Cipher Crack Race

Adrianna Holden-Gouveia
Website: aholdengouveia.name
: aholdengouveia

Accessibility Notice

This document is also available in HTML format at:

Link: `https://aholdengouveia.name/InfoSec/labs/cipherrace.html`

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

Learning Outcomes

By the end of this activity, you will be able to:

- Explain how a substitution cipher works
- Use frequency analysis to break a simple cipher
- Explain why modern encryption can't be broken this way

Instructions

Work in teams of 3 or 4. The first team to decode the whole message wins. You have about 20 minutes.

The message below was encrypted with a substitution cipher. Every letter was swapped for a different letter, and the same swap was used every time. For example, if E became I once, every E in the message became I. Spaces and punctuation were not changed.

Tips

1. Count how many times each letter shows up in the message, and fill in the count table.
2. Compare your counts with the most common letters in English, listed below. The letter that shows up the most in the message is probably E.
3. Look at short words. One-letter words are almost always A or I. The most common three-letter words are THE and AND.
4. Look for double letters, such as LL, SS, EE, and OO.

5. Each time you figure out a letter, write it in the decoding table, then fill it in everywhere in the message. Every letter you solve makes the next one easier.

Most common letters in English, from most to least common: E, T, A, O, I, N, S, H, R, D, L, C, U, M, W, F, G, Y, P, B, V, K, J, X, Q, Z. About 1 in every 8 letters in English is an E.

The Message

```
ASI FIXA HTXXZMYB OX WMRP TRB ITXQ AM YILILFIY, FNA STYB
AM PNIXX. T XOLHWI VOHSIY WOJI ASOX MRI VTR FI FYMJIR ZOAS
T HIRVOW TRB XMLI HTAOIRVI, FIVTNXI ASI LMXA VMLLMR WIAAIYX
OR IRPWOXS XSMZ NH TPTOR TRB TPTOR. ASTA OX ZSQ YITW IRVYQHAOMR
NXIX LTAS ASTA ZMNWB ATJI T VMLHNAIY LOWWOMRX MC QITYX AM
FYITJ. OC QMN VTR YITB ASOX, YTOXI QMNY STRBX. QMNY AITL
ZORX. VMRPYTANWTAOMRX, VMBIFYITJIYX!
```

Your Work

Count how many times each letter shows up in the message.

Table 1: Count table, first half

Letter	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Count													

Keep counting with the rest of the alphabet.

Table 2: Count table, second half

Letter	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Count													

As you solve each code letter, write the real letter under it.

Table 3: Decoding table, first half

Code letter	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Real letter													

Keep going with the rest of the code letters.

Table 4: Decoding table, second half

Code letter	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Real letter													

Write the decoded message here, with your team's names:

After the Race

Talk about these as a class:

- Which letters were easiest to find? Which were hardest, and why?
- How long did it take? How long would it take a computer?
- Why can't you break AES the same way?

Resources

References, a video, a PowerPoint and some notes are available at my website Link: `https://www.aholdengouveia.name/InfoSec/Cryptography.html`

Letter frequency in English, from Wikipedia Link: `https://en.wikipedia.org/wiki/Letter_frequency`