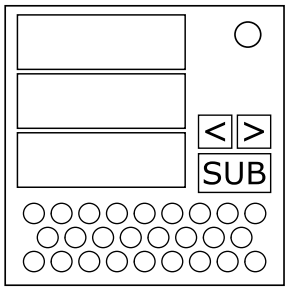
On the Subject of Lempel-Ziv Ciphers



Precursor to modern zip files. Though nothing really in common anymore.

This module contains 3 screens, a keyboard, 2 arrows, and a submit button that displays the current page you're on.

Pressing the left or right arrow takes you to the previous or next page. There are 2 pages.

To disarm the module, decrypt a word using the following three steps. Once you have the decrypted word, type it in using the keyboard. When you start typing, the screens go blank and the bottom screen will show what you are typing.

To clear your input, click one of the arrows.

Once you are satisfied with your input, press the button labeled "SUB" to submit your answer.

Step 1: Encrypted Binary Retrieval

For this step, use the letters from the top, middle and bottom screens on page 1 and the top screen on page 2. Concatenate them in this order and convert this encoded string to binary by replacing each letter with a binary code from the table on the right.

A	00000
B	00001
C	00010
D	00011
E	00100
F	00101
G	00110
H	00111
I	01000
J	01001
K	01010
L	01011
M	01100
N	01101
O	01110
P	01111
Q	10000
R	10001
S	10010
T	10011
U	1010
V	1011
W	1100
X	1101
Y	1110
Z	1111

Step 2: Lempel-Ziv Decryption

Split the binary message into chunks as follows: 1 chunk of length 1, 2 chunks of length 2, 4 chunks of length 3, 8 chunks of length 4, etc. The number of chunks of each length is 2 to the power of one less than the length. The number of chunks may vary (e.g. you may have fewer than 8 chunks of length 4) but the message does not end in the middle of a chunk.

Convert each chunk from binary into a number, obtaining the "coded sequence".

Next, you will replace each of these numbers with a bit sequence obtained from a numbered list, the "dictionary". However, you will construct the dictionary as you go.

Initially, the dictionary contains two entries:

- Entry #0: "0" (length 1)
- Entry #1: "1" (length 1)

For every number in the coded sequence, follow these steps:

- Replace the number with its entry from the dictionary.
- Add a new entry to the dictionary consisting of the bit sequence you just used plus one extra bit. The extra bit is the first bit of the dictionary entry for the next number in the coded sequence. (Even if that number refers to the very entry you're adding, you know what its first bit is.)

Step 3: Bitmap Decoding

Remove the last bit from the bit sequence obtained in step 2. The rest of the bit sequence is a monochrome bitmap whose width and height are prime. If the removed bit is 1, the bitmap's width is the larger prime, otherwise the smaller one.

The solution word may be represented within the bitmap in any of the following ways:

- Vertical Morse code: each pixel column is one letter, to be read from top to bottom.
- Pigpen: each 3×3 box of pixels represents a letter written in Pigpen cipher.
- Semaphore: each 3×3 box of pixels has its middle pixel set and the remaining pixels indicate the positions of Semaphore flags.
- Unified English Braille: each 2×3 box of pixels represents a Braille glyph.
- Alphabet: the message may also be written in plain English using a 4-pixel-tall font.