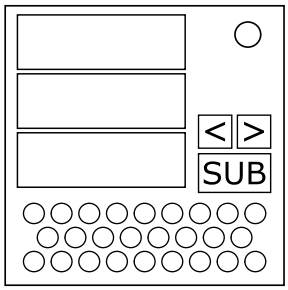
On the Subject of Huffman Ciphers



Ironically, more something for a Ravenclaw than a Hufflepuff.

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: Huffman Tree Construction

For this step, use all the letters on the top, middle and bottom screens on page 1 and the top and middle screens on page 2 (in that order). This gives a 26-letter code. Convert the letters into their alphabetic positions to obtain a list of 26 "scores". Associate the first with the letter A, then B, etc., up to Z.

Find the two entries with the lowest scores. In case of ties, take the earliest in the list. Create a new entry at the end of the list whose score is the sum of the scores of the two entries. The new entry is a binary tree whose left child node is the entry with the lowest score (or earliest if tied) and the right child node is the other one. Remove the two original entries from the list.

Repeat this a total of 25 times, iteratively reducing the list to a single binary tree.

The next page illustrates these steps with an example.

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

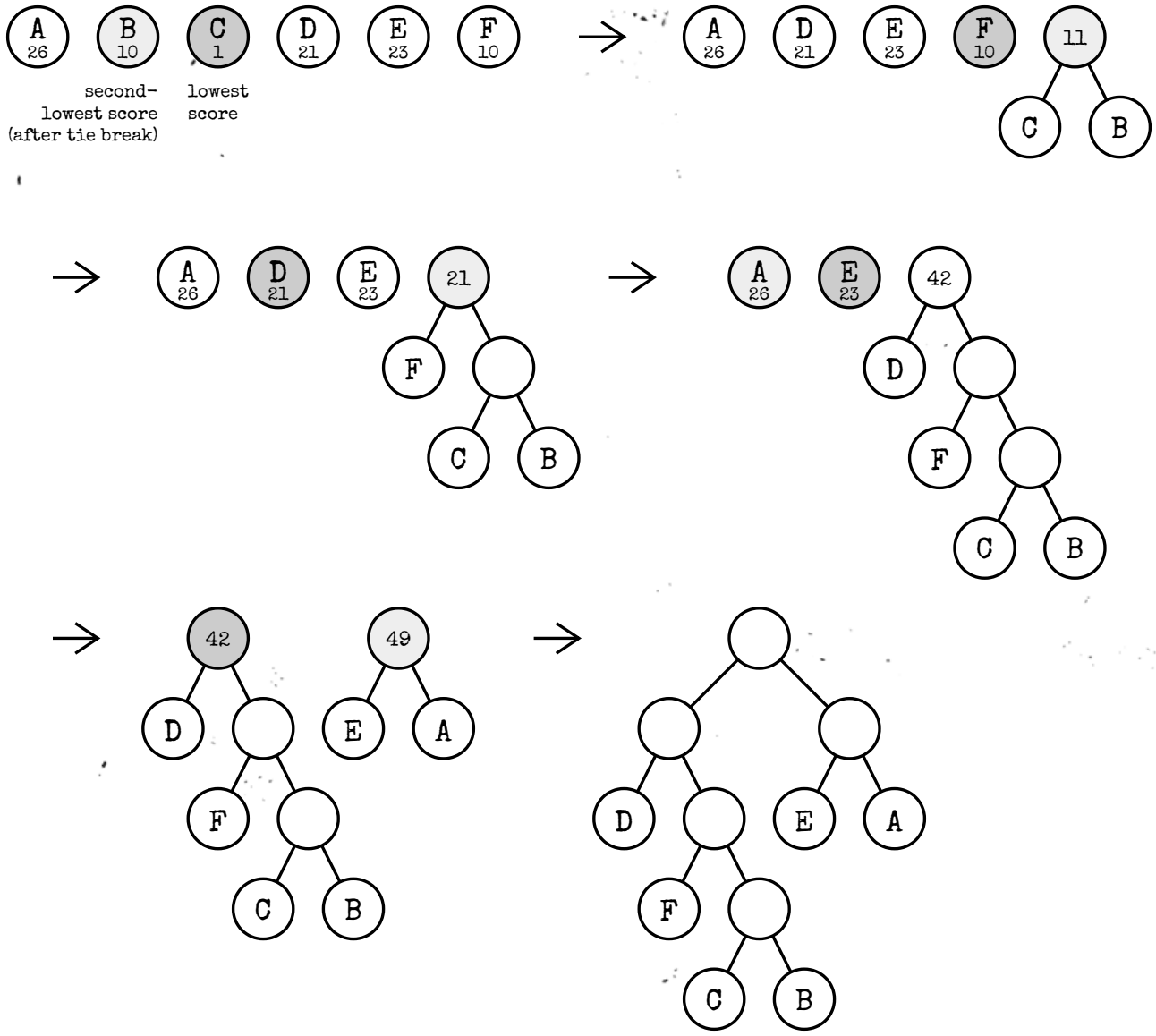
Step 2: Encrypted Binary Retrieval

Convert the encoded word from the third screen on page 2 to a single binary string by replacing each letter with a binary code from the table on the right.

