



UNIVERSITY of HAWAII®
MAUI COLLEGE

RING - Cybersecurity Curriculum

Debasis Bhattacharya, JD, DBA
University of Hawaii Maui
College
debasisb@hawaii.edu
maui.hawaii.edu/cybersecurity

Abstract

RING (Regions Investing in the Next Generation) is a free online high school cybersecurity course that offers engaging content specifically for rural students, homeschool students, and students attending schools without existing cybersecurity programs.

RING is structured for high school students, grades 9-12. The curriculum has been developed through the National Security Agency's RING program grant to the University of Alabama in Huntsville (UAH).

University of Hawaii Maui College is part of a coalition of colleges across the U.S. supported by funds from the NSA to teach RING to high school teachers and students.

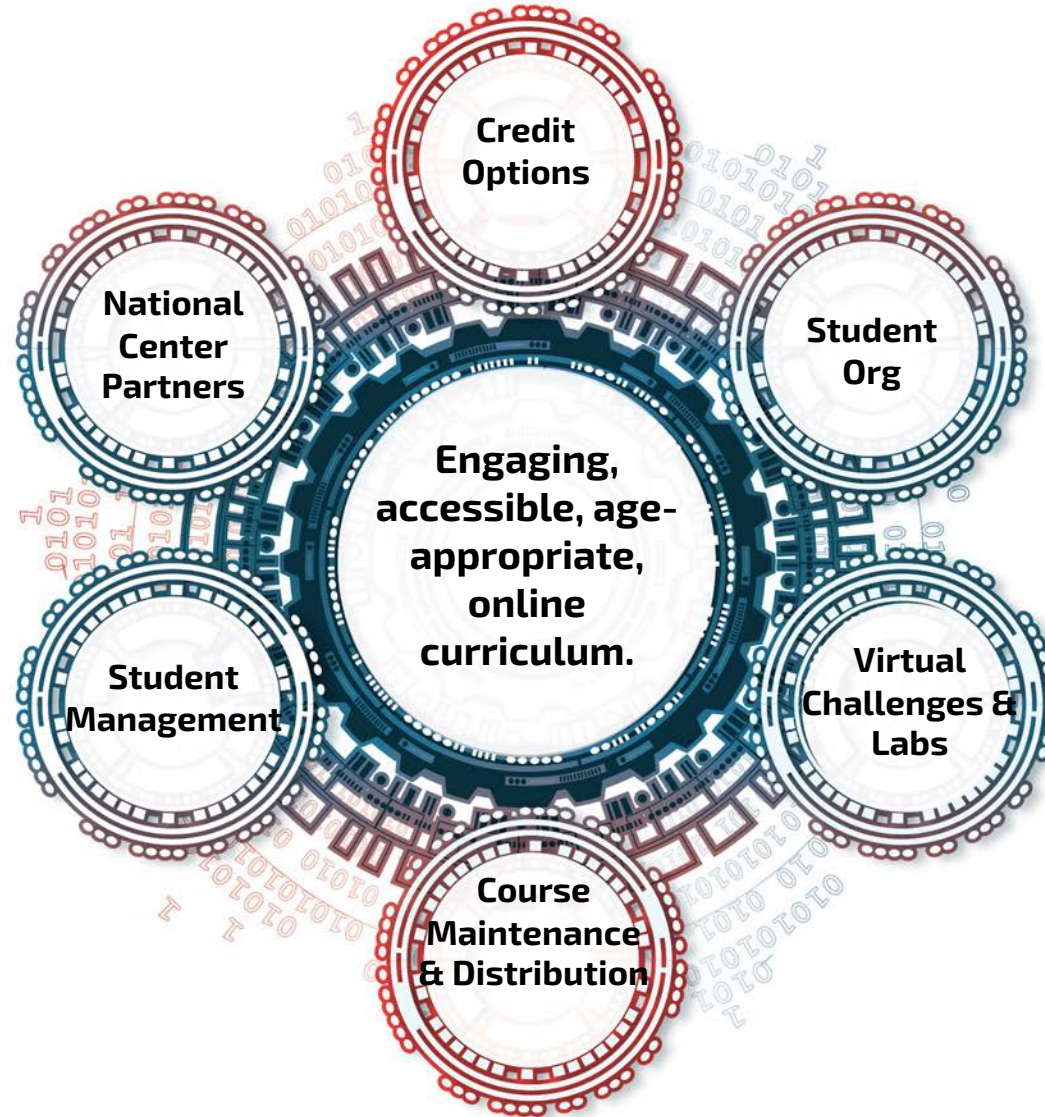
Agenda

1. What is RING?
2. How do teachers access RING?
3. What are the modules within RING?
 - Sample Module - Unit 2 - Establishing Trust
 - Sample Activity - Caesar Cypher
4. Implementation of RING in Hawaii Dept of Education
5. Reflections!

