# Simple Encryption

Unit 4 Lesson 7 (U4L7)

Table of Contents

## Warm Up

Writing Prompt - IN YOUR NOTES, answer the following:

a) In your daily life what are some things that you or other people re on keeping a secret?
b) Who are these secrets being kept from?
c) How are these things kept secret?

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

- Social interactions (e.g., a surprise birthday party)
- A play in a sports game, your hand in a card game
- Personal identification information, PIN numbers, etc.
- Business and government negotiations

# Unit 4 Lesson 7 (U4L7)
# Simple Encryption


Secrecy is a critical part of our lives, in ways big and small. As our lives increasingly are conducted on the Internet, we want to be sure we can maintain the privacy of our information and control who has access to privileged information.

Digital commerce, business, government operations, and even social networks all rely on our ability to keep information from falling into the wrong hands.

Recall: As we saw with our activities on the Internet Simulator the internet is NOT secure

- We need a way to send secret messages...

## Classic Encryption - The Caesar Cipher

First…..a little background knowledge:

Many of the ideas we use to keep secrets in the digital age are far older than the Internet. The process of encoding a plain text message in some secret way is called Encryption

For example in Roman times Julius Caesar is reported to have encrypted messages to his soldiers and generals by using ***a simple alphabetic shift*** - every character was encrypted by substituting it with a character that was some fixed number of letters away in the alphabet.

As a result an alphabetic shift is often referred to as the Caesar Cipher.

**Prompt:**

- The message below was encrypted using a Caesar Cipher (an "alphabetic shift").
- Let's see how long it takes you to decode this message (remember it's just a shifting of the alphabet):

```
serr cvmmn va gur pnsrgrevn
```

**Recap**:

- With this simple encryption technique it only took a few minutes to decode a small message.
- What if the message were longer BUT you had a computational tool to help you?!

```
serr cvmmn va gur pnsrgrevn
```

Free pizza in the cafeteria

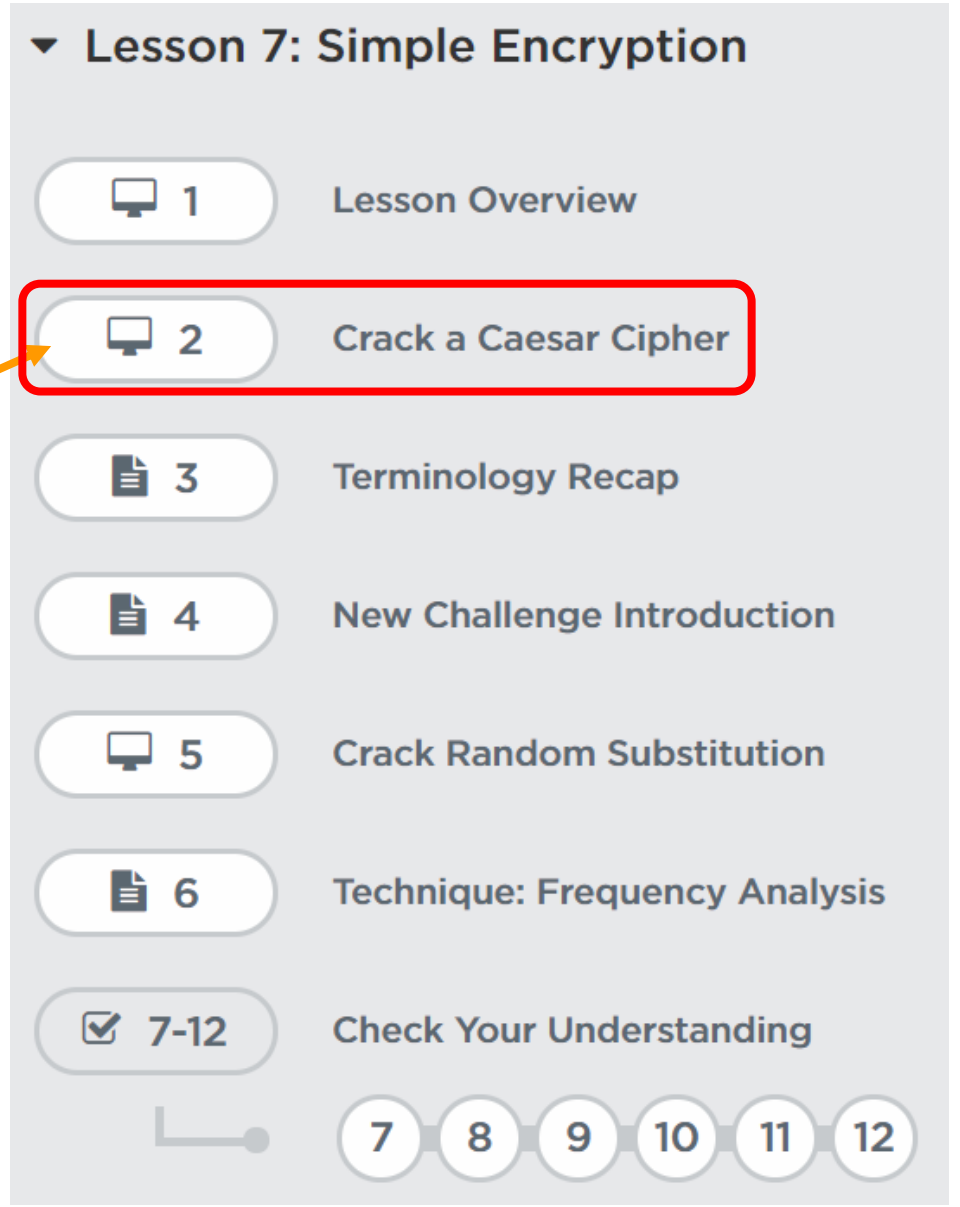
## Activity - Cracking Substitution Ciphers (35-minutes)

