Encryption with Keys and Passwords

Unit 4 Lesson 8 (U4L8)
2 Days

Exploring the Vigenere Cipher Widget
Keys and Passwords
(Optional) How Not to Get Hacked

Table of Contents

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

Opening thoughts:

In the previous lesson you saw how relatively easy it was to crack a substitution cipher with a computational tool.

Today we'll try to crack a different code to see what it's like. Beforehand, however, we should consider why someone might want to crack a cipher in the first place.

Written Prompt - *IN YOUR NOTES*, answer the following (2-min.)

Are there ethical reasons to try to crack secret codes?

Share with a partner

Share as a class

-Counterterrorism
-Understand abstract patterns (ex: DNA)
-To see how strong the code really is!

Encryption: Algorithms vs. Keys

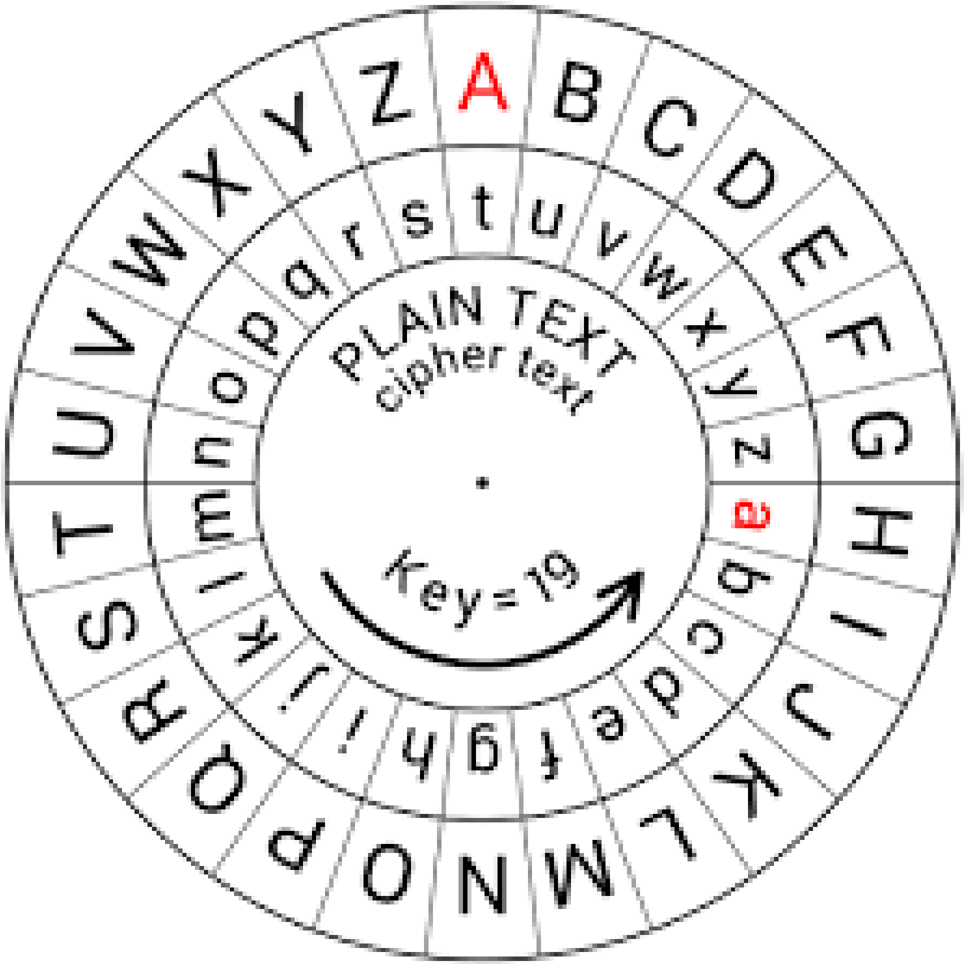
Today, we will attempt to crack codes, paying particular attention to the processes and algorithms that we use to do so.

