Technology Skills Curriculum Lesson 8:

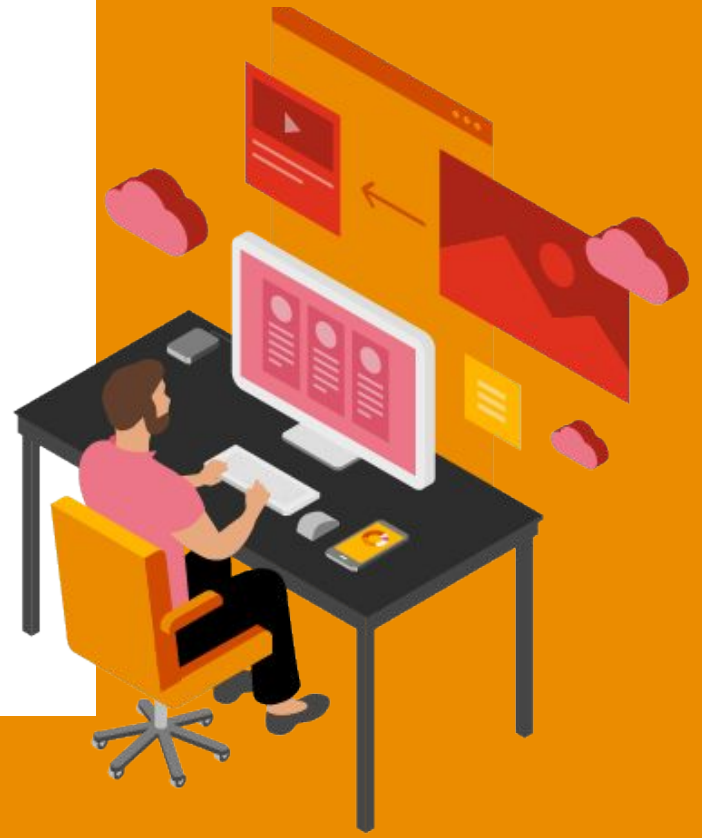
Cybersecurity- Simple Encryption

pwc

Agenda

Let's get started

1. Getting started: Classic Encryption
2. Main activity: Cracking Substitution Ciphers
3. Crack a Caesar Cipher
4. Crack a random substitution Cipher
5. Wrap up: Video
6. Careers reflection



Objectives

You will be able to:

- **Explain why encryption is an important need for everyday life on the Internet.**
- **Crack a message encrypted with a Caesar cipher using a Caesar Cipher Widget**
- **Crack a message encrypted with random substitution using Frequency Analysis**
- **Explain the weaknesses and security flaws of substitution ciphers**