RING Overview



Regions
Investing in the
Next
Generation




RING is...
Cybersecurity for
students without
access to a cyber
program.

- Rural
- Homeschool
- Under-resourced

RING site!

caecommunity.org/initiative/k12-ring


Log In

 CAE
IN CYBERSECURITY
COMMUNITY

HOME ABOUT US ▸ NEWS EVENTS ▸ CAE MAP RESOURCES ▸

K-12 PATHWAY PROGRAM: RING

Initiatives / K-12 Pathway Program: RING

 RING | REGIONS INVESTING IN
THE NEXT GENERATION

Leading Institutions: The University of Alabama Huntsville, Moraine Valley Community College

<https://caecommunity.org/initiative/k12-ring>

RING sign up

Resource Links

[RING Curriculum Request Form for Educators](#)
[RING Student Enrollment Request Form](#)
[RING Guest Speaker Registration Form](#)
[Affiliated Public Resource - Interactive E-Mates](#)
[Affiliated Public Resource - Interactive Virtual Escape Rooms](#)

Files

No Files Found.

Contacts

Jesse R. Hairston

Initiative Co-Primary POC

Email: ring@caecommunity.org

Dr. John Sands

Initiative Co-Primary POC

Email: sands@morainevalley.edu

Link for Teachers to sign up - [here!](#)

Teach with RING!

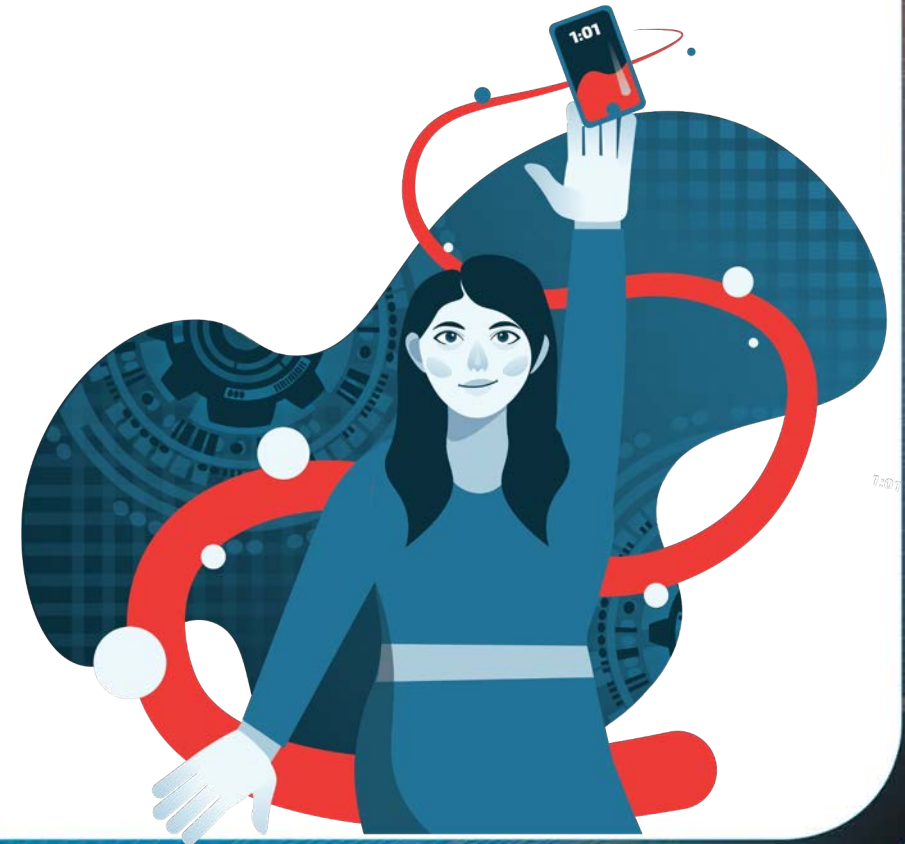
Teacher Curriculum Request Form



Educators* can gain full access to the curriculum package

- All Units available
- Gain access to virtual labs
- RING Student Org events
- Provide feedback

*Educators who request access must provide proof of their school/homeschool affiliation.



RING Canvas site



≡ RING 2023


RING Summer 2023

Edit



Content Update - Summer 2023

IMPORTANT ANNOUNCEMENT

- If you have accessed the course prior to July 20, 2023, please see the following [Change Log](#)  for a list of course changes that may have impacted any resources you have downloaded.
- If you previously have been utilizing an export of the course (such as an .imsc file), it is now out of date. If a new file of the course is needed, please reach out to ring@caecommunity.org to request the updated version.