Before starting today we want to make sure that we distinguish between an encryption algorithm and an encryption key

- An Encryption algorithm is some method of doing encryption.
- The Encryption key is a specific input that dictates how to apply the method and can also be used to decrypt the message. Some people might say "What is the key to unlocking this message?"

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

Encryption: Algorithms vs. Keys


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key = 19

For example:

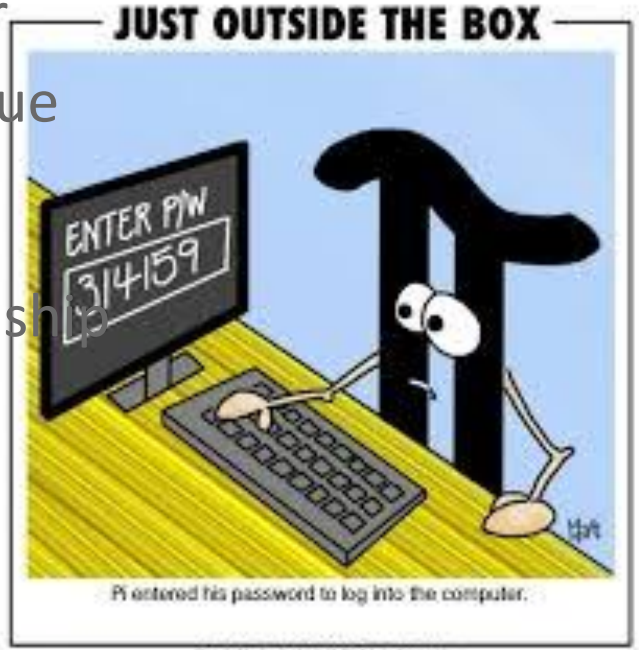
- The **Caesar Cipher** is an encryption algorithm that involves shifting the alphabet
- The **amount of alphabetic shift** used to encode the message is the key

Encryption: Algorithms vs. Keys

So, there is a difference between the algorithm (how to execute the encryption and decryption) and key (the secret piece of information).

- In encryption you should always assume that your 'enemy' knows the encryption algorithm and has access to the same tools that you do.
- What makes encryption REALLY strong is making it hard to guess or crack the "key," even if the "enemy" knows the encryption technique you're using.

Today we'll learn a little more about it and about keys and their relationship to passwords you use everyday.



Pi entered his password to log into the computer.

Copyright www.justoutsidetheboxcartoon.com

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

Activity #1 - Explore the Vigenere Cipher Widget (pass out worksheet)

First: Navigate to the Vigenere Cipher Widget (U4L8 - bubble 2)

