Pre is a symmetric cryptosystem based primarily on prefix (instantaneous) codes. It's best explained through symbol examples, and this program exists primarily to demonstrate the system.

First a key is printed, and then several words are encoded and decoded, with each step of the process shown.

For instance, here's the first piece of a key, which defines its zeroth mode.

```
0
|||0          0|          4
00            |0|0        0
||0|0         ||00        1
0             ||0|        2
|             |00         3
```

The top line includes just a 0, which is simply the number of the state. The rest is the actual definition.

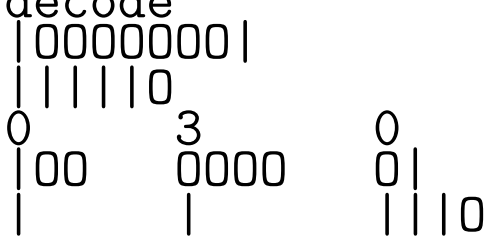
Each line should be read as **finds puts goes**. So the first column represents **finds**, and it is what the mode searches for as a prefix in the plaintext. The entries are checked for from the top to the bottom, so that the mode tends to consume as many symbols as possible. The prefix is consumed and the entry to its right is added to the output string. Finally the last entry in that same row is the new state or mode of the machine. Here's the encoding of a short string.

```
encode
|||||0
|OOOOOOO|
0       3       0
|       |       |||0
|OO     OOOO    0|
```

First the task and the result are given. The first line is the task. The second line is the plain text. And the third line is the resulting cipher text. Then the next three lines show the coding process in detail.

We see that the machine starts in mode 0, found a I, and wrote a IOO, then going to state 3. Then it finds I, writes OOOO, and goes back to state O. Finally it finds IIIO and writes a OI. Its plaintext is consumed, so the machine halts.

Here's the decoding:



Decoding makes use of the fact that modes write prefix codes. Because the machine knows that encoding was started in mode 0, it can deduce that it should consume exactly the symbols IOO. Then the machine deduces that the encoder must have found a I in the original plaintext and went into mode 3. And so on.

I've included several text files of such examples that use more symbols, etc.

Note that a more serious (secure) version would use multiple rounds and more complicated keys. But this system was primarily created as a work of art – as a kind of mathematical sculpture.