# Roadmaps for Cybersecurity Concept Lessons

Computer Science Principles

Cybersecurity Concept Lessons

| Creative Development (CRD) | DATA (DAT) | Algorithms and Programming (AAP) | Computing Systems and Networks (CSN) | Impact of Computing (IOC) |
|---|---|---|---|---|
| Input Validation & Conditionals | CIA Triad | Networking | CIA Triad | CIA Triad |
| Iterative Process | Personal Data Vulnerabilities | Input Validation & Conditionals | Networking | Personal Data Vulnerabilities |
| Data Structures | Steganography | Iterative Process | Risk | Identity Authentication Authorization |
| Caesar Cipher | Cybersecurity Ethics | Data Structures | Cybersecurity Ethics | Risk |
| Vigenère Cipher | | Caesar Cipher | | Networking |
| Symmetric and Public Key Cryptography | | Vigenère Cipher | | Symmetric and Public Key Cryptography |
| Steganography | | Symmetric and Public Key Cryptography | | Cybersecurity Ethics |
| Cybersecurity Ethics | | Steganography | | |
| | | Cybersecurity Ethics | | |

Community Colleges Catalyzing Computing and Cybersecurity

Based on 2020-21 Framework

Computer Science Principles

Creative Development CRD

Algorithms and Programming AAP

Impact of Computing IOC

## Caesar Cipher

Explain how computing innovations are improved through collaboration. (LO CRD-1.A)

Demonstrate effective interpersonal skills during collaboration. (LO CRD-1.C)

Explain how a program or code segment functions. (LO CRD-2.B)

For errors in an algorithm or program:
a. Identify the error.
b. Correct the error. (LO CRD-2.I)

Represent a value with a variable. (LO AAP-1.A)

Represent a list or string using a variable. (LO AAP-1.C)

Evaluate expressions that use arithmetic operators. (LO AAP-2.C)

Evaluate expressions that manipulate strings. (LO AAP-2.D)

# Cybersecurity Concept Lesson: Caesar Cipher

**Students will: 1) investigate how Caesar Ciphers work to achieve the goal of confidentiality of information, their historical context, and strengths and weaknesses, 2) encrypt and decrypt text using Caesar Ciphers, 3) implement a Caesar Cipher in a programming language, and 4) ascertain the correctness of their program as a functional program to protect information assets and computing resources.**

**Prerequisite Knowledge: Students will need to be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. This CCL assumes that students have been introduced to the general topics of cybersecurity and cryptography.**

**Length of Completion: 2 to 3 class periods (based on 50 minutes)**

CRD-1.A.3 Effective collaboration produces a computing innovation that reflects the diversity of talents and perspectives of those who designed it.

CRD-1.C.1 Effective collaborative teams practice interpersonal skills, including but not limited to: communication, consensus building, conflict resolution, and negotiation.

CRD-2.B.1 A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.I.1 A logic error is a mistake in the algorithm or program that causes it to behave incorrectly or unexpectedly.

CRD-2.I.2 A syntax error is a mistake in the program where the rules of the programming language are not followed.

CRD-2.I.3 A run-time error is a mistake in the program that occurs during the execution of a program. Programming languages define their own run-time errors.

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP-1.A.3 Some programming languages provide types to represent data, which are referenced using variables. These types include numbers, Booleans, lists, and strings.

AAP-1.A.4 Some values are better suited to representation using one type of data rather than another.

AAP-1.C.1 A list is an ordered sequence of elements. For example, [value1, value2, value3, . . .] describes a list where value1 is the first element, value2 is the second element, value3 is the third element, and so on.

AAP-1.C.3 An index is a common method for referencing the elements in a list or string using natural numbers.

AAP-1.C.4 A string is an ordered sequence of characters.

AAP-2.A.1 An algorithm is a finite set of instructions that accomplish a specific task.

AAP-2.A.3 Algorithms executed by programs are implemented using programming languages.

AAP-2.C.1 Arithmetic operators are part of most programming languages and include addition, subtraction, multiplication, division, and modulus operators.

AAP-2.C.2 The exam reference sheet provides a MOD b, which evaluates to the remainder when a is divided by b. Assume that a is an integer greater than or equal to 0 and b is an integer greater than 0. For example, 17 MOD 5 evaluates to 2.

AAP-2.D.1 String concatenation joins together two or more strings end-to-end to make a new string.