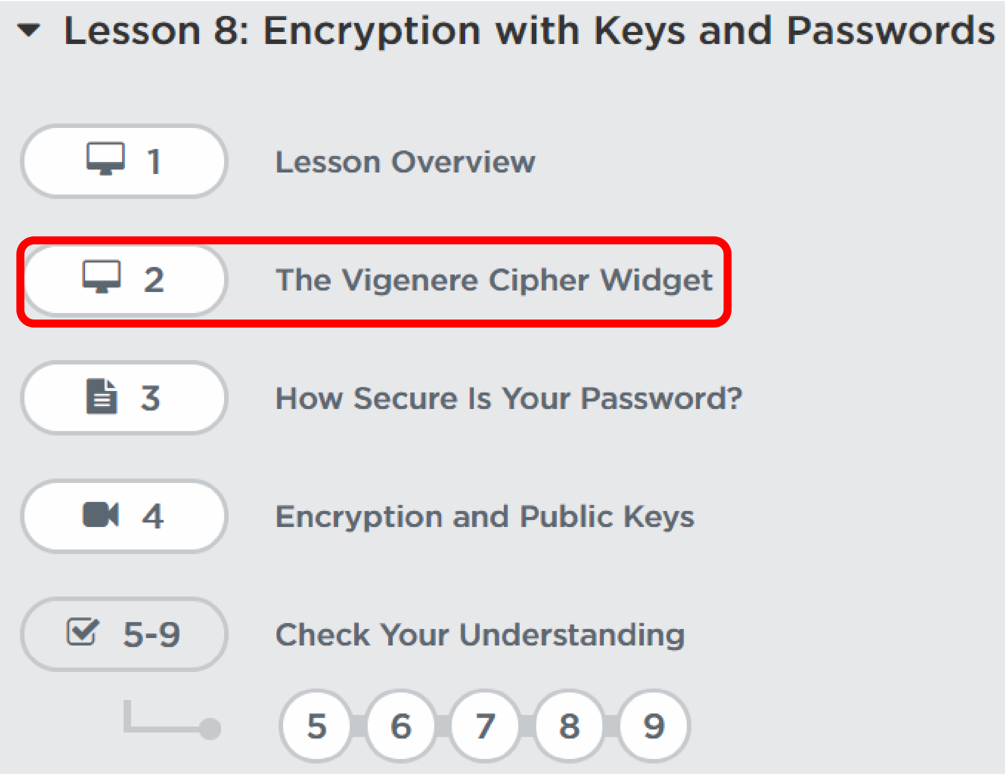
Second: With a partner, start by exploring the widget

Third: Complete the U4L6 worksheet (front and back)

Goals:

- Understand how the Vigenère Cipher Algorithm works
- Understand why simple frequency analysis doesn't work against this cipher
- Figure out what makes for a good v. bad secret key

KEY - Exploring the Vigenere Cipher Widget - Answer Key



▾ Lesson 8: Encryption with Keys and Passwords

1 Lesson Overview

2 The Vigenere Cipher Widget

3 How Secure Is Your Password?

4 Encryption and Public Keys

5-9 Check Your Understanding

Verbal Prompt:

From what you've seen, what are the properties of the Vigenere Cipher that make it harder to crack? In other words, if you had to crack a vigenere cipher what would you do?

______________***Share with a neighbor - Share as a class***

- Vigenere is strong because looking at the ciphertext there are no discernable patterns assuming a good key was chosen.
- Because the ciphertext is resistant to analysis it leaves us simply having to guess what the key is.
- Even if we know the length of the key we might still have to try every possible letter combination which is a prohibitively large number of possibilities.

Activity #2 (20 mins): Computationally Hard Problems -- How good is your password?

Introduction:

- We know that a good encryption algorithm reduces the problem of cracking it to simply guessing the key.
- We want the key to be **Computationally Hard** to guess - in other words, hard for a computer to guess.
- Computationally Hard typically means that arriving at the solution would take a computer a prohibitively long time - as in: centuries or eons.
- In terms of cracking encryption that means that the number of possible keys must be so large, that even a computer trying billions of possible keys per second is unlikely to arrive at the correct key in a reasonable amount of time.
- Nowadays when you use a password for a website or device, your password is used as a cryptographic key.
- So, choosing a good password is meaningful because we want the key to be hard for a computer to guess. How good is your password?...

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

Activity #2: Computationally Hard Problems -- How good is your password?