Curriculum Package

Lesson Plans & Instructor Slides

Unit Timeline

Lesson Plan

Tuesday Sep 22, 2020

Ubiquitous Connectivity

Day 3: 3.1

Standards and Objectives

3.1.1 EU The Internet is a large, globally distributed network that is divided into L...

3.1.1 LO Students will explain how devices use layers to communicate across L...

3.1.1a EK Networks carry two types of information, those that allow for the co...

CAE KUs

Lesson Delivery and Setup

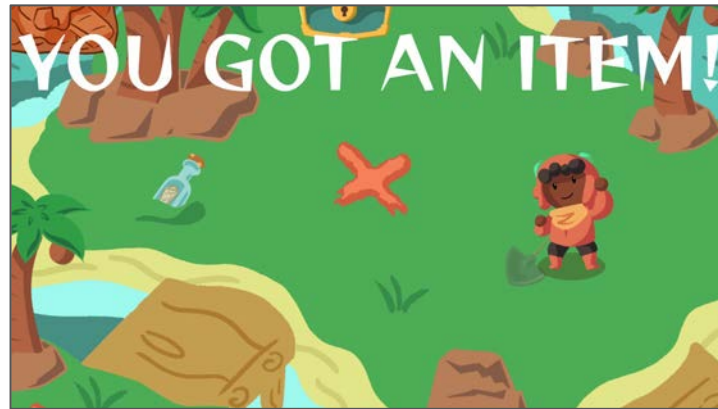
Instructor will need a computer, access to the Internet, and a projector (or appropriate screen sharing software if virtual). Student activities can be completed on paper or digitally. Students will need access to the Internet for some activities.

Procedures

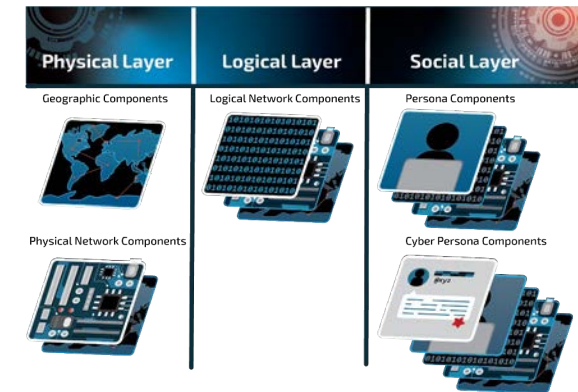
Warm Up Activity

Have students work with a partner to describe a grocery store. They might list things like the customers, the employees, the cash

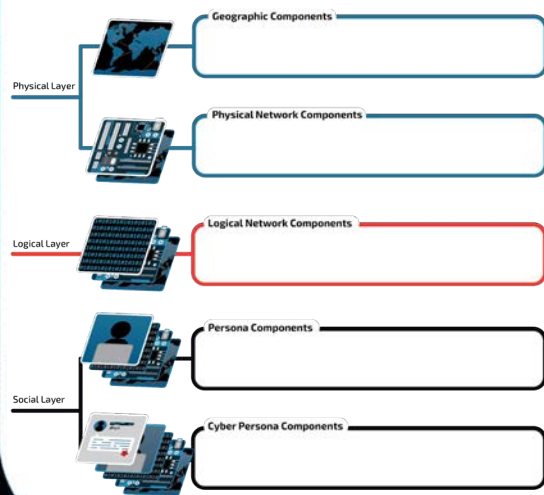
Labs & Games



Visually-Rich Content



Graphic Organizers



Name: _____ Date: _____

Class: _____

Period/Block: _____

Classify the CIA Triad (Print)

Objective: I can categorize the CIA Triad.

Part 1: Drag-and-drop each part of the CIA Triad to match the scenario.

Confidentiality **Integrity** **Availability**

Scenario 1: Fraudulent dollar bills.

Which part of the Triad does this scenario VIOLATE?

Scenario 2: Glasses with a built-in microphone.

Which part of the Triad does this scenario VIOLATE?

Scenario 3: A cell phone signal jammer.

Which part of the Triad does this scenario VIOLATE?

Assessments

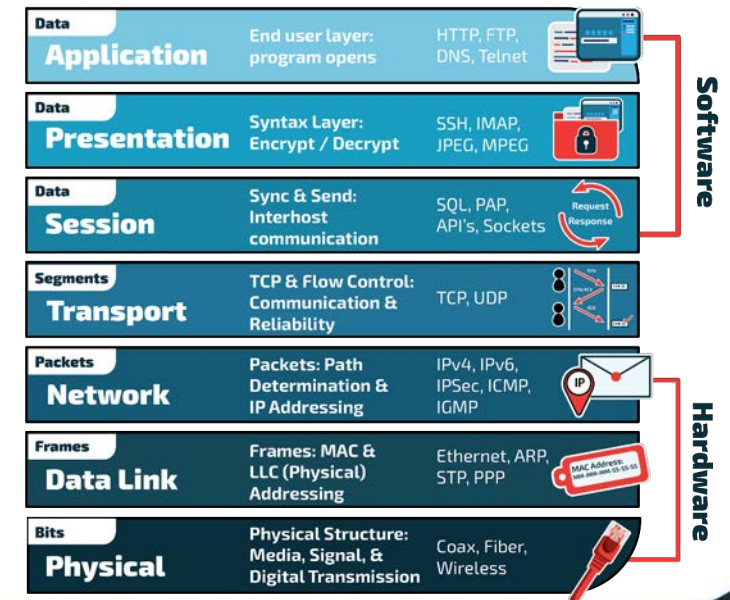
Name: _____ Class: _____ Date: _____ ID: A