Computer Science Principles

Creative Development CRD

Algorithms and Programming AAP

Impact of Computing IOC

## Caesar Cipher

Express an algorithm that uses selection without using a programming language. (LO AAP-2.G)

For selection:
a. Write conditional statements.
b. Determine the result of conditional statements. (LO AAP-2.H)

For iteration:
a. Write iteration statements.
b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

For algorithms:
a. Create algorithms.
b. Combine and modify existing algorithms. (LO AAP-2.M)

For list operations:
a. Write expressions that use list indexing and list procedures.
b. Evaluate expressions that use list indexing and list procedures. (LO AAP-2.N)

For algorithms involving elements of a list:
a. Write iteration statements to traverse a list.
b. Determine the result of an algorithm that includes list traversals. (LO AAP-2.O)

For procedure calls:
a. Write statements to call procedures.
b. Determine the result or effect of a procedure call. (LO AAP-3.A)

Explain how the use of procedural abstraction manages complexity in a program. (LO AAP-3.B)

For generating random values:
a. Write expressions to generate possible values.
b. Evaluate expressions to determine the possible results (LO AAP-3.E)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Caesar Cipher

Students will: 1) investigate how Caesar Ciphers work to achieve the goal of confidentiality of information, their historical context, and strengths and weaknesses, 2) encrypt and decrypt text using Caesar Ciphers, 3) implement a Caesar Cipher in a programming language, and 4) ascertain the correctness of their program as a functional program to protect information assets and computing resources.

Prerequisite Knowledge: Students will need to be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. This CCL assumes that students have been introduced to the general topics of cybersecurity and cryptography.

Length of Completion: 2 to 3 class periods (based on 50 minutes)

AAP-2.G.1 Selection determines which parts of an algorithm are executed based on a condition being true or false

AAP-2.H.1 Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP-2.K.1 Iteration statements change the sequential flow of control by repeating a set of statements zero or more times, until a stopping condition is met.

AAP-2.M.1 Algorithms can be created from an idea, by combining existing algorithms, or by modifying existing algorithms.

AAP-2.N.1 The exam reference sheet provides basic operations on lists, including: accessing an element by index, assigning a value of an element of a list to a variable, assigning a value to an element of a list, inserting elements at a given index, adding elements to the end of the list, removing elements, and determining the length of a list.

AAP-2.O.1 Traversing a list can be a complete traversal, where all elements in the list are accessed, or a partial traversal, where only a portion of elements are accessed.

AAP-2.O.2 Iteration statements can be used to traverse a list.

AAP-3.A.1 A procedure is a named group of programming instructions that may have parameters and return values.

AAP-3.A.2 Procedures are referred to by different names, such as method or function, depending on the programming language.

AAP-3.A.3 Parameters are input variables of a procedure. Arguments specify the values of the parameters when a procedure is called.

AAP-3.A.4 A procedure call interrupts the sequential execution of statements, causing the program to execute the statements within the procedure before continuing. Once the last statement in the procedure (or a return statement) has executed, flow of control is returned to the point immediately following where the procedure was called.

AAP-3.B.1 One common type of abstraction is procedural abstraction, which provides a name for a process and allows a procedure to be used only knowing what it does, not how it does it.

AAP-3.B.2 Procedural abstraction allows a solution to a large problem to be based on the solution of smaller subproblems. This is accomplished by creating procedures to solve each of the subproblems.

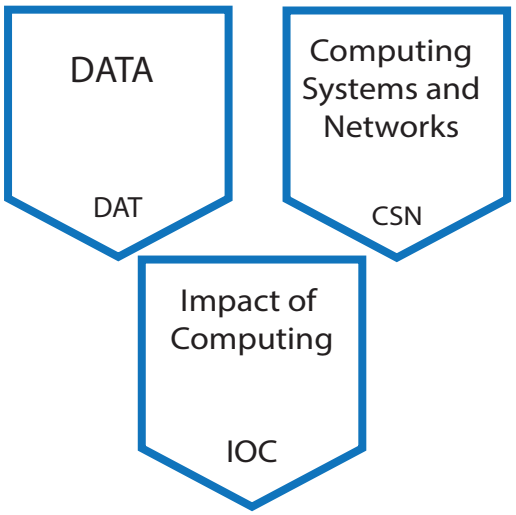
AAP-3.B.5 Using parameters allows procedures to be generalized, enabling the procedures to be reused with a range of input values or arguments.