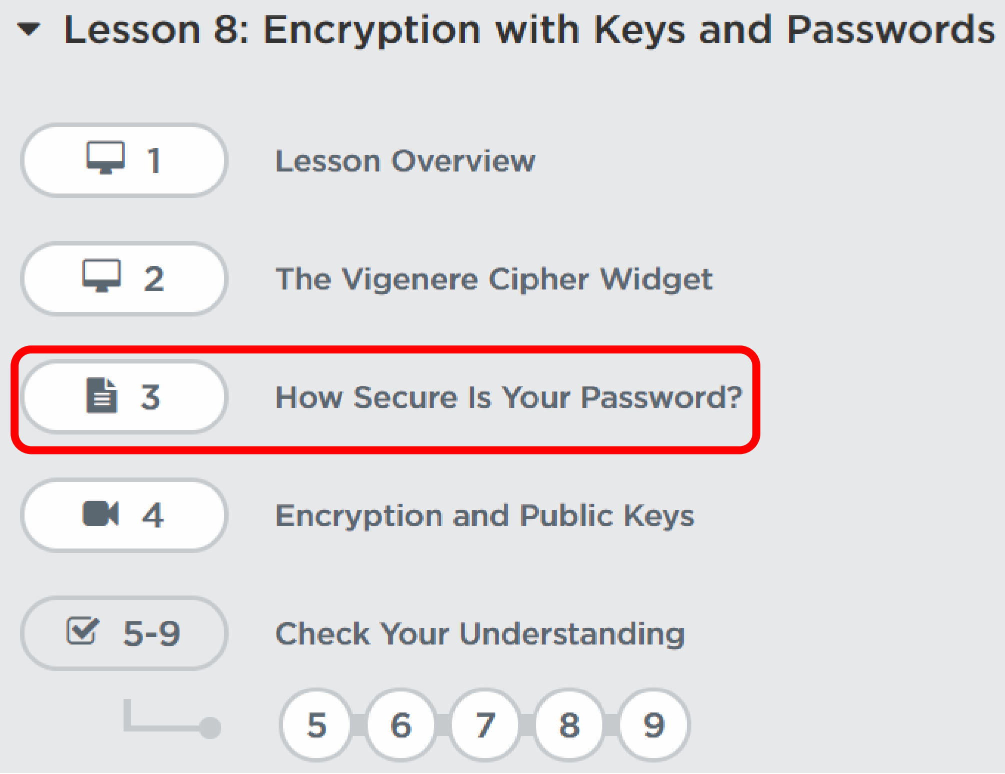
**Distribute Keys and Passwords - Worksheet

First: navigate to U4L8 - bubble 3

Second: read and attempt the suggested tasks

Third: complete the questions on the worksheet

PASSWORD ERROR:
SNOW WHITE AND THE SEVEN DWARFS NOT RECOGNISED AS EIGHT CHARACTERS
LYNCH


▾ Lesson 8: Encryption with Keys and Passwords

1 Lesson Overview

2 The Vigenere Cipher Widget

3 How Secure Is Your Password?

4 Encryption and Public Keys

5-9 Check Your Understanding

5 6 7 8 9

Wrap-Up (10-15 minutes)

Before the Vigenere cipher was cracked, many governments openly used it. That is, they made no secret about the fact that they were using the Vigenere cipher - it was publicly known. In the modern day, it remains the case that most encryption techniques are publicly known.

Wrap-Up (continued)

Written Prompt - ***IN YOUR NOTES***, respond to the following (2-minutes):

Why might it actually be a good thing that encryption algorithms are freely shared, so that anyone who wishes can try to crack them?

- If the security of an encryption technique relies solely on the method remaining a secret, it actually may not be that secure.
- Ideally, a method will be so secure that even if you know which technique was used, it is difficult or impossible to crack the message.
- By making encryption techniques public, we open them up to being tested by anyone who wishes to ensure there are no clever ways of cracking the encryption.

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

Video: Encryption and Public Keys (6:40)

Wrap-Up (continued)

We’re circling in on some powerful ideas of how secure communication works on the Internet these days. But we need to learn two more things:

1. We’ve seen how keys relate to the strength of encryption, but we haven’t seen the other side of it -- how modern encryption algorithms actually work. Vigenère was cracked, so what are we using now? In order to do this, we need to understand what kinds of problems are “hard” for computers to solve.
2. Right now, the only encryption we know uses a "symmetric key" -- both sender and reciever need to know the secret key, and so they need to meet ahead of time.

But is it possible for you and me to have a secure, private, encrypted exchange without meeting ahead of time and agreeing on a secret password.