Unit 11 Authentication and Identity Management

Multiple Choice

Identify the choice that best completes the statement or answers the question.

1. This ties behavior to a specific user.
a. password
b. username
c. least privilege
d. multi-factor
2. Which of the following is NOT a way to authenticate a user?
a. Something the user knows
b. Someone the user knows
c. Something the user is
d. Something the user has
3. Which of the following is something the user does?
a. smartcard
b. fingerprint
c. signature recognition
d. retinal scan
4. Which of the following is NOT a good password strategy?
a. Making a good password and using it over and over
b. Having a password that is easy to remember but difficult to guess
c. Having a password that is complex
d. Making a unique password for each account
5. Which of the following is NOT a factor in password strength?
a. length
b. type of account
c. complexity
d. unpredictability
6. Simon finds a briefcase that has a lock that is three numbers long (_____) what is the maximum number of tries it would take her to find the correct combination of the lock?
a. 10
b. 100
c. 1,000
d. 10,000
7. Which password would take the longest to crack?
a. 123456
b. T@ke1T
c. apple1
d. qwerty
8. Which of the following is an example of good password security?
a. changing passwords often
b. hiding the password underneath the keyboard
c. sharing your password with only your best friend
d. keeping your password the same as the default password

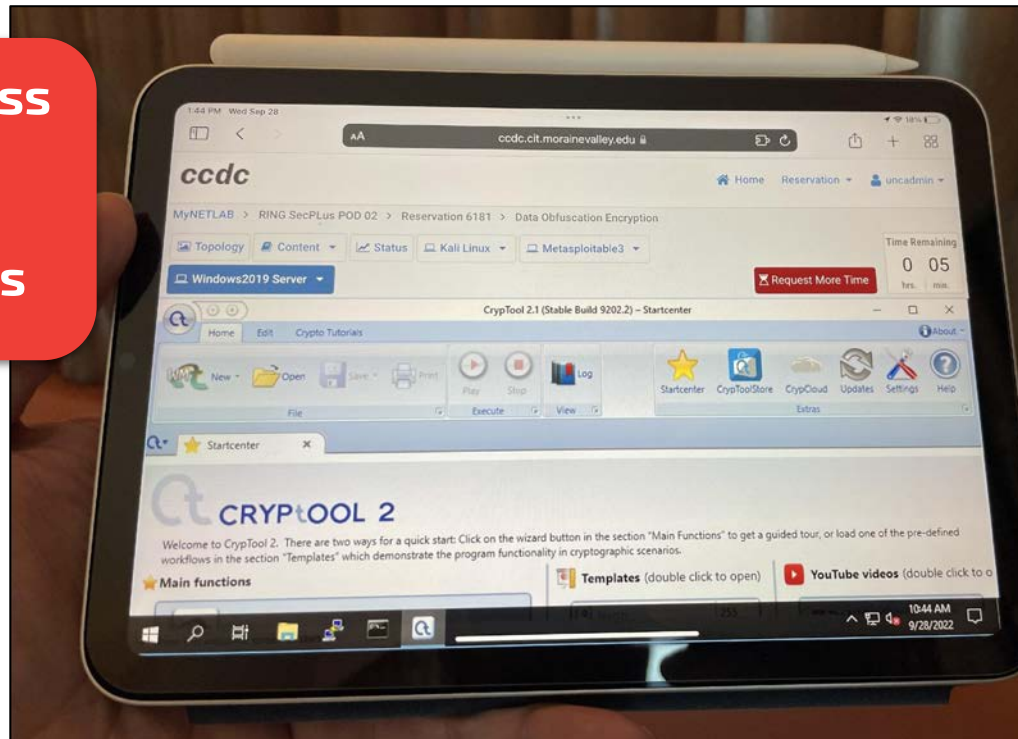


Lab Access

Netlabs offer virtual machines on any device.
Coastline Community College hosts Netlab access for RING teachers across the country.

