☐ Transposition cipher

Un-selected is correct

☑ Vigenére cipher

Correct

☐ Turing cipher

Un-selected is correct

☑ Caesar cipher

Correct

Continue

▶ 5:28 / 5:29 💬 🔊 ⚙ ⛶

👍 👎 🚩

A Brief History of Cryptography

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

Interactive Transcript

Search Transcript | English ▾

0:03
Welcome back. Today you're going to learn a little bit about security. Which will show the importance of the problems you're going to solve in this module. Suppose you want to buy something online. You use your computer which is connected to the internet. So it can communicate with the servers at the online store from which you're making your purchases. To complete your purchase, you put your credit card or other payment information into your computer. When you purchase the items in your shopping cart, for example, your computer sends that information with your credit card information across the Internet to the online store. But what if a thief is looking at the data going across the Internet? This thief might be able to intercept your credit card information and use it to make fraudulent purchases. You certainly don't want that, and neither does the online store. It wants your business. So, what makes online shopping safe? What actually happens is that your computer encrypts the information before it sends it to the web servers for the online store. The two computers agree on a special piece of data called the key. And then use that with an encryption algorithm to transform the data so that only another computer with the key can decrypt the data. Now your computer sends the encrypted data across the Internet and any potential thief is thwarted. The thief can only see the encrypted data and cannot understand what the message says. Their receiving computer, which has the key, can then decrypt the data and understand the original message. When you are doing anything online, your web browser will tell you if you have a secure connection. For example, Chrome displays the https in green and shows a green lock icon next to it. The s in https is for secure.

1:47
It's a different kind of connection to a web server than the standard HTTP.

1:52
If you were to click on the lock icon, it would tell you the technical details of the encryption used to secure the connection. There are many algorithms involved in securing your internet connection. And algorithm called AES is typically used to encrypt the data that is sent to the server once the connection is set up. However, your computer and the server must agree on the key in a secure fashion before any information can be sent. While this may sound quite difficult, there are algorithms that can make this happen. In this example my computer used two algorithms to securely set up the connection with the server. One called elliptic curve diffie hellman and one called RSA. These algorithms are very important to the secure operation of the internet but the math involved is a bit advanced to go into here. To implement these encryption algorithms, you would need to spend several days or months just learning that math which is not the focus of this course. If you're interested in advanced cryptography, Coursera has some excellent courses on the subject which you could take after you've mastered basic programming.

2:56
Even though modern cryptography requires some advanced math, you can however learn a lot about cryptography by looking to the past. Classical cryptography, the cryptographic algorithms used in past centuries, involved simple mathematics and even predate computers. These algorithms are not secured today. They can be easily cracked by computers. But learning how they work and implementing them will teach you some important lessons. Furthermore, learning how to break them will teach you a critical lesson. Do not try to make up your own cryptographic scheme. If you need security, use a well-tested implementation of a modern cryptographic library. So how far into history will we need to look to find the first use of cryptography? The first known use of something resembling cryptography comes from ancient Egypt 4,000 years ago. However, historians believe that the hiding of messages was not a serious attempt to guard secrets.

3:51
If you look forward a few hundred years to Mesopotamia around 1500 BCE, you will find records of craftsmen using simple encryption schemes to guard their secrets when they recorded them on stone tablets. Going further forward to the Roman Empire, the Caesar Cipher, which you will learn about in the rest of this module is named after Julius Caesar, who used it extensively. Looking forward another 1500 years you will find the Vigenere Cipher. Giovan Bastiste Belosa actually described this algorithm in 1553, but it named after Blaise Vigenere in the 19th century. His algorithm is historically very important, as it was long regarded as unbreakable. However, In the mini project, you are going to write a program to break it.

4:38
Continuing forward to the 1940s, cryptography was a critical part of World War II. The Allies devoted significant resources to breaking the German codes, with a core of that effort taking place at Bletchley Park in England. Alan Turing was a leader in this code breaking effort and made many important contributions to computer science. In fact, he's so important that the highest honor in computer science is called the Turing award. So now that you know a little bit about cryptographic history, what will you be doing? In this module, you're going to learn about the Caesar Cipher. You will implement it and then break it.

5:15
In the mini project at the end of this course, you're going to learn about the Vigenere Cipher and will also implement it and break it. Of course, all of these problems are going to teach you several important skills that can help you solve a wide variety of other problems.

Downloads

Lecture Video mp4

Subtitles (English) WebVTT

Transcript (English) txt

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