Z....V.....Q.
cipher 6  ...A.............S.Z..U...
```

from which a partial decryption is made:

```
the.y..e.....o.a........th.....e....o.r.e.t......re...h...ed.........
.er...e...e...wh..a..ir.....e..sto.ea........t..e...he....e......e...
or..e......theresthekeywordandtheperiodandthe........t.e......d....o.
.....................three.
```

We are missing 147 letters of plaintext and, unless very intuitive, we cannot guess any words at this stage. Now is the time to use the symmetry properties. We see aReT between plain and cipher 4 rows in the matrix -- we also see a.rT between plain and cipher 2 rows. The unknown letter in row cipher 2 must be an 'E'. Again, we see rStZ between plain and cipher 6 rows, and also rTs. between plain and cipher 2 rows. The missing letter must be Z. In this way, the partial matrix can be extended to:

```
abcdefghijklmnopqrstuvwxyz
.......YW.....M....K......
E...H..P......R..TZS......
A..DE..HI.K.MNOP.RST..W.Y.
R...T..S.......Z..........
....G........Z....V.....Q.
H..AP.......K.T..S.Z..U...
```

which gives a fuller partial decrypt with another 36 letters visible:

```
the.ym.et..e.o.a....m..etha....ea..oo.r.e.ta.....re...h.o.ed..th.o.si
.er...e.a.ea..whata..irs....ea.sto.ea.o..o...tt.e...he....ea.....e...
ora.ea..a..theresthekeywordandtheperiodandthe........t.e......d..e.om
.....ph...ti.....m..ethree.
```

Now we are in a position to guess a few words. At the start, following 'the', we have '.ym.et..e.o' and a little thought (or reference to word lists) suggests the word must be 'symmetry' or perhaps 'symmetries'. The 'y' in the former gives a conflict in the matrix, but 'symmetries' fits perfectly. A little further we see 'tha...' and there's a good chance this is either 'that or 'than'. The latter has a conflict but the former fits perfectly. These two additions give rise to a mass of further symmetries and the partial decrypt:

```
thesymmetrieso.a..a.mi.ethat...eal.oo.rme.tali.yare..sh.o.ed..th.o.si
.era.le.area..whata..irst...earsto.ea.ommo...ttle...herisreal.ya.el..
oratea..ai.theresthekeywordandtheperiodandthe..l..li.t.e.ri.a.dt.e.om
m..alph..eti...a.mi.ethree
```

There is now plenty of scope to guess more words. It's not difficult to recognise 'first' and 'really' and then 'little' becomes clear and 'quagmire' at the end. The symmetries then complete the decryption:

```
thesymmetriesofaquagmirethatappealtoourmentalityarefashionedwithconsi
derablecareandwhatatfirstappearstobeacommonlittlecipherisreallyanelab
orateaffairtheresthekeywordandtheperiodandthejollylittlecribandthecom
monalphabetinquagmirethree.
```

We have solved the cipher by guessing just a couple of words, thanks to the symmetries. But how does one find these symmetries without the pain of a pencil and paper search with the associated lengthy expenditure of time? The answer is to use the computer.

A computer algorithm. The computer goes through similar steps that you would take with pencil and paper but of course gets through the task very much quicker – in just a second or so. Here is the algorithm I followed:

1. find the period at the optimum IC and then place the crib with repeated letters, as described above;
2. construct a partial matrix from the placed crib;
3. make a list of all different 4-letter rectangles in the partial matrix;
4. go through the partial matrix, picking out rectangles with just three letters and an empty space. For each of these, look for a match in the list, using all eight symmetries. When a match is found, put the fourth letter into the space in the matrix, and add the discovered 4-letter group to the list;
5. repeat steps 3 and 4 until no more matches between 3 letter rectangles and 4-letter rectangles are found. Then display the new partial matrix and the decrypt.

After finding the complete solution, the matrix appears like this:

```
plain     abcdefghijklmnopqrstuvwxyz
cipher 1  STVRZOUYWNGCIQMXPLJKHEABDF
cipher 2  EAGBHDNPCFJKLORIMTZSQUVWXY
cipher 3  ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher 4  ROXNTGWSYCIPHVUZEQLMABDFJK
cipher 5  CITPGHSNREABDZYOFXVWJKLMQU
cipher 6  HENAPBOIGDFJKRTCLSYZMQUVWX
```

Note the setting SEARCH in the column under plain 'a'.
The correct mixed alphabet can be found by chaining and decimating. If you chain alphabet 6 with alphabet 2 you get

HEABDFJKLMQUVWXYZSTRONGCIP

from which the keyword 'STRONGCIPHER' is immediately evident. The original enciphering matrix would have been:

```
plain     strongcipheabdfjklmquvwxyz
cipher 1  JKLMQUVWXYZSTRONGCIPHEABDF
cipher 2  YZSTRONGCIPHEABDFJKLMQUVWX
```

and so on.

On the other hand if you choose to chain alphabet 3 with alphabet 2 you get:

AEHPICGNORTSZYXWVUQMLKJFDB

Here the key and mixed alphabet is obtained as the 25th decimation. If you chain alphabet 1 with 2 then you will get a repeating half-chain:

SEUNFYPMRBWCKSEUNFYPMRBWCK.

It's possible with some matrices for all chaining combinations to give such repeating half chains, in which case resort must be made to double chaining.

A program using symmetries. You can run a program that starts with a partial matrix, seeks out the symmetries and extends the matrix with them. You input the partial matrix using the cipher alphabets only, such as the one below. You copy the matrix and paste it into the program where indicated.:

```
.......YW.....M....K......
....H..P......R..T........
...DE.....K......R........
R...T..........Z..........
....G........Z....V.....Q.
...A.............S.Z..U...
```

The program is at

http://www.cryptoden.com/programs/Sym_WW.html