AAP-3.E.1 The exam reference sheet provides RANDOM(a, b) which generates and returns a random integer from a to b, inclusive. Each result is equally likely to occur. For example, RANDOM(1, 3) could return 1, 2, or 3.

AAP-3.E.2 Using random number generation in a program means each execution may produce a different result.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Computer Science Principles




**CIA Triad**

Explain how data can be represented using bits. (LO DAT-1.A)

Explain how computing devices work together in a network. (LO CSN-1.A)

Describe the differences between the Internet and the World Wide Web. (LO CSN-1.D)

Describe the risks to privacy from collecting and storing personal data on a computer system. (LO IOC-2.A)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: CIA Triad

Students will: 1) explain con¬fidentiality, integrity, and availability (CIA Triad) as the foundation of information security, 2) explore how email phishing attacks, fake social media accounts, ransomware, and identity theft can violate the cybersecurity goals of confidentiality, integrity and availability, and 3) describe security controls that can be used to protect computing resources.

Prerequisite Knowledge: Students should have a basic understanding of how the Internet works.

Length of Completion: 2 to 3 class periods (based on 50 minutes)

DAT-1.A.5 Abstraction is the process of reducing complexity by focusing on the main idea. By hiding details irrelevant to the question at hand and bringing together related and useful details, abstraction reduces complexity and allows one to focus on the idea.

CSN-1.A.3 A computer network is a group of interconnected computing devices capable of sending or receiving data.

CSN-1.D.1 The World Wide Web is a system of linked pages, programs, and files.

IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.

IOC-2.A.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Computer Science Principles

Creative Development

CRD

Impact of Computing

IOC

**Cybersecurity Ethics**

Explain how computing innovations are improved through collaboration. (LO CRD-1.A)

Describe the purpose of a computing innovation. (LO CRD-2.A)

Identify input(s) to a program. (LO CRD-2.C)

Identify output(s) produced by a program. (LO CRD-2.D)

Explain how an effect of a computing innovation can be both beneficial and harmful. (LO IOC-1.A)

Explain how a computing innovation can have an impact beyond its intended purpose. (LO IOC-1.B)

Explain how the use of computing could raise legal and ethical concerns. (LO IOC-1.F)

# Cybersecurity Concept Lesson: Cybersecurity Ethics

*Overview: Students will: 1) explain how ease of access and malleability of computing resources are beneficial aspects of computing, these properties raise important legal and ethical concerns, and 2) articulate concepts of right and wrong conduct with regard to important ethical concerns such as bias, surveillance, ownership, and digital divide.*

*Prerequisite Knowledge: Students should complete one of the CCL pathways found in the roadmap. The roadmaps are a list of CCLs which address each of the five Big Ideas in the Advanced Placement Computer Science Principles framework.*

*This Cybersecurity-Centered Lesson (CCL) is a possible capstone activity which engages students to reflect on the ethical decision-making process behind cybersecurity issues.*

*Length of Completion: 4 or 5 class periods (based on 50 minutes)*

CRD-1.A.1 A computing innovation includes a program as an integral part of its function.

CRD-2.A.1 The purpose of computing innovations is to solve problems or to pursue interests through creative expression.

CRD-2.A.2 An understanding of the purpose of a computing innovation provides developers with an improved ability to develop that computing innovation.

CRD-2.C.6 Input can come from a user or other programs.

CRD-2.D.2 Program output is usually based on a program's input or prior state (e.g., internal values).

IOC-1.A.2 As computing evolves, the way people complete tasks often changes to incorporate new computing innovations.

IOC-1.A.3: The total effects of a computing innovation are not always anticipated in advance.

IOC-1.A.4: A single effect can be viewed as both beneficial and harmful based on an individual's perspectives.

IOC-1.B.1: Computing innovations can be used in ways that the creator had not originally intended.

IOC-1.B.2: Some of the unintended ways computing innovations can be used may have a harmful impact on society, economy, or culture

IOC-1.B.3: Responsible programmers try to consider the unintended ways their computing innovations can be used and the potential beneficial and harmful effects of these new uses.

IOC-1.B.6: Rapid sharing of the program or the results of running a program with a large number of users can result in significant impacts beyond the intended purpose or control of the programmer.

IOC-1.F.1: Material created on a computer is the intellectual property of the creator or an organization.

