Cryptanalysis of a Vignère cipher

Overview. We will try to decrypt a Vignère-enciphered text without knowledge of the keyword.

Cryptanalysis of a Vignère cipher comprises two main steps:

1. Determining (or guessing) the length of the keyword.
2. Breaking the shift cipher corresponding to each letter of the keyword.

Step 1 involves looking through the text for repeated sequences of four or more letters, listing all the distances between the repeated sequences, and finding the common factors of all the distances. For this exercise, we won't spend much time on this step.

For step 2, we will need to make up a set of frequency tables. Each one will count the letters that were encrypted using a single letter of the keyword. By matching these against the standard frequency table, we should be able to reconstruct the keyword, and thus decrypt the message.

Things to do:

1. Obtain a copy of the handout "Cryptograms #6: Vignère ciphers" and a couple of blank frequency histograms.

   Look at cryptogram 1 on this handout. There are repetitions at distances of 8, 20, and 132, strongly suggesting that the keyword for this cryptogram has length either 2 or 4. We'll assume the length is 4.

2. Start with either the first, second, third, or fourth letter in the cryptogram, and circle every fourth letter (count carefully!) for the first eight lines of the text. You should see a pattern in your circles – if you don't, then erase the circles and try again.

3. Record the circled letters in a frequency histogram.

4. Match your frequency histogram against the standard frequency histogram, and determine what key letter was used to encode the letters you circled.

5. We'll assemble all the key letters and try to decrypt some of this text.