Breaking the Vigenère Cipher

- Module Resources 10 min
- Introduction 2 min
- Known Language and Key Length 5 min
- Programming Exercise: Known Language and Key Length 10 min
- **Practice Quiz:** Known Language and Key Length 2 questions
- Unknown Key Length 4 min
- Programming Exercise: Unknown Key Length 10 min
- **Practice Quiz:** Unknown Key Length 4 questions
- Unknown Language 4 min
- Programming Exercise: Unknown Language, Unknown Key Length 10 min
- **Quiz:** Breaking the Vigenère Cipher 7 questions
- Extend Your Program 10 min
- End of Module Survey 10 min

Here are some optional ideas to extend your program even further:

- **Test edge cases.** 'Edge cases' refer to special situations where a program might break down. For example, consider text files or languages where the most common letter is unreliable or nearly tied with another letter. For example, the original message encrypted in the text file **aida_keyverdi.txt** is in Italian, which has letter frequencies E 11.49%, A 10.85%, I 10.18% (http://www.sttmedia.com/characterfrequency-italian). You could also experiment with determining the maximum allowable key length.
- **Use a different set of data.** Try different length texts and different languages. This can also help you identify edge cases.
- **Explore different statistics.** This program assumes one character is the most frequent. Are there other ways to determine the key to a cipher? One possibility to address certain edge cases, such as breaking decryption of Italian-language texts could be to find multiple possible keys of each length and try all of them (**tryKeyLength** might return a 2D array—if you find every key length **n** where there are two possibilities for the most frequent letter, there would be 2^**n** possible keys).
- **Adapt your program to a new problem.** This project focused on the Vigenère cipher. What other ciphers could you write algorithms for? How is cryptography different from steganography?

Whatever you do to extend your program and solve new problems, share it with us and your peers in the forums! Happy programming!

✓ Complete