IOC-1.F.2: Ease of access and distribution of digitized information raises intellectual property concerns regarding ownership, value, and use.

IOC-1.F.3: Measures should be taken to safeguard intellectual property.

IOC-1.F.8: Using computing to harm individuals or groups of people raise legal and ethical concerns.

Computer Science Principles

Creative Development

CRD

Impact of Computing

IOC

**Cybersecurity Ethics**

Explain how the use of computing could raise legal and ethical concerns. (LO IOC-1.F)

Describe the risks to privacy from collecting and storing personal data on a computer system. (LO IOC-2.A)

Explain how computing resources can be protected and can be misused. (LO IOC-2.B)

# Cybersecurity Concept Lesson: Cybersecurity Ethics

*Overview: Students will: 1) explain how ease of access and malleability of computing resources are beneficial aspects of computing, these properties raise important legal and ethical concerns, and 2) articulate concepts of right and wrong conduct with regard to important ethical concerns such as bias, surveillance, ownership, and digital divide.*

*Prerequisite Knowledge: Students should complete one of the CCL pathways found in the roadmap. The roadmaps are a list of CCLs which address each of the five Big Ideas in the Advanced Placement Computer Science Principles framework.*

*This Cybersecurity-Centered Lesson (CCL) is a possible capstone activity which engages students to reflect on the ethical decision-making process behind cybersecurity issues.*

*Length of Completion: 4 or 5 class periods (based on 50 minutes)*

IOC-1.F.9: Computing can play a role in social and political issues which in turn often raise legal and ethical concerns.

IOC-1.F.11: Computing innovations can raise legal and ethical concerns.

IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.

IOC-2.A.2 Search engines can record and maintain a history of searches made by users.

IOC-2.A.3 Websites can record and maintain a history of individuals who have viewed their pages.

IOC-2.A.4 Devices, websites, and networks can collect information about a user's location.

IOC-2.A.5 Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.

IOC-2.A.6 Search engines can use search history to suggest websites or for targeted marketing.

IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.

IOC-2.A.10 Commercial and governmental curation of information may be exploited if privacy and other protections are ignored.

IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.

IOC-2.A.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

IOC-2.A.13: It is difficult to delete information once it has been placed online.

IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.

IOC 2.B.5: Encryption is the process of encoding data to prevent unauthorized access to information. Decryption is the process of decoding the data.

Computer Science Principles

Creative Development

CRD

Impact of Computing

IOC

**Cybersecurity Ethics**

IOC-2.B Explain how computing resources can be protected and can be misused. (LO IOC-2.B)

IOC-2.C Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Cybersecurity Ethics

*Overview: Students will: 1) explain how ease of access and malleability of computing resources are beneficial aspects of computing, these properties raise important legal and ethical concerns, and 2) articulate concepts of right and wrong conduct with regard to important ethical concerns such as bias, surveillance, ownership, and digital divide.*

*Prerequisite Knowledge: Students should complete one of the CCL pathways found in the roadmap. The roadmaps are a list of CCLs which address each of the five Big Ideas in the Advanced Placement Computer Science Principles framework.*

*This Cybersecurity-Centered Lesson (CCL) is a possible capstone activity which engages students to reflect on the ethical decision-making process behind cybersecurity issues.*

*Length of Completion: 4 or 5 class periods (based on 50 minutes)*

*IOC-2.B.6 Certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.*

*IOC-2.B.7 Computer virus and malware scanning software can help protect a computing system against infection.*

*IOC-2.B.8 A computer virus is a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.*

*IOC-2.B.9 Malware is software intended to damage a computing system or to take partial control over its operation.*

*IOC-2.B.10 All real-world systems have errors or design flaws that can be exploited to compromise them. Regular software updates help fix errors that could compromise a computing system.*

*IOC-2.B.11 Users can control the permissions programs have for collecting user information. Users should review the permission settings of programs to protect their privacy.*

*IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.*

*IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.*

*IOC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.*

*IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.*

*IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.*

*IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.*

*IOC-2.C.7 Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.*

Computer Science Principles

Creative Development

CRD

Algorithms and Programming

AAP

## Data Structures

Student will be able to identify how a segment of program code functions. (LO CRD-2.B)

Students will be able to identify inputs in a program. (LO CRD-2.C)

Students will be able to identify outputs in a program. (LO CRD-2.D)

Identify inputs and corresponding expected outputs or behaviors that can be used to check the correctness of an algorithm or program. (LO CRD-2.J)

Students will be able to represent a value with a variable. (LO AAP-1.A)

Determine the value of a variable as a result of an assignment. (LO AAP-1.B)

Students will be able to represent a string using a variable. (LO AAP-1.C)

# Cybersecurity Concept Lesson: Data Structures

Students will: 1) develop a program to validate input, 2) test whether inputs to a program are producing the expected output, and 3) represent data in various types, including numbers, strings, lists, and Booleans.

