CYBERSECURITY

*Developed for GIRLsmarts4tech*

<https://www.cs.ubc.ca/girlsmarts4tech/>

# OVERVIEW

This lesson consists of a powerpoint presentation and 3 associated activities. The activities are described in detail below, and the powerpoint slides are accompanied by detailed speaker notes. There are video examples for the instructor’s use which further explain the activities and concepts. This lesson has previously been used with the grade 6 age group, but the first two activities may be appropriate for younger children and the third activity may be appropriate for older children.

# LEARNING GOALS

By the end of the activity, participants should:

1. Understand and be able to explain the terms: encryption, decryption, cipher, key, and cryptography.
2. Understand the basic principles behind encryption, including why it is so useful today, and be able to decrypt simple messages using a key.
3. Understand public-key encryption in terms of simple analogies and be able to use a public map to send messages to others.

# OVERLAP WITH BC CURRICULUM

1. Internet Safety
2. Simple algorithms

# TECHNICAL REQUIREMENTS

1. The instructor should have access to a computer and projector to show the powerpoint presentation.

# FACILITATOR INSTRUCTIONS

* The instructor should read through the activities and preview the powerpoint to familiarize themselves with the content and key terms.
* The instructor should preview the videos linked on slides 4 and 12 of the powerpoint.
* For more information regarding the activities, the instructor can watch the associated videos:
  + Shift Cipher Teacher Overview
  + Pigpen Cipher Teacher Overview
  + Public Key Encryption Teacher Overview
* The activities require students to complete part of the activity individually and part of the activity in pairs. The instructor can choose whether to split students up at the beginning of the activity or after the individual component, and whether to keep the same pairs for subsequent activities.
* Activity 3 requires each student to have a printed copy of Activity 3 Printable Worksheet - Public Map
* Activity 3 is more challenging than activity 1 and 2, so the instructor may feel that only a selection of the activities are appropriate for their class.

# INTRODUCTION: POWERPOINT

Start the lesson by presenting slides 1-12 of the powerpoint. Students will learn the basics of cybersecurity and some of the key terms used in cybersecurity and throughout this lesson.

# ACTIVITY 1: SHIFT CIPHER

## OVERVIEW

In this activity, students will use a shift cipher to encrypt and decrypt a message.

## ASSOCIATED VIDEO (for instructor)

Shift Cipher Teacher Overview

## REQUIRED MATERIALS (per student)

* Writing utensil
* A slip of paper (large enough to write a sentence on)
* A piece of scrap paper for rough work

## POWERPOINT

This activity follows powerpoint slides 13 - 19.

## ACTIVITY STEPS

1. Present powerpoint slides 13-18 explaining the shift cipher.
2. Introduce the activity using powerpoint slide 19.
3. Have every student choose a number. It is easiest if the numbers are between 1-10.
4. Have every student come up with a message to encrypt. You can recommend the length of the message based on the students’ ability level, or provide a message for them to encrypt. An example message is: “Stay safe online”.
5. Students will now encrypt their message using a shift cipher. To encrypt their message, they will shift each letter in their message forward by the number of letters corresponding to the number they have chosen. For example, if the chosen number is 5, “Stay safe online” becomes “Xyfe xfkj tsqnsj”. They should use their scrap paper to encrypt their message. Once they are sure it is correct, they should copy the encrypted message and chosen number onto their slip of paper.
6. Have students partner up. They should each have a slip of paper, on which is their encrypted message and the number used to encrypt it. Students will trade their slip of paper with their partner.
7. Students will now decrypt their partner’s message by shifting all of the letters backward by the provided number. They should use their scrap paper to decrypt the message, then write the decrypted message on the back of their slip of paper.
8. The students have now passed a secret message between each other! They can check with their partners to see if the decrypted message is correct.

# ACTIVITY 2: PIGPEN CIPHER

## OVERVIEW

In this activity, students will use a pigpen cipher to encrypt and decrypt a message.