RING Netlab Access

- 18 teachers
- 12 states
- 350 students



Competency Lab 3 – Hashing, Encryption, and Password Cracking

After your excellent work on the network, the agency is loaning you to help law enforcement to take down a ransomware group. As part of the sting operation, we have to send the file 'Meeting' from the StingOps folder located on Kali Linux desktop. We suspect that the group will try to change the contents of the message in-transit so your job is to make sure our agent inside has a way to verify the integrity of the document he receives.

1. Produce text file 'HASH' that can be sent via secure channel for verification purposes. Please make sure the file ONLY contain the SHA256 hash of the secret file (i.e., get rid of the file's name). Take a screenshot of the open HASH file.

Command: `sha256sum <filename> | awk '{print $1}' > HASH`

```
student@kali-lite: ~/Desktop/StingOps$ sha256sum Meeting | awk '{print $1}' > HASH
student@kali-lite: ~/Desktop/StingOps$
-D:\Desktop\StingOps\HASH - Messagepad
File Edit View Document Help
1 1e3d5a377598f4e9079288cc7be2626a947aa768a1492c2365de333134efdb668
```

2. Count the number of characters in the HASH file. Is the number correct? Why?

Command: `wc -m HASH`

```
student@kali-lite: ~/Desktop/StingOps$ wc -m HASH
64 HASH
student@kali-lite: ~/Desktop/StingOps$
```

YES
SHA256 create 64-character hash

Excellent job. We sent the document and our agent already replied. For security purposes he used the polyinstantiation strategy and sent multiple documents as part of the package. The documents, along with the hash file Verification we received through secure channel were saved to Reply folder on the Linux Kali desktop. We need your help to detect the correct document.

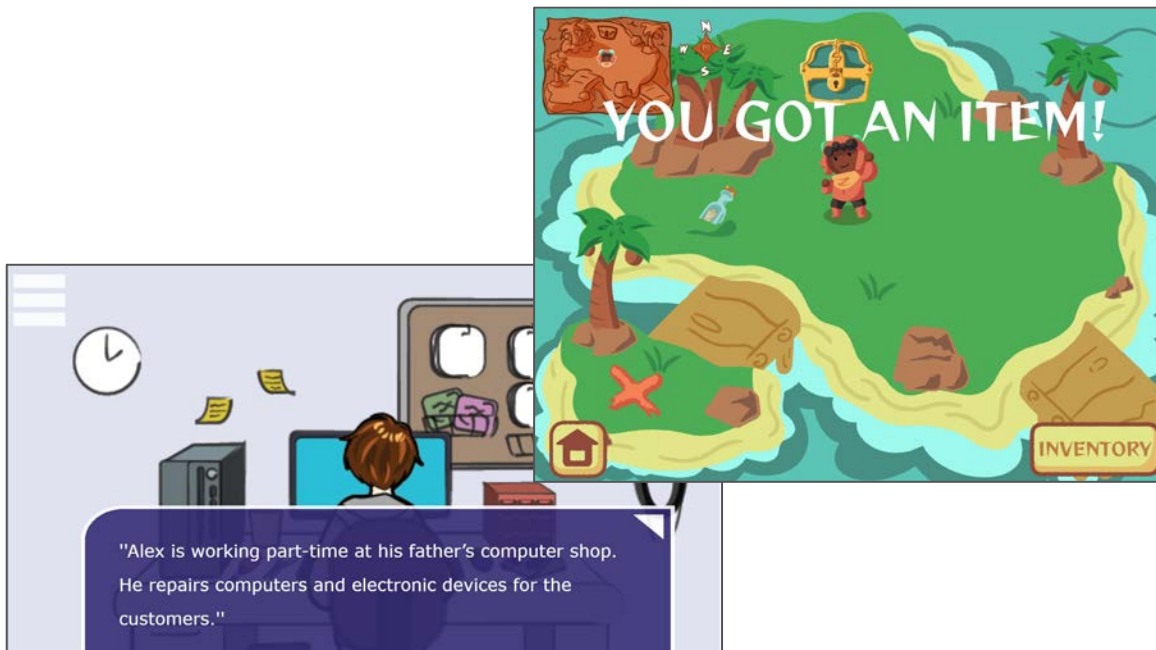
3. Please identify the correct document.

Command: `sha256sum <file(s)> >> Candidates OR find -type f -exec sha256sum {} \; >> Candidates
grep -f <sent_hash_file> Candidates`

Labs and Games

Labs provide hands-on learning through an online portal.

Games map to Big Ideas that drive the primary learning objectives.



Asymmetric Practice

Name: _____
Date: _____
Period/Block: _____

Objectives:

Explain the relationship between public and private keys in asymmetric cryptography.

Apply an asymmetric cryptographic tool to accomplish confidentiality and integrity in a practical scenario.

Overview

RSA is a popular algorithm used for asymmetric cryptography. It can be used to generate public-private key pairs and both encrypt and decrypt information. You will explore RSA using a simple online tool to encrypt a message to your partner. In a future assignment, we will install and use a more realistic version of RSA.