Prerequisite Knowledge: Students should be familiar with strings, Booleans, user input, variables and conditionals.

Length of Completion: 3 to 5 class periods (based on 50 minutes)

CRD-2.B.1A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.B.2 A code segment refers to a collection of program statements that are part of a program.

CRD-2.B.3 A program needs to work for a variety of inputs and situations.

CRD-2.B.4 The behavior of a program is how a program functions during execution and is often described by how a user interacts with it.

CRD-2.C.1 Program input is data sent to a computer for processing by a program. Input can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.C.4 Inputs usually affect the output produced by a program.

CRD-2.C.6 Input can come from a user or other programs.

CRD-2.D.1Program output is any data sent from a program to a device. Program output can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.D.2 Program output is usually based on a program's input or prior state (e.g., internal values).

CRD-2.J.1In the development process, testing uses defined inputs to ensure that an algorithm or program is producing the expected outcomes. Programmers use the results from testing to revise their algorithms or programs.

CRD 2.J.2: Defined inputs used to test a program should demonstrate the different expected outcomes that are at or just beyond the extremes (minimum and maximum) of input data.

AAP-1.A.1A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP 1.A.3: Some programming languages provide types to represent data, which are referenced using variables. These types include: numbers, Booleans, lists, and strings.

AAP 1.B.1: The assignment operator allows a program to change the value represented by a variable.

AAP 1.B.3: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 1.C.4: A string is an ordered sequence of characters.



Based on 2020-21 Framework

Computer Science Principles

Creative Development

CRD

Algorithms and Programming

AAP

## Data Structures

For relationships between two variables, expressions, or values:
a. Write expressions using relational operators.
b. Evaluate expressions that use relational operators. (LO AAP-2.E)

Students will be able to write and evaluate conditional statements. (LO AAP-2.H)

For iteration:
a. Write iteration statements.
b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

For list operations:
a. Write expressions that use list indexing and list procedures.
b. Evaluate expressions that use list indexing and list procedures. (LO AAP-2.N)

For algorithms involving elements of a list:
a. Represent using iterative statements to traverse a list.
b. Determine the result of an algorithm with list traversals. (LO AAP-2.O)

# Cybersecurity Concept Lesson: Data Structures

Students will: 1) develop a program to validate input, 2) test whether inputs to a program are producing the expected output, and 3) represent data in various types, including numbers, strings, lists, and Booleans.

Prerequisite Knowledge: Students should be familiar with strings, Booleans, user input, variables and conditionals.

Length of Completion: 3 to 5 class periods (based on 50 minutes)

AAP 2.E.1: A Boolean value is either true or false.

AAP 2.H.1: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 2.K.1: Iteration statements change the sequential flow of control by repeating a set of statements zero or more times until a stopping condition is met.

AAP 2.H.1: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 2.K.1: Iteration statements change the sequential flow of control by repeating a set of statements zero or more times until a stopping condition is met.

AAP 2.N.1: The exam reference sheet provides basic operations on lists, including: a) Accessing an element by index, b) Assigning a value of an element of a list to a variable, c) Assigning a value to an element of a list, d) Inserting elements at a given index, e)Adding elements to the end of the list, f) Removing elements, g) Determining the length of the list

AAP 2.N.2: List procedures are implemented in accordance with the syntax rules of the language.

AAP 2.0.1: Traversing a list can be a complete traversal where all elements in the list are accessed, or a partial traversal where only a portion of elements are accessed.



Based on 2020-21 Framework

Computer Science Principles

Impact of Computing

IOC

# Cybersecurity Concept Lesson: Identity, Authentication, and Authorization

Students will: 1) explain concepts of identity, authentication, and authorization, 2) describe ways in which attackers gain unauthorized access to systems and data, and 3) identify aspects of for passwords, multifactor authentication, and the concept of least privilege as security controls for protecting information assets and computing resources.

