

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


Vigenère Cipher

Message

Meet Me At Dawn

Key

- Previously: learned Caesar cipher
- Now: Vigenère cipher



Now you're going to learn a bit about the Vigenere Cipher, which historically

Introduction

Have a question? Discuss this lecture in the week forums.



Interactive Transcript

Search Transcript

English ▾

0:03

If you think back to the start of this course, you learned a little bit about cryptography and implemented the Caesar cipher. [Now you're going to learn a bit about the Vigenere Cipher, which historically](#) is quite important, as it was thought to be unbreakable for hundreds of years.

0:20

However, as you're going to see and do, the cipher is quite easy to break with the computer. Now, let's see how this cipher works.

0:29

The key in Vigenere was classically a word. For example, here we picked dice as our key.

0:36

You write down the word repeatedly to match the message length.

0:42

Each letter represents a number for how much to shift by, so dice means shift by 3, 8, 2, and 4, repeatedly. In a Java program, it would be quite convenient to represent the key as an array of ints.

1:00

Now to encrypt, you shift each letter by the amount written under it, much like you in a Caesar cipher, but each letter gets shifted by a different amount.

1:12

The first letter is M, which has 3 added to it, so you get P. The second letter is E, which has 8 added to it, so you get M.

1:22

Then you repeat this process across the entire message.

1:27

As we did for Cesar, we'll have to skip anything that's not a letter.

1:32

Notice that conceptually, this cipher is like four different Cesar cyphers. One with a shift of three, shown in blue. One with a shift of eight, shown in red. Another with a shift of two, shown in green. And a fourth with a shift of four, shown in purple. This similarity means that a programmer who has already written an implementation of Caesar cipher could make use of it to help implement a Vigenere Cipher. In fact, you could make an array of Caesar cipher objects, one with each shift specified in the key and use them for your encryption. If you did something like this, you could use the mod operator to wrap a count into the pattern, 0,1,2,3, 0,1,2,3. For this mini-project, we're going to give you the code for a Vigenere cipher and you are going to write the code to break it. Your goal is to take messages that we have encrypted with Vigenere and find the decrypted message without knowing the key we used. You will start with breaking a message that you know is in English, and then expand your program so that you can try to break encryption in a variety of languages.

Downloads

Lecture Video mp4

Subtitles (English) WebVTT

Transcript (English) txt

Would you like to [help us translate](#) the transcript and subtitles into additional languages?