Problem 59

Each character on a computer is assigned a unique code and the preferred standard is ASCII (American Standard Code for Information Interchange). For example, uppercase A = 65, asterisk (*) = 42, and lowercase k = 107.

A modern encryption method is to take a text file, convert the bytes to ASCII, then XOR each byte with a given value, taken from a secret key. The advantage with the XOR function is that using the same encryption key on the cipher text, restores the plain text; for example, 65 XOR 42 = 107, then 107 XOR 42 = 65.

For unbreakable encryption, the key is the same length as the plain text message, and the key is made up of random bytes. The user would keep the encrypted message and the encryption key in different locations, and without both “halves”, it is impossible to decrypt the message.

Unfortunately, this method is impractical for most users, so the modified method is to use a password as a key. If the password is shorter than the message, which is likely, the key is repeated cyclically throughout the message. The balance for this method is using a sufficiently long password key for security, but short enough to be memorable.

Your task has been made easy, as the encryption key consists of three lower case characters. Using cipher1.txt (right click and ‘Save Link/Target As...’), a file containing the encrypted ASCII codes, and the knowledge that the plain text must contain common English words, decrypt the message and find the sum of the ASCII values in the original text.

Solution

I created this answer assuming we could use any three bytes as the key, not any three lowercase ASCII letters - the answer could be correspondingly simpler, although it is already essentially instantaneous.

```
data = {79, 59, 12, 2, 79, 35, 8, 28, 20, 2, 3, 68, 8, 9, 68, 45, 0, 12, 9, 67, 68, 4, 7,
    5, 23, 27, 1, 21, 79, 85, 78, 79, 85, 71, 38, 10, 71, 27, 12, 2, 79, 6, 2, 8, 13,
    9, 1, 13, 9, 8, 68, 19, 7, 1, 71, 56, 11, 21, 11, 68, 6, 3, 22, 2, 14, 0, 30, 79,
    1, 31, 6, 23, 19, 10, 0, 73, 79, 44, 2, 79, 19, 6, 28, 68, 16, 6, 16, 15, 79, 35,
    8, 11, 72, 71, 14, 10, 3, 79, 12, 2, 79, 19, 6, 28, 68, 32, 0, 0, 73, 79, 86, 71,
    39, 1, 71, 24, 5, 20, 79, 13, 9, 79, 16, 15, 10, 68, 5, 10, 3, 14, 1, 10, 14, 1,
    3, 71, 24, 13, 19, 7, 68, 32, 0, 0, 73, 79, 87, 71, 39, 1, 71, 12, 22, 2, 14, 16,
    2, 11, 68, 2, 25, 1, 21, 22, 16, 15, 6, 10, 0, 79, 16, 15, 10, 22, 2, 79, 13, 20,
    65, 68, 41, 0, 16, 15, 6, 10, 0, 79, 1, 31, 6, 23, 19, 28, 68, 19, 7, 5, 19, 79,
    12, 2, 79, 0, 14, 11, 10, 64, 27, 68, 10, 14, 15, 2, 65, 68, 83, 79, 40, 14, 9,
    1, 71, 6, 16, 20, 10, 8, 1, 79, 19, 6, 28, 68, 14, 1, 68, 15, 6, 9, 75, 79, 5, 9,
    11, 68, 19, 7, 13, 20, 79, 8, 14, 9, 1, 71, 8, 13, 17, 10, 23, 71, 3, 13, 0, 7,
    16, 71, 27, 11, 71, 10, 18, 2, 29, 29, 8, 1, 1, 73, 79, 81, 71, 59, 12, 2, 79,
    8, 14, 8, 12, 19, 79, 23, 15, 6, 10, 2, 28, 68, 19, 7, 22, 8, 26, 3, 15, 79, 16,
    15, 10, 68, 3, 14, 22, 12, 1, 1, 20, 28, 72, 71, 14, 10, 3, 79, 16, 15, 10, 68,
    3, 14, 22, 12, 1, 1, 20, 28, 68, 4, 14, 10, 71, 1, 1, 17, 10, 22, 71, 10, 28,
    19, 6, 10, 0, 26, 13, 20, 7, 68, 14, 27, 74, 71, 89, 68, 32, 0, 0, 71, 28, 1,