### Part 1 - Crack a Caesar Cipher (5 minutes)

**First:** Navigate to U4L5 bubble 2 (“Crack a Caesar Cipher”)

**Second**: Explore the widget to see what it does and doesn’t do

**Third**: Crack the code of **two or more messages**

## Activity - Cracking Substitution Ciphers (continued)

**Vocabulary - *IN YOUR NOTES*, write down the following terms:**

- **Encryption** - a process of encoding messages to keep them secret, so only "authorized" parties can read it.
- **Decryption** - a process that reverses encryption, taking a secret message and reproducing the original plain text
- **Cipher** - the generic term for a technique (or algorithm) that performs encryption
- **Caesar's Cipher** - a technique for encryption that shifts the alphabet by some number of characters.

# Activity - Cracking Substitution Ciphers (continued)

## Part 2 - Crack a Random Substitution Cipher

- What if instead of shifting the whole alphabet, we mapped every letter of the alphabet to a random different letter of the alphabet? This is called a *random substitution cipher*.
- The new version of the widget you'll see is a more sophisticated version of the encryption tool that shows you lots of different stuff.
- But what it does is bit of a mystery! Let's check it out...

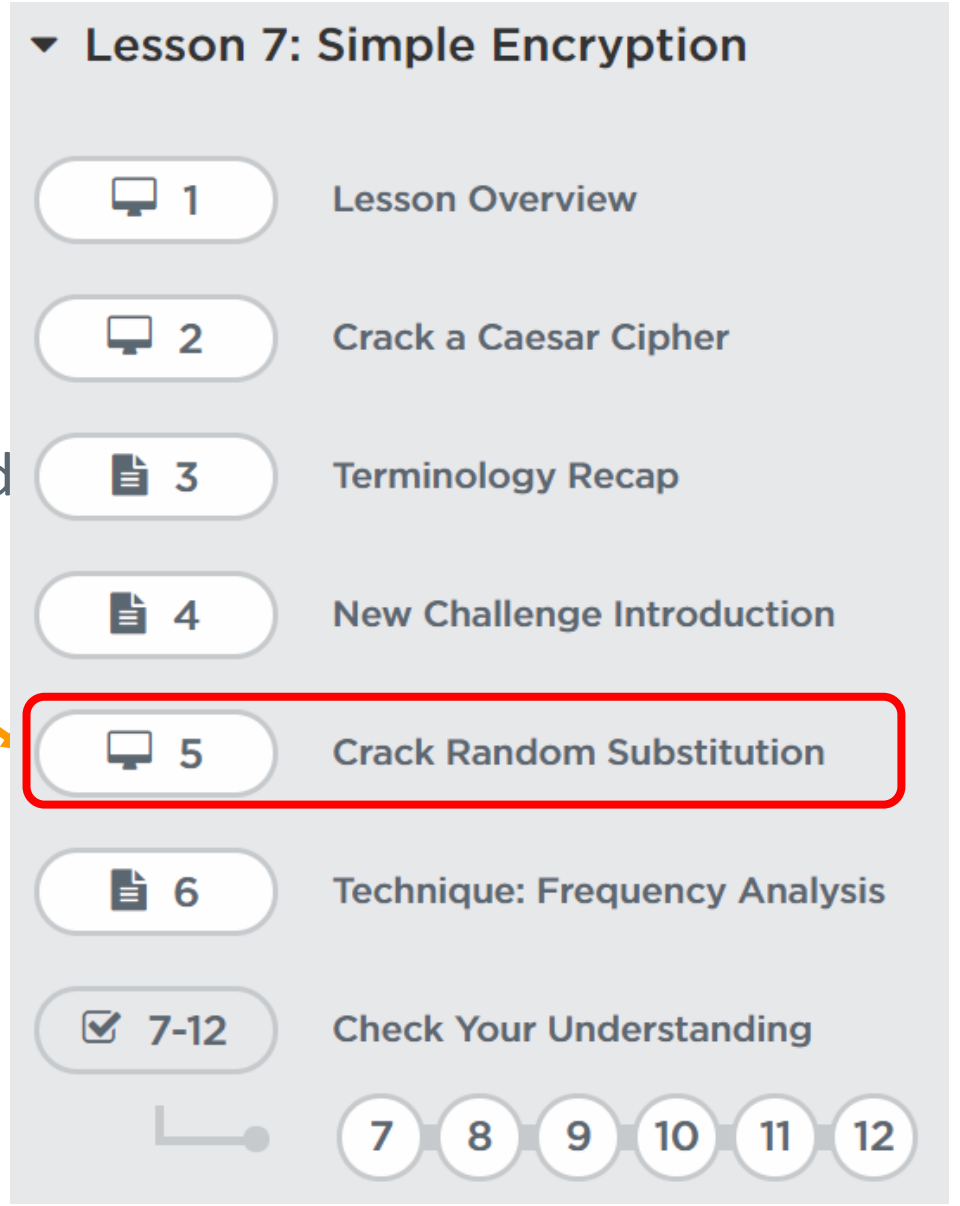
## Activity - Cracking Substitution Ciphers (continued)