Setup

1. This is a paired activity. Grab a partner and work together!
2. Both you and your partner visit the website: <https://www.javainuse.com/rsagenerator>
(Note: if the website is down, use the backup site: <https://www.codeusingjava.com/tools/rsa>)
3. You and your partner will need a way to copy and paste data back and forth (e.g., Zoom, Slack, email).

1. Key Generation

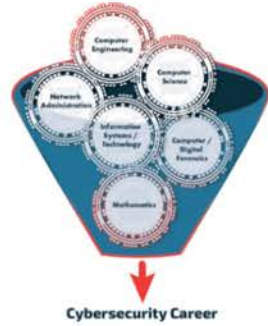
You and your partner will each generate your RSA public and private keys: click **Generate Keys**.

RSA Generate Keys

This tool generates RSA public key as well as the private key of sizes - 512 bit, 1024 bit, 2048 bit, 3072 bit and 4096 bit with Base64 encoded. The generated private key is generated in PKCS#8 format and the generated public key is generated in X.509 format.

RING Modules

RING Modules



[Unit 0: Introduction](#)

[Content List](#)



[Unit 1: Ethics](#)

[Content List](#)



[Unit 2: Establishing Trust](#)

[Content List](#)



[Unit 3: Ubiquitous
Connectivity](#)

[Content List](#)



[Unit 4: Data Security](#)

[Content List](#)



[Unit 5: Introduction to Python
Programming](#)

[Content List](#)



[Unit 6: System Security](#)

[Content List](#)



[Unit 7: Adversarial Thinking](#)

[Content List](#)



[Unit 8: Risk](#)

[Content List](#)



[Unit 9: Implications](#)

[Content List](#)

Unit 2 - Establishing Trust - Content List

Slide Deck	Lesson Plans	Graphic Organizers & Viewing Guides	Activities & Labs	Reviews & Resources	Assessments
Instructional Slides (Teacher) ➞	Lesson Plans ➞	Classify the CIA Triad Graphic Organizer (Student) ➞	Caesar Cipher Activity (Student) ➞	Unit 2.1 Quizlet ➞	Mid Unit 2 Assessment ➞
Instructional Slides (Student) ➞		Classify the CIA Triad Graphic Organizer (Teacher) ➞	Caesar Cipher Activity (Teacher) ➞	Unit 2.1 Kahoot ➞	Final Unit 2 Assessment ➞
		Cybersecurity Principles Examples Graphic Organizer (Student) ➞	Changing Privilege Activity (Student) ➞	Caesar Cipher Demo ➞	
		Cybersecurity Principles Examples Graphic Organizer (Teacher) ➞	Changing Privilege Activity (Teacher) ➞	Steganography Online Tool ➞	Unit 2 Study Guides ➞
		Inside a Computer Graphic Organizer (Student) ➞	Hiding Files Activity (Student) ➞	Unit 2.2 Quizlet ➞	
		Inside a Computer Graphic Organizer (Teacher) ➞	Hiding Files Activity (Teacher) ➞	Unit 2.2 Kahoot ➞	
		Pick Your Access Control Graphic Organizer (Student) ➞	Linux Commands Activity (Student) ➞	Cybersecurity First Principles Explained (1) ➞	
		Pick Your Access Control Graphic Organizer (Teacher) ➞	Linux Commands Activity (Teacher) ➞	Cybersecurity First Principles Explained (2) ➞	
		Vocabulary Practice 2.2 Graphic Organizer (Student) ➞	McCumber Cube Challenge E-mate ➞	Fort Knox and Its Security ➞	

Unit 2 - Establishing Trust - Daily Guide

Day 1

 [Graphic Organizer: Vocabulary Practice 2.1 \(Student\)](#) 

 [Graphic Organizer: Vocabulary Practice 2.1 \(Teacher\)](#) 

 [Viewing Guide: "What is the C.I.A. Triad?" \(Student\)](#) 

 [Viewing Guide: "What is the C.I.A. Triad?" \(Teacher\)](#) 

 [Extension Activity: \(E-mate\) McCumber Cube](#) 

 [Extension Activity: \(E-mate\) McCumber Cube Challenge](#) 

 [Extension Activity: Build a Scytale \(Physical\) \(Cryptool.org Site\)](#) 

 [Extension Activity: Scytale \(YouTube\)](#) 

Day 2

 [Activity: Caesar Cipher \(Student\)](#) 

 [Activity: Caesar Cipher \(Teacher\)](#) 

 [Extension Activity: \(E-mate\) Cryptography](#) 

Unit 2 - Caesar Cypher

Caesar Cipher

Objective: I can practice confidentiality using the Caesar cipher.