    9, 27, 68, 45, 0, 12, 9, 79, 16, 15, 10, 68, 37, 14, 20, 19, 6, 23, 19, 79, 83,
    71, 27, 11, 71, 27, 1, 11, 3, 68, 2, 25, 1, 21, 22, 11, 9, 10, 68, 6, 13, 11,
    18, 27, 68, 19, 7, 1, 71, 3, 13, 0, 7, 16, 71, 28, 11, 71, 27, 12, 6, 27, 68,
    2, 25, 1, 21, 22, 11, 9, 10, 68, 10, 6, 3, 15, 27, 68, 5, 10, 8, 14, 10, 18, 2,
    79, 6, 2, 12, 5, 18, 28, 1, 71, 0, 2, 71, 7, 13, 20, 79, 16, 2, 28, 16, 14, 2,
    11, 9, 22, 74, 71, 87, 68, 45, 0, 12, 9, 79, 12, 14, 2, 23, 2, 3, 2, 71, 24, 5,
    20, 79, 10, 8, 27, 68, 19, 7, 1, 71, 3, 13, 0, 7, 16, 92, 79, 12, 2, 79, 19, 6,
    28, 68, 8, 1, 8, 30, 79, 5, 71, 24, 13, 19, 1, 1, 20, 28, 68, 19, 0, 68, 19, 7,
    1, 71, 3, 13, 0, 7, 16, 73, 79, 93, 71, 59, 12, 2, 79, 11, 9, 10, 68, 16, 7, 11,
    71, 6, 23, 71, 27, 12, 2, 79, 16, 21, 26, 1, 71, 3, 13, 0, 7, 16, 75, 79, 19, 15,
    0, 68, 0, 6, 18, 2, 28, 68, 11, 6, 3, 15, 27, 68, 19, 0, 68, 2, 25, 1, 21, 22,
    11, 9, 10, 72, 71, 24, 5, 20, 79, 3, 8, 6, 10, 0, 79, 16, 8, 79, 7, 8, 2, 1, 71,
    6, 10, 19, 0, 68, 19, 7, 1, 71, 24, 11, 21, 3, 0, 73, 79, 85, 87, 79, 38, 18,
    27, 68, 6, 3, 16, 15, 0, 17, 0, 7, 68, 19, 7, 1, 71, 24, 11, 21, 3, 0, 71, 24,
    5, 20, 79, 9, 6, 11, 1, 71, 27, 12, 21, 0, 17, 0, 7, 68, 15, 6, 9, 75, 79, 16,
    15, 10, 68, 16, 0, 22, 11, 11, 68, 3, 6, 0, 9, 72, 16, 71, 29, 1, 4, 0, 3, 9, 6,
    30, 2, 79, 12, 14, 2, 68, 16, 7, 1, 9, 79, 12, 2, 79, 7, 6, 2, 1, 73, 79, 85, 86,
    79, 33, 17, 10, 10, 71, 6, 10, 71, 7, 13, 20, 79, 11, 16, 1, 68, 11, 14, 10, 3,
    79, 5, 9, 11, 68, 6, 2, 11, 9, 8, 68, 15, 6, 23, 71, 0, 19, 9, 79, 20, 2, 0, 20,
    11, 10, 72, 71, 7, 1, 71, 24, 5, 20, 79, 10, 8, 27, 68, 6, 12, 7, 2, 31, 16, 2,
    11, 74, 71, 94, 86, 71, 45, 17, 19, 79, 16, 8, 79, 5, 11, 3, 68, 16, 7, 11, 71,
    13, 1, 11, 6, 1, 17, 10, 0, 71, 7, 13, 10, 79, 5, 9, 11, 68, 6, 12, 7, 2, 31, 16,
    2, 11, 68, 15, 6, 9, 75, 79, 12, 2, 79, 3, 6, 25, 1, 71, 27, 12, 2, 79, 22, 14,
    8, 12, 19, 79, 16, 8, 79, 6, 2, 12, 11, 10, 10, 68, 4, 7, 13, 11, 11, 22, 2, 1,
    68, 8, 9, 68, 32, 0, 0, 73, 79, 85, 84, 79, 48, 15, 10, 29, 71, 14, 22, 2, 79,
    22, 2, 13, 11, 21, 1, 69, 71, 59, 12, 14, 28, 68, 14, 28, 68, 9, 0, 16, 71, 14,
    68, 23, 7, 29, 20, 6, 7, 6, 3, 68, 5, 6, 22, 19, 7, 68, 21, 10, 23, 18, 3, 16,
    14, 1, 3, 71, 9, 22, 8, 2, 68, 15, 26, 9, 6, 1, 68, 23, 14, 23, 20, 6, 11, 9,
    79, 11, 21, 79, 20, 11, 14, 10, 75, 79, 16, 15, 6, 23, 71, 29, 1, 5, 6, 22, 19,
    7, 68, 4, 0, 9, 2, 28, 68, 1, 29, 11, 10, 79, 35, 8, 11, 74, 86, 91, 68, 52, 0,
    68, 19, 7, 1, 71, 56, 11, 21, 11, 68, 5, 10, 7, 6, 2, 1, 71, 7, 17, 10, 14, 10,
    71, 14, 10, 3, 79, 8, 14, 25, 1, 3, 79, 12, 2, 29, 1, 71, 0, 10, 71, 10, 5, 21,
    27, 12, 71, 14, 9, 8, 1, 3, 71, 26, 23, 73, 79, 44, 2, 79, 19, 6, 28, 68, 1, 26,
    8, 11, 79, 11, 1, 79, 17, 9, 9, 5, 14, 3, 13, 9, 8, 68, 11, 0, 18, 2, 79, 5, 9,
    11, 68, 1, 14, 13, 19, 7, 2, 18, 3, 10, 2, 28, 23, 73, 79, 37, 9, 11, 68, 16,
    10, 68, 15, 14, 18, 2, 79, 23, 2, 10, 10, 71, 7, 13, 20, 79, 3, 11, 0, 22, 30,
    67, 68, 19, 7, 1, 71, 8, 8, 8, 29, 29, 71, 0, 2, 71, 27, 12, 2, 79, 11, 9, 3,
    29, 71, 60, 11, 9, 79, 11, 1, 79, 16, 15, 10, 68, 33, 14, 16, 15, 10, 22, 73};
```