## ASSOCIATED VIDEO (for instructor)

Pigpen Cipher Teacher Overview

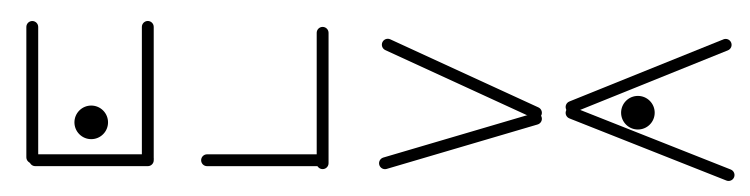
## REQUIRED MATERIALS (per student)

* Writing utensil
* A label to write their name on (e.g. a sticky label for their shirt or a paper name plate for their desk)
* A slip of paper (large enough to write a sentence on)
* A piece of scrap paper for rough work

## POWERPOINT

This activity follows powerpoint slides 20 - 22.

## ACTIVITY STEPS

1. Present powerpoint slides 20-21 explaining the pigpen cipher.
2. Introduce the activity using powerpoint slide 22.
3. Have every student encrypt their own name to make themselves a name label. To encrypt their name, they will find the symbol which corresponds to each letter in their name and replace the letter with the symbol. For example, the name “Katy” would be encrypted as . They should use their scrap paper to encrypt their name. Once they are sure it is correct, they should copy the encrypted name onto their name label.
4. Now have every student come up with a message to encrypt. You can recommend the length of the message based on the students’ ability level, or provide a message for them to encrypt. An example message is: “Stay safe online”.
5. Students will now encrypt their message using a pigpen cipher, the same way they encrypted their name. They should use their scrap paper to encrypt their message. Once they are sure it is correct, they should copy the encrypted message onto their slip of paper.
6. Have students partner up. They should each have a slip of paper, on which is their encrypted message. Students will trade their slip of paper with their partner.
7. Students will now decrypt their partner’s message by finding the letter which corresponds to each symbol then replacing the symbol with that letter. They should use their scrap paper to decrypt the message, then write the decrypted message on the back of their slip of paper.
8. The students have now passed another secret message between each other! They can check with their partners to see if the decrypted message is correct.

# 

# 

# ACTIVITY 3: PUBLIC KEY ENCRYPTION

## OVERVIEW

This activity is based on the CS Unplugged [Kid Krypto - Public-key Encryption](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf) activity. Students will use a public map to encode a number, which can be decoded using a private map.

## 

## ASSOCIATED VIDEO (for instructor)

Public Key Encryption Teacher Overview

## REQUIRED MATERIALS (per student)

* Pencil
* Eraser
* Copy of Activity 3 Printable Worksheet - Public Map
* Optional: a coloured pencil/pen

## POWERPOINT

This activity follows powerpoint slides 24 - 41.

## ACTIVITY STEPS

1. Present powerpoint slides 24-27 explaining public key encryption.
2. Introduce the activity using powerpoint slide 28. Go through slides 28-35 to give an overview of the activity and explain how it works.
3. Start the activity with slide 36. Have the students complete the tasks on the slide, then go to slide 37. Repeat until you reach slide 39. More detailed instructions are provided in the speaker notes on the powerpoint.
4. Each student should now have a public map with a number at each intersection. The number at each intersection should be the sum total of the original numbers at the connected intersections.
5. Have students partner up and trade their maps.
6. Present slide 40-41. Students should now decrypt the public map using the private map on slide 41. They will sum the numbers at the enlarged nodes and should produce the number their partner encrypted using the public map.
7. The students have now passed a secret number between each other. Start a class discussion on how they could use the public/private map method to send a more complex message. (Suggestions: Assign numbers to each letter of the alphabet, then send several maps which spell out a message, or send a message that has been encrypted using a shift cipher alongside a map which has encoded the number used for the shift cipher.)

# 

# 

# THANK YOU!