Example for Step 1

For brevity, in this example we will pretend the alphabet has only 6 letters (A-F) and there are a total of 6 letters on the relevant five screens.

Example code from screens: ZJAUWJ



Example for Step 2

Encrypted word on last screen on page 2: LNS

Encrypted binary: L=01011 N=01101 S=10010 → 0101101101110010

Step 3: Huffman Decryption

Start at the root (top node) of the Huffman tree obtained in Step 1.

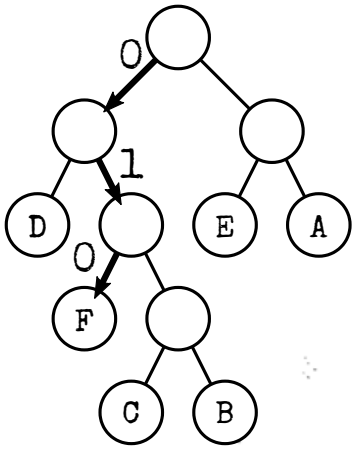
Read the first bit from the encrypted binary. If it's a 0, move to the left child node, else the right child node.

Continue this until you reach a letter node. At this point, write down the letter, then move back to the root.

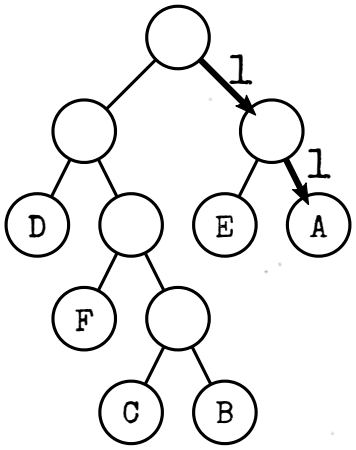
Repeat until all bits in the encrypted binary are exhausted. The received letters form the deciphered word.

Example for Step 3

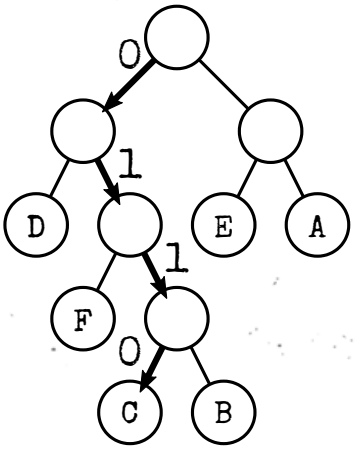
Encrypted binary from Step 2: 0101101101100010 → deciphered word: FACADE



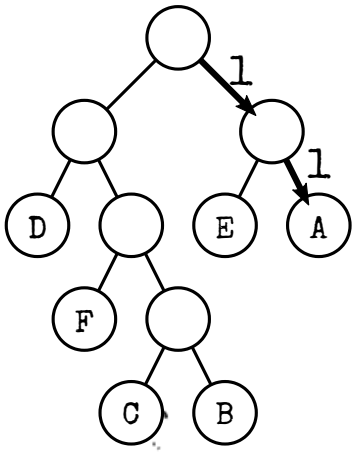
010 → F



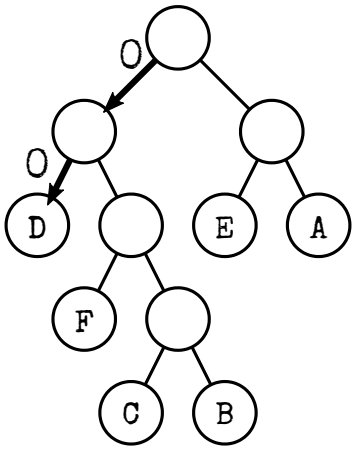
11 → A



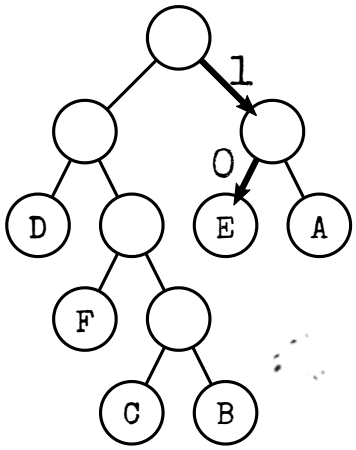
0110 → C



11 → A



00 → D



10 → E