We don’t want to allow extended ASCII, so the only possibilities for the characters are below 127. We check each block of three for which characters are allowed to be the key, so that the result is ASCII; we then take the intersection of the allowed characters over each block of 3.

```
dat =
  Function[{pos}, BitXor[data[[pos ;; pos + 2]], #] & /@ Range[32, 122] // Transpose] /@
    Range[1, Length[data] - 2, 3] // Transpose;

allowedKeys = Intersection @@@ dat
```

```
{{102, 103}, {108, 110, 111}, {100}}
```

```
decrypt[nums_, key_] :=
 BitXor[nums, First@Partition[key, Length[nums], 3, {1, 1}, key]]
```

This could easily be done by brute force, but here is a function that checks for the presence of “the” or “THE”, and also that the proportion of {letters and “ “} is greater than 3/4.

```
valid[nums_] :=
 With[{alloweds = Flatten@ToCharacterCode@Join[CharacterRange["A", "Z"],
       CharacterRange["a", "z"], {" "}]}, Count[Partition[nums, 3, 1],
     _List?(# === {84, 72, 69} || # === {116, 104, 101} &)] > 1 &&
   Count[nums, _?(MemberQ[alloweds, #] &)] / Length[nums] > 0.75]

Select[Tuples[allowedKeys], valid[decrypt[data, #]] &]
```

```
{{103, 111, 100}}
```

```
FromCharacterCode[decrypt[data, First@%]]
```

```
(The Gospel of John, chapter 1) 1 In the beginning the Word already existed.
  He was with God, and he was God. 2 He was in the beginning with God. 3
  He created everything there is. Nothing exists that he didn't make. 4
  Life itself was in him, and this life gives light to everyone. 5 The
  light shines through the darkness, and the darkness can never extinguish
  it. 6 God sent John the Baptist 7 to tell everyone about the light so
  that everyone might believe because of his testimony. 8 John himself
  was not the light; he was only a witness to the light. 9 The one who
  is the true light, who gives light to everyone, was going to come into
  the world. 10 But although the world was made through him, the world
  didn't recognize him when he came. 11 Even in his own land and among
  his own people, he was not accepted. 12 But to all who believed him and
  accepted him, he gave the right to become children of God. 13 They are
  reborn! This is not a physical birth resulting from human passion or
  plan, this rebirth comes from God.14 So the Word became human and lived
  here on earth among us. He was full of unfailing love and faithfulness.
  And we have seen his glory, the glory of the only Son of the Father.
```

```
decrypt[data, First[%%]] // Total
```

```
107 359
```

In[61]:=
```
FromCharacterCode[%%%]
```

Out[61]=
```
{god}
```