Prerequisite Knowledge: Students should be familiar with phishing and the concepts of confidentiality, integrity, availability (CIA Triad).

Length of Completion: 2 to 3 class periods (based on 50 minutes)

## Identity, Authentication, and Authorization

Explain how computing resources can be protected and can be misused. (LO IOC-2.B)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

IOC-2.B.1 Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.

IOC-2.B.2 A strong password is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.

IOC-2.B.3 Multifactor authentication is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge, possession, and inheritance.

IOC-2.B.4 Multifactor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.

IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.

IOC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.

IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.

IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.

IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.

Computer Science Principles

Creative Development

CRD

Algorithms and Programming

AAP

## Input Validation & Conditionals

Students will be able to identify how a segment of program code functions. (LO CRD-2.B)

Students will be able to identify inputs in a program. (LO CRD-2.C)

Students will be able to identify outputs in a program. (LO CRD-2.D)

Identify inputs and corresponding expected outputs or behaviors that can be used to check the correctness of an algorithm or program. (LO CRD-2.J)

Students will be able to represent a value with a variable. (LO AAP-1.A)

Determine the value of a variable as a result of an assignment. (LO AAP-1.B)

Students will be able to represent a string using a variable. (LO AAP-1.C)

For relationships between two variables, expressions, or values: a. Write expressions using relational operators. b. Evaluate expressions that use relational operators. (LO AAP-2.E)

Students will be able to write and evaluate conditional statements. (LO AAP-2.H)

# Cybersecurity Concept Lesson: Input Validation & Conditionals

*Overview: Students will: 1) develop a program to validate passwords, and more specifically, 2) identify how a segment of program code functions, 3) identify inputs and outputs in a program, 4) represent a value with a variable, 5) represent a string using a variable, and 6) write and evaluate conditional statements.*

*Prerequisite Knowledge: Students should be familiar with strings, booleans, user input and variables.*

*Length of Completion: 2 or 3 class periods (based on 50 minutes)*

CRD-2.B.1 A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.B.2 A code segment refers to a collection of program statements that are part of a program.

CRD-2.B.3 A program needs to work for a variety of inputs and situations.

CRD-2.B.4 The behavior of a program is how a program functions during execution and is often described by how a user interacts with it.

CRD-2.C.1 Program input is data sent to a computer for processing by a program. Input can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.C.4 Inputs usually affect the output produced by a program.

CRD-2.C.6 Input can come from a user or other programs.

CRD-2.D.1 Program output is any data sent from a program to a device. Program output can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.D.2 Program output is usually based on a program's input or prior state (e.g., internal values).

CRD-2.J.1 In the development process, testing uses defined inputs to ensure that an algorithm or program is producing the expected outcomes. Programmers use the results from testing to revise their algorithms or programs.

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP 1.A.3: Some programming languages provide types to represent data, which are referenced using variables. These types include: numbers, Booleans, lists, and strings.

AAP 1.B.1: The assignment operator allows a program to change the value represented by a variable.

AAP 1.B.3: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 1.C.4: A string is an ordered sequence of characters.

AAP 2.E.1: A Boolean value is either true or false.

AAP 2.H.1: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

Community Colleges Catalyzing Computing and Cybersecurity

Based on 2020-21 Framework

Computer Science Principles

Creative Development

CRD

Algorithms and Programming

AAP

## The Iterative Process

Student will be able to identify how a segment of program code functions. (LO CRD-2.B)

Students will be able to identify inputs in a program. (LO CRD-2.C)

Students will be able to identify outputs in a program. (LO CRD-2.D)

Identify inputs and corresponding expected outputs or behaviors that can be used to check the correctness of an algorithm or program. (LO CRD-2.J)

Students will be able to represent a value with a variable. (LO AAP-1.A)

Determine the value of a variable as a result of an assignment. (LO AAP-1.B)

Students will be able to represent a string using a variable. (LO AAP-1.C)

For relationships between two variables, expressions, or values: a. Write expressions using relational operators. b. Evaluate expressions that use relational operators. (LO AAP-2.E)

Students will be able to write and evaluate conditional statements. (LO AAP-2.H)

For iteration: a. Write iteration statements. b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

# Cybersecurity Concept Lesson: The Iterative Process

*Overview: Students will: 1