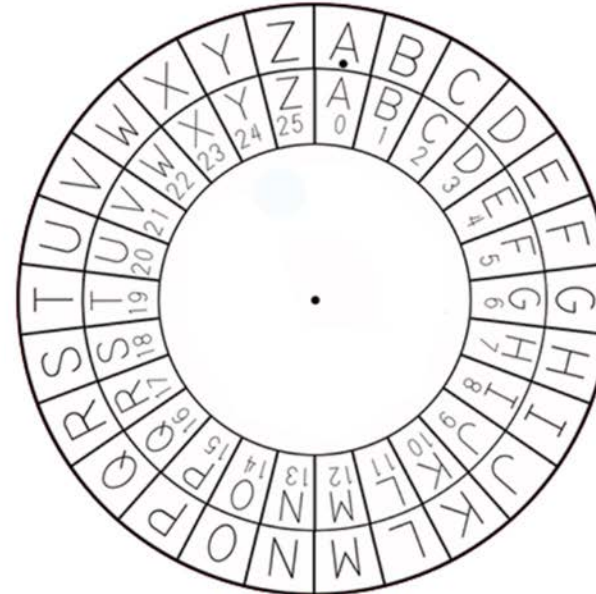
Overview

The Caesar cipher is an early form of cryptography. It is a foundational cipher performed by placing one alphabet on top of another in a circle, then shifting the top alphabet by three spaces to the right.

Setup

1. Visit the InventWithPython website link to use a visual Caesar cipher wheel too.

<http://inventwithpython.com/cipherwheel/>

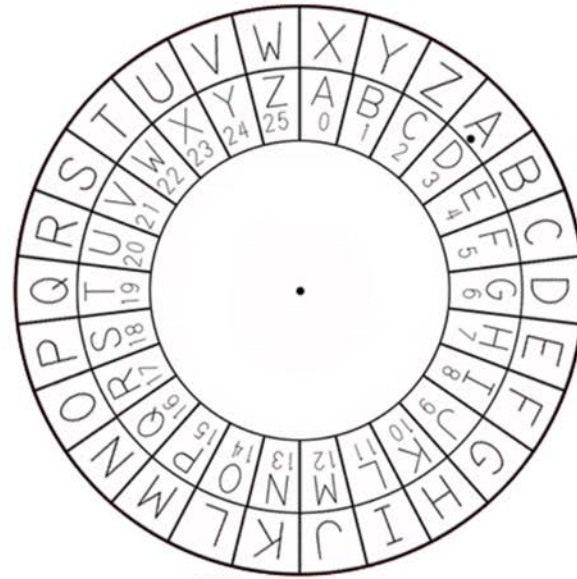


Click wheel to rotate.

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
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Click the wheel, then move your mouse. The outer ring of the cipher wheel will begin rotating. To achieve the Caesar cipher, you must rotate the top wheel three spaces to the right. 'A' should now be on top of 'D.' Note the 'A' has a period under it -- this allows you to see your shift number. When 'A' is over 'D,' the number 3 indicates the shift. Your wheel should look like the one below.

Unit 2 - Caesar Cypher



Click wheel to rotate.

X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher

First, let's decrypt a simple message: **ULQJ**

To decrypt:

1. Look at the message letter-by-letter
2. Find the letter on the inner ring
3. Change it to the outer ring letter it is touching

For this example:

U -> R

L -> I

Q -> N

J -> G

So, the message is: **RING**

Unit 2 - Caesar Cypher

1. Decrypt the following message: **FDHVDU**

CAESAR

2. Decrypt the following message: **FRQILGHQWLDOLWB**

CONFIDENTIALITY

Shifting Things Up

The Caesar cipher uses the shift of three, but any shift is possible to create a new kind of secret message.

Change your cipher wheel to a **shift of 13** to solve the following problems.

3. Decrypt the following message: **FPLGNYR**

SCYTALE

4. Decrypt the following message: **GEHFG**

TRUST

Brute Force

For this final activity, you have to figure out the shift value. **It will not be told to you.** You can accomplish this through the brute force method by testing every possible shift value. However, there is a trick that will save you some time. This encrypted message is multiple words.

5. Decrypt the following message: **V NZ PYRIRE**

If you figure out the trick, explain how you did it.

I AM CLEVER The trick is that there are only two one-letter words in English: A or I. Clever students will notice this, align 'V' with 'A' or 'I' on the cipher wheel, and find the answer within two tries.