### Part 2 - Crack a Random Substitution Cipher

**First:** Navigate to U4L7 bubble 5 ("Crack Random Substitution")

**Second**: Explore the widget to see what it does and doesn't d (6 minutes)

**Third**: Share out about findings

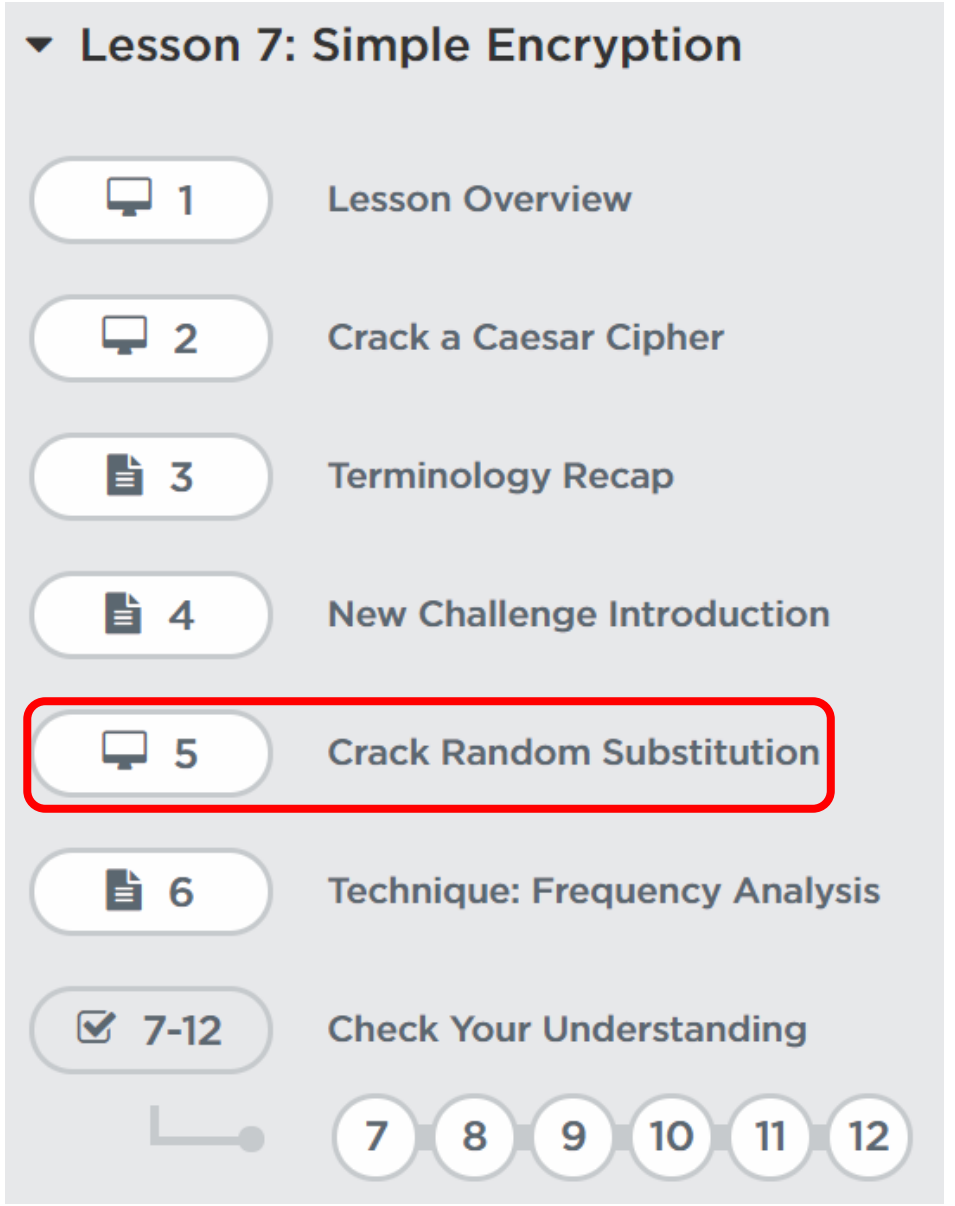



## Activity - Cracking Substitution Ciphers (continued)

### Part 2 - Crack a Random Substitution Cipher

**Challenge (15 minutes)**

Try to crack one (or more) of the encrypted messages

## Wrap Up

- The "strength" of encryption is related to how easy it is to crack a message, assuming adversary knows the technique but not the exact "key"
- A random substitution cipher is very crackable by hand though it might take some time, trial and error.
- However, when aided with computational tools, a random substitution cipher can be cracked by a novice in a matter of minutes.
- If we are to create a secure Internet, we will need to develop tools and protocols which can resist the enormous computational power of modern computers.

## Wrap Up - Writing Prompts (IN YOUR NOTES, answer the following…)

**Prompt #1**: How much easier is it to crack a caesar cipher than a random substitution cipher? Can you put a number on it?

**Prompt #2**: Recall that in RFC 3271, “The Internet is for Everyone” Vint Cerf wrote the following:

*Internet is for everyone - but it won't be if its users cannot protect their privacy and the confidentiality of transactions conducted on the network. Let us dedicate ourselves to the proposition that cryptographic technology sufficient to protect privacy from unauthorized disclosure should be freely available, applicable and exportable.*

What did he mean by "cryptographic technology?" What does it mean to you now?

# Unit 4 Lesson 7 (U4L7)
# Simple Encryption


## Lesson 7: Simple Encryption