Instructions for the Three-Stage Aguilar Cipher

Note: You read columns from top to bottom; they are labeled by the first row of the box below them. You write rows from left to right; if there are blocked-out squares, just write around them.

1) Write your message in lowercase print (except for L, to distinguish it from 1) in the first box of the form. The first 29 squares of the second row and the first 14 squares of the third row are blocked out; just write around them. There must be three to six rows and the last one must be complete. If you run out of things to say, finish with random symbols.

2) In the next box on the form, write a scrambled alphabet (using all 43 symbols exactly once) in the first row, above the blocked-out squares. It is imperative that this alphabet be completely random and completely different from one message to the next.

3) The scrambled alphabet is the key to the first stage of encipherment. It is also the first 43 symbols of the first-stage ciphertext. (Attaching the key to the ciphertext is my primary innovation.) Write column 0 as the beginning of a new row, subtracting each symbol from the symbol 0. Then continue the row by writing column 1, subtracting each symbol from the symbol 1. Continue writing rows of ciphertext, writing around the blocked out squares. Cross off the plaintext columns as they are used so you do not lose your place.

4) In the next box on the form, write a scrambled alphabet (using all 43 symbols exactly once) in the first row. It is imperative that this alphabet be completely random and completely different from one message to the next.

5) The scrambled alphabet is the key to the second stage of encipherment. It is also the first 43 symbols of the second-stage ciphertext. Do not block off any squares. Write column 0 as the beginning of a new row. Then continue the row by writing column 1. Continue writing rows of ciphertext. Do not perform any subtraction in this or the next stage. Cross off the first-stage ciphertext columns as they are used.

6) The key to the cipher, which is the same for every message that you send, is a scrambled alphabet. You should have it written on a strip of paper which you carry in your pocket. Use paper clips to attach the strip of paper to the form where it says, "place key strip here."

7) Do not block off any squares. Write column 0 as the beginning of a new row. Then continue the row by writing column 1. Continue writing rows of ciphertext. Do not perform any subtraction. Cross off the second-stage ciphertext columns as they are used. This is the final ciphertext; copy it into an e-mail or text message.

To decipher, start by filling in the bottom box and then work up to the top. Once you have enciphered a message, it should be clear how to reverse the process for deciphering. Note that you use subtraction for both enciphering and deciphering; you never use addition.