01

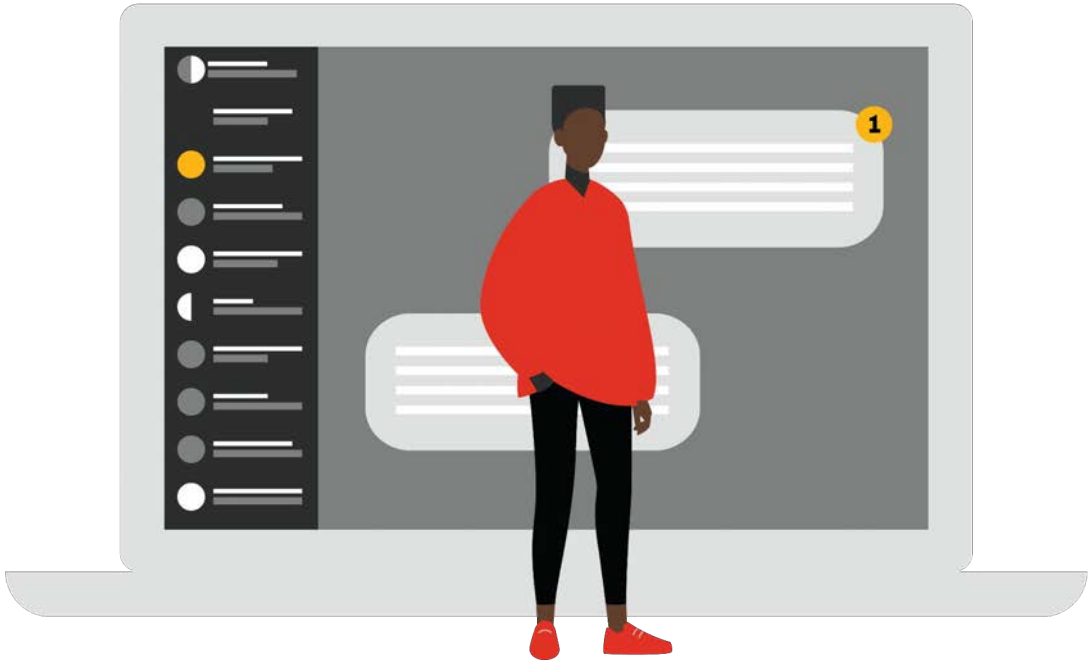
Classic Encryption

Classic Encryption: The Caesar Cipher

The process of encoding a plain text message in some secret way is called Encryption.

Historical example

Many of the ideas we use to keep secrets in the digital age are far older than the Internet. 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. So **an alphabetic shift is often referred to as the Caesar Cipher.**



Why do we need encryption?

This security is necessary as **the Internet is not inherently secure.** Packets traveling across the Internet move through many routers, each of which could be owned by different people or organisations

02

Cracking Substitution Ciphers

Can you crack this encryption?

This message was encrypted using a Caesar Cipher (an "alphabetic shift")

Task:
Try and decode this message (remember it's just a shifting of the alphabet). **You have 5 minutes do this**