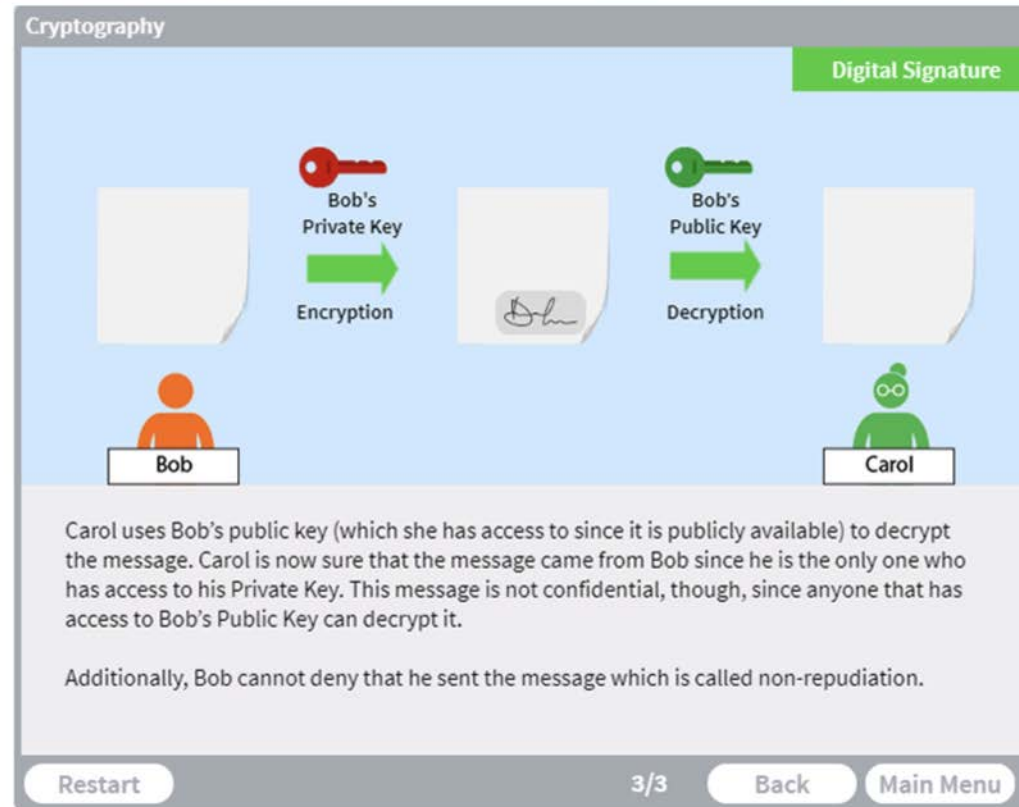
6. You have practiced decryption in this activity. How would you encrypt a message using the Caesar cipher? If time permits, encrypt a message to share with a friend.

When encrypting a message, the process is very similar. The difference is that you transform the outside ring letter into the inside ring letter.

E-Mates from CSSIA - myEmates.org

Cryptography

Home / Cybersecurity / Cryptography



Instructing RING

RING instruction is carried out nationwide within three categories.



RING in Hawaii - Entry level College Course

- University of Hawaii Maui College -
 - Educational Pathway Institution (EPI)
 - Working under the Educational Pathway National Center (EPNC) - Moraine Valley CC
- Online College Course that now covers RING
 - ICS 169 - Introduction to Information Security
 - Available to high school students under Early College
 - First college course in a cybersecurity certificate

RING in Hawaii - Public High Schools

- Training for high school teachers in Hawaii
 - Cyber Summit - hosted by EPNC, UHMC and HI DoE
 - March 1, 2023 - Presentation to HI DoE leadership
 - Half day workshop on RING by team from UAH
 - Intensive training in RING - Summer 2023
 - Two days, online training, June 12-13, 2024
 - First two days of GenCyber camp covered RING
 - Follow up with high school teachers in SY 2023-24
- Repeat summer training in 2024 for 30 additional teachers!
- Expect Hawaii schools to start teaching RING starting Fall 2024
 - Netlabs to be initially hosted at Moraine Valley CC

RING is start
of existing
cyber
pathway!

Certificate of Competence (CO) in Information Security (12 credits):

(All courses are taught completely online via the WWW)

- **ICS 101** – Digital Tools for an Information World (3 credits)...introduction to digital technology.
- **ICS 169** – Introduction to Information Security (3 credits)...covers 10 core areas of **ISC2**
- **ICS 184** – Introduction to Networking (3 credits)...covers CompTIA **Network+**
- **ICS 171** – Introduction to Computer Security (3 credits)...covers CompTIA **Security+**

Certificate of Achievement (CA) in Information Security (24 credits):

(All 4 courses required in the above Certificate of Competence, plus 4 below)

- **ICS 281** – Ethical Hacking (3 credits)...covers EC-Council **CEH**
- **ICS 282** – Digital Forensics (3 credits)...covers EC-Council **CHFI**
- **ENG 100 (or higher)** – English Composition I (3 credits)
- **MATH 103 (or higher)** – College Algebra (3 credits)



UNIVERSITY of HAWAII®
MAUI COLLEGE

Questions?
Comments?!



Debasis
Bhattacharya

debasisb@hawaii.edu

maui.hawaii.edu/cybersecurity