**2.4 Substitution Ciphers**

One of the more popular cryptosystems is the substitution cipher. It is commonly used in the puzzle section of the weekend newspapers, for example. The principle is simple: Each letter in the alphabet Is replaced by another (or possibly the same) letter. More precisely, a permutation of the alphabet is chosen and applied to the plaintext. In the puzzle pages, the spaces between the words are usually preserved, which is a big advantage to the solver, since knowledge of word structure becomes very useful. However, to increase security it is better to omit the spaces.

The shift and affine ciphers are examples of substitution ciphers. The Vigenere and Hill ciphers (see Sections 2.3 and 2.7) are not, since they permute blocks of letters rather than one letter at a time.

Everyone “knows" that substitution ciphers can be broken by frequency counts. However, the process is more complicated than one might expect.

Consider the following example. Thomas Jefferson has a potentially treasonous message that he wants to send to Ben Franklin. Clearly he does not want the British to read the text if they intercept it, so he encrypts using a substitution cipher. Fortunately, Ben Franklin knows the permutation being used, so he can simply reverse the permutation to obtain the original message (of course, Franklin was quite clever, so perhaps he could have decrypted it without previously knowing the key).

Now suppose we are working for the Government Code and Cypher School in England back in 1776 and are given the following intercepted message to decrypt.

LWNSOZBNWVWBAYBNVBSQWVUOHWDIZWRBBNPBPOOUWRPAWXAW

PBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNVIAXAWPBSALIBNXWA

BPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPAWOIHWOIQWAB

JPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV

ESDWARUWRBVPAWIRVBIBYBWZPUSREUWRZWAIDIREBHWIATYV

BFSLWAVHASUBNWXSRVWRBSHBNWESDWARWZBNPBLNRWWDWAPR

JHSAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWWRZVIB

IVBNVAIENBSHBNWFWSFOWBSPOBWASABSPQSOIVNIBPRZBSIR

VBIBYBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAI

RXIFOOTPRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWWUU

SVBOICWOJBSWHHWXBBNWIAVPHWBJPRZNPFFIRWW

A frequency count yields the following (there are 520 letters in the text):

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W | B | R | S | I | V | A | P | N | 0 |
| 76 | 64 | 39 | 36 | 36 | 35 | 34 | 32 | 30 | 16 |

The approximate frequencies of letters in English were given in Section 2.3. We repeat some of the data here in Table 2.2. This allows us to guess with

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| e | t | a | o | i | n | s | h | r |
| .127 | 0.91 | .082 | .075 | .070 | .067 | .063 | .061 | .060 |

Table 2.2: Frequencies of Most Common Letters in English

reasonable confidence that W represents e (though B is another possibility). But what about the other letters? We can guess that B , R, S, I, V, A, P, N , with maybe an exception or two, are probably the same as t, a, o, i, n, s, h, r in some order. But a simple frequency count is not enough to decide which is which. What we need to do now is look at digrams, or pairs of letters. We organize our results in Table 2.3 (we only use the most frequent letters here, though it would be better to include all).

The entry 1 in the IV row and N column means that the combination W N appears 1 time in the text. The entry 14 in the N row and W column means that AHV appears 14 times.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | W | B | R | S | I | V | A | P | N |
| W | 3 | 4 | 12 | 2 | 4 | 10 | 14 | 3 | 1 |
| B | 4 | 4 | 0 | 11 | 5 | 5 | 2 | 4 | 20 |
| R | 5 | 5 | 0 | 1 | 1 | 5 | 0 | 3 | 0 |
| S | 1 | 0 | 5 | 0 | 1 | 3 | 5 | 2 | 0 |
| I | 1 | 8 | 10 | 1 | 0 | 2 | 3 | 0 | 0 |
| V | 8 | 10 | 0 | 0 | 2 | 2 | 0 | 3 | 1 |
| A | 7 | 3 | 4 | 2 | 5 | 4 | 0 | 1 | 0 |
| P | 0 | 8 | 6 | 0 | 1 | 1 | 4 | 0 | 0 |
| N | 14 | 3 | 0 | 1 | 1 | 1 | 0 | 7 | 0 |

Table 2.3: Counting Digrams

We have already decided that W = e, but if we had extended the table to include low-frequency letters, we would see that W contacts many of these letters, too, which is another characteristic of e. This helps to confirm our guess.

The vowels a, i, o tend to avoid each other. If we look at the R row, we see that R does not precede S, I, A, N very often. But a look at the R column shows that R follows S, I, A fairly often. So we suspect that R is not one of a, i, o. V and N are out because they would require a, i, or o to precede W = e quite often, which is unlikely. Continuing, we see that at the most likely possibilities for a, i, o are S, I, P in some order.

The letter n has the property that around 80% of the letters that precede it ore vowels. Since we already have identified W, S, I, P as vowels, we see that R and A are the most likely candidates. We’ll have to wait to see which is correct.

The letter h often appears before e and rarely after it. This tells us that N = h.

The most common digram is th. Therefore, B = t.

Among the frequent letters, r and s remain, and they should equal V and one of A, R. Since r pairs more with vowels and s pairs more with consonants, we see th at V must be s and r is represented by either A or R.

The combination rn should appear more than nr, and A R is more frequent than RA, so our guess is that A = r and R = n.

We can continue the analysis and determine that S — o (note that to is much more common than ot), I = i, and P — a are the most likely choices. We have therefore determined reasonable guesses for 382 of the 520 characters in the text:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | W | N | S | O | Z | B | N | W | V | W | B | A | Y | B | N | V | B | S |
|  | e | h | o |  |  | t | h | e | s | e | l | r |  | t | h | s | t | o |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q | W | V | W | O | H | W | D | I | Z | W | R | B | B | N | P | B | P | … |
|  | e | s | e |  |  | e |  | i |  | e | n | t | t | h | a | t | a |  |

At this point, knowledge of the language, middle-level frequencies (i, d,...), and educated guesses can be used to fill in the remaining letters. For example, in the first line a good guess is that Y = u since then the word truths appears. Of course, there is a lot of guesswork, and various hypotheses need to be tested until one works.

Since the preceding should give the spirit of the method, we slop the remaining details. The decrypted message, with spaces (but not punctuation) added, is as follows (the text is from the middle of the Declaration of Independence):

*we hold these truths to be self evident that all m en are created equal that they are endowed by their creator with certain unalienable right) that among these are life liberty and the pursuit of happiness that to secure these rights governments are instituted among men deriving their just powers from the consent of the governed that whenever any form of government becomes destructive of these ends it is the right of the people to alter or to abolish it and to institute new government laying its foundation on such principles and organizing its powers in such form as to seem most likely to effect their safety and happiness*