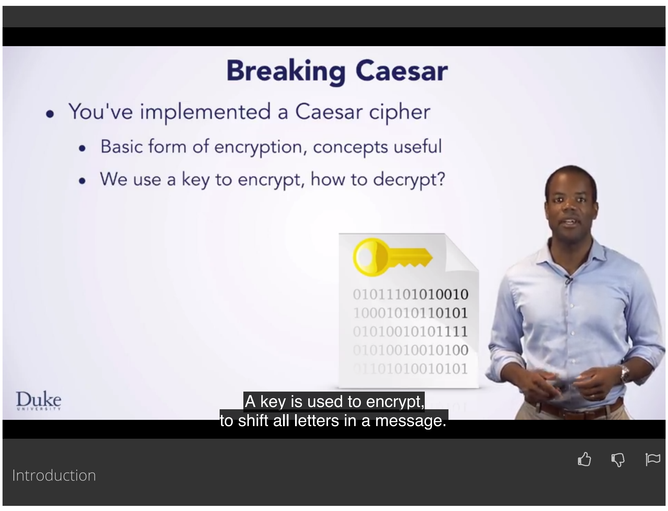

Introduction

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

Interactive Transcript

Search Transcript English

0:03
Hi, I'm Jeff Forbes, a Computer Science professor at Duke University. And a friend of Susan, Owen, Robert, and Drew.

0:13
I do research in Computer Science Education and Learning Analytics. But I also teach the Data Structures and Algorithms course using Java.

0:21
I'm really excited to be able to give a guest lecture about using arrays to break or crack a Caesar cipher, a method of encryption I know you'd been studied.

0:32
You or someone else has implemented a program to encrypt text using a Caesar cipher.

0:41
This is a very basic and historically interesting form of decryption, though it's not secure given patience or access to a computer and your skills at programming. The concepts in cracking this cipher are useful in solving other problems too.

0:57
A key is used to encrypt, to shift all letters in a message. But how do we decrypt?

1:04
We know that decryption must be possible, since the intended recipient must be able to decrypt and read the encrypted message being sent.

1:15
Because a shift of 26 is the same as a shift of 0, encrypting with the shift of 7, followed by Decrypting with the shift of 19 will result in the original message. Just like a shift of 26. How does knowing this help us cracked the cipher? A thief or hacker could find the key, which is a number. Keys are often numbers both in the Caesar cipher and many other forms of encryption.

1:46
The hacker simply subtracts from 26 and will be able to decrypt the message.

1:52
If the hacker or thief doesn't have the key is it possible to use brute force or some other way to crack the cipher?

2:02
Brute force means trying every possible key with a human helping using brute force with the Caesar cipher makes it relatively easy to decrypt a message.

2:13
Suppose we intercept this message which is too difficult to pronounce.

2:18
Can we tell what this message says simply by looking at it? That seems unlikely.

2:25
If we knew the key used to encrypt this message we could easily decrypt it.

2:32
But how many keys are there? Perhaps we could simply try them all, that's what a brute force approach is.

2:39
The basic idea is to try every key.

2:43
We already have the code to encrypt the message we'll use every key from one

2:49
to 26 or 25 to encrypt the message we're trying to decrypt. Since the decryption shift is just 26 minus the original encryption shift, if we try all 26 shifts, we'll find the original message.

3:05
We can try every key using this brute force approach because the number of keys is small and trying each key is fast. The same approach won't work for other forms of encryption because there might be too many keys. It's also possible that using each key to encrypt could take a long time.

3:27
Before we talk about an approach that's more sophisticated than brute force, let's work to understand brute force in what we call eyeball decryption.

3:38
Our goal is to unlock, or decrypt, an encrypted message. We don't have the key used to decrypt. We're not that fortunate.

3:47
However, we do have the key used to encrypt, from the class Caesar cipher. Using that we can try all 26 keys.

3:57
To decrypt using a human or eyeball approach, we'll create a Caesar cipher object.

4:04
We'll try all 26 keys from 0 to 25. We'll use our Ceasar Cipher object named cipher to shift a message with each of the 26 keys then we'll print the result of the shift. As we'll see we can decrypt the message if we recognize words.

4:25
How do we find the original message? When we run the code we just discussed, we'll be able to view or eyeball the result of encrypting 26 times.

4:37
We'll scan all 26 strings produced by 26 different keys, and we'll do this methodically.

4:46
As we eyeball each string, we look carefully to see if the string is recognizable as English, since we're looking for an English language message.

4:57
This line isn't recognizable.

5:01
This line doesn't look like English, but let's look closely.

5:06
No, it's not English.

5:09
We'll look at the next line. Let's examine this line closely.

5:14
This line easily recognizes English text, and we see that encryption and security are a fundamental parts of today's Internet.

Downloads

Lecture Video mp4
Subtitles (English) WebVTT
Transcript (English) txt

Would you like to help us translate the transcript and subtitles into additional languages?