The answer is “yes,” and we'll find out how it works in the next lesson.

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords

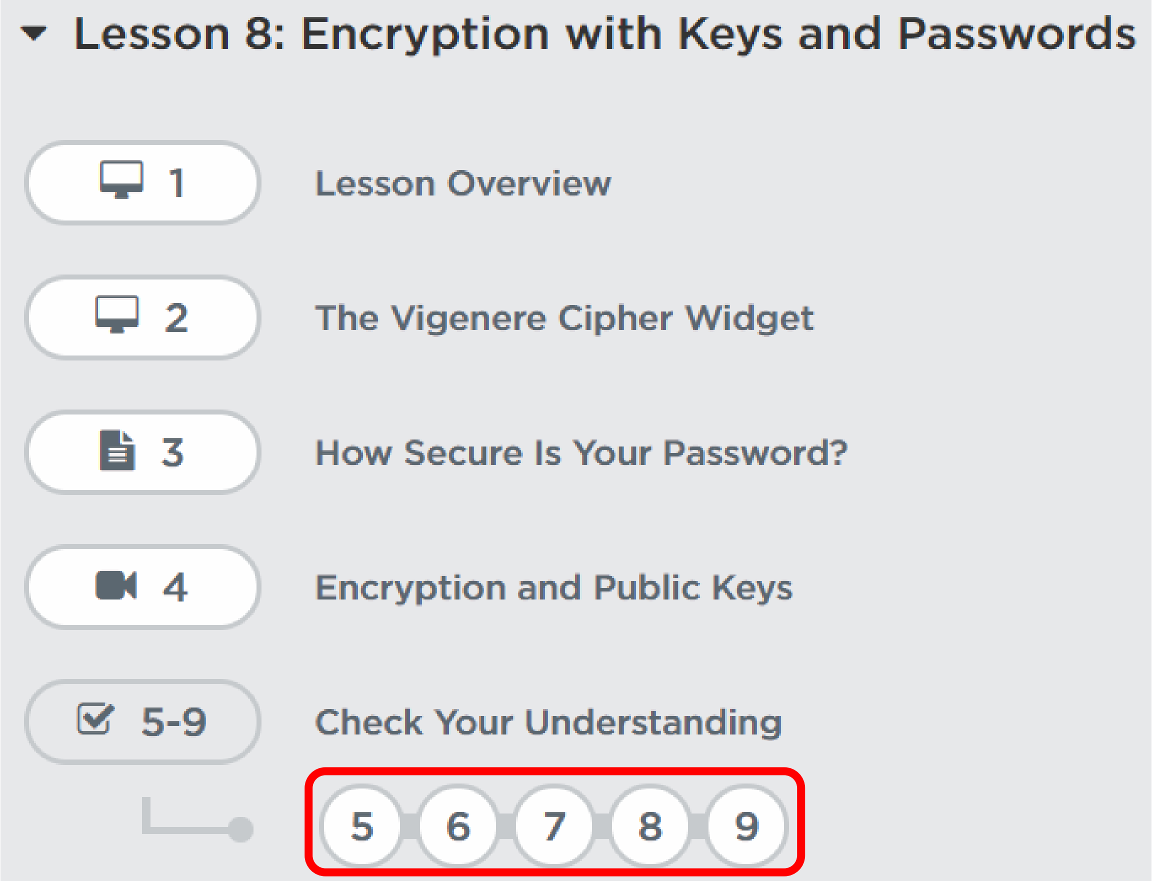
2nd video

(if time)

The Internet - Cybersecurity and Crime

(5:00)

Unit 4 Lesson 8 (U4L8)
Encryption with Keys and Passwords



Lesson 8: Encryption with Keys and Passwords

1 Lesson Overview

2 The Vigenere Cipher Widget

3 How Secure Is Your Password?

4 Encryption and Public Keys

☑ 5-9 Check Your Understanding

5 6 7 8 9