SERR CVMMN VA GUR PNSRGREVN

03

Crack a Caesar Cipher

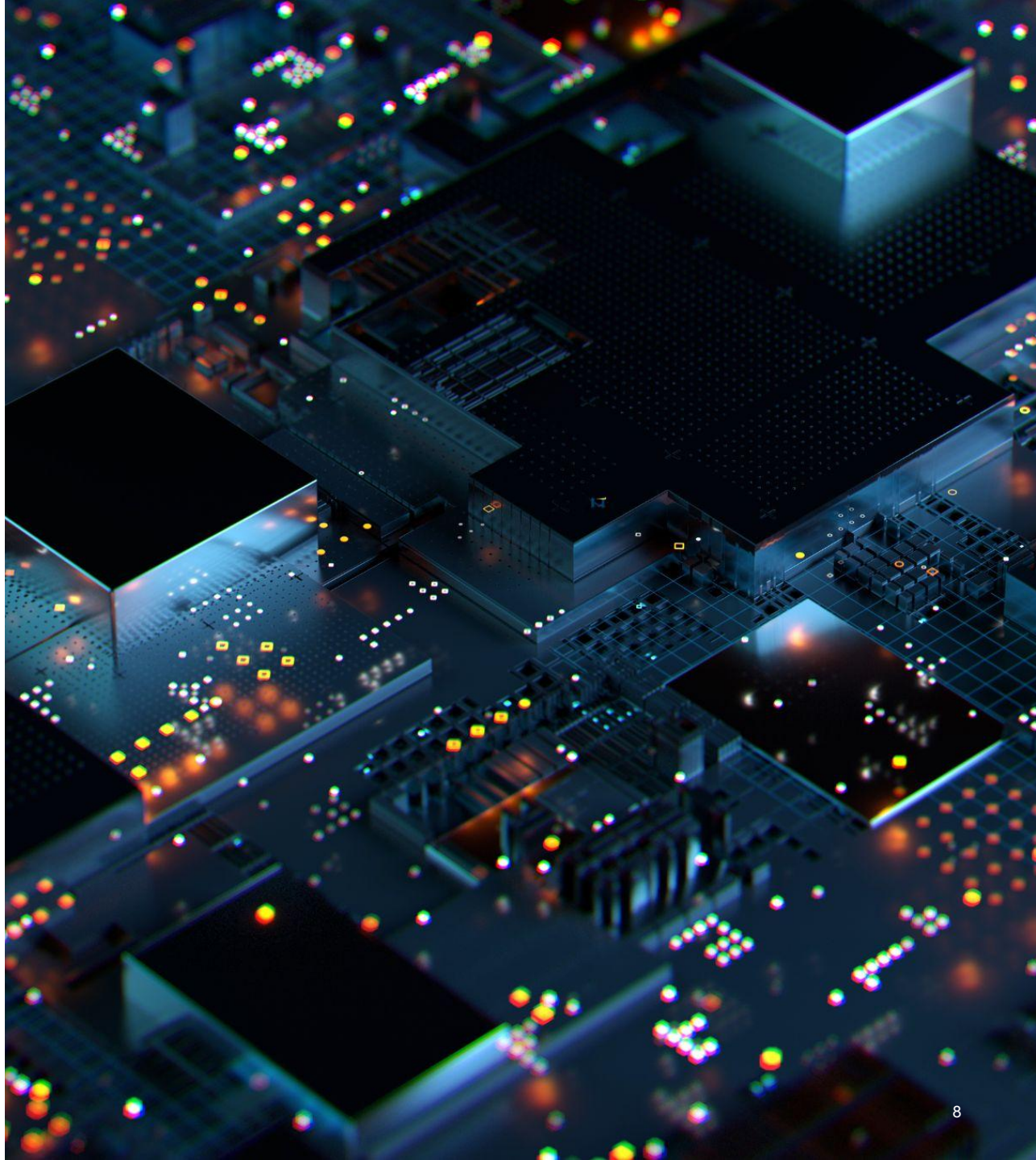
Crack a Caesar Cipher

Get yourselves into pairs and following this link:
https://studio.code.org/s/pwc

Task:

1. **Select a message encrypted** with a caesar cipher and use the provided widget to "crack" it.
2. **Experiment with the tool** - click things, poke around, figure out what it's doing.
3. **Choose one of the messages from the pull down menu** and try to crack it using the tool.
4. If you want to, **enter you own message**, encrypt it, and have a friend decrypt it.

You have 10 minutes to get into the tool and crack a few messages with your partner



04

Crack a random substitution Cipher

Crack a random substitution Cipher

Next we're going to look at a new version of the widget. This is a more sophisticated version of the encryption tool that shows you lots of different stuff.

Click to the next bubble to see the frequency analysis version of the widget. It should look like the picture on the right

Task:

1. **Explore this widget to see if you can discover what the tool is showing you and allowing you to do.** What information is being presented to you? Try and figure out what the tool lets you do. You have **10 minutes**
2. **Try and crack one of the messages**. You have **15-20 minutes.** If you finish there are more to try.
3. **Stretch task:** If you time left to spare you can enter your own messages, do a random substitution to encrypt it, then copy/paste the encrypted version and see if your partner can crack it.

Definition: A Widget: A small mechanical device or control

05

Wrap up: Video

Wrap up and reflection:

Task: Watch this video

Reflection questions

- What is the relationship between cryptographic keys and passwords?
- What is the difference between a Key and an encryption algorithm?
- Why does using longer passwords make them harder to guess?

06

Careers reflection

What employability skills have you developed in this session?

Leadership	Business minded	Technical capabilities	Global acumen	Relationships
• Teamwork • Problem solving • Decision making	• Quality in everything you do • Improvement • Thinking commercially	• Your knowledge of potential jobs you could apply for • What have you done you are proud of • Ability to learn	• Seeking new perspectives • Sharing ideas • Coping with change • Open minded	• Communication skills • Building relationships • Working with others

Want to find out more?

Keep up to date: PwC Podcast - spotify - A-Z of tech: A is for Artificial Intelligence, B is for Blockchain, C is for Cyber Security. Follow our journey through an alphabet of technology trends with PwC's technologists and special guests.

Opportunities in tech: You might be interested in technology opportunities at university or in the workplace. Lots of companies and universities have opportunities. **Here are some at PwC:**

- 5 day paid work experience ‘Insight Weeks’ for Year 12 students.
- Technology Degree Apprenticeships and Data Science Graduate Apprenticeships.
- School and College Leaver Apprenticeships at PwC

Thank you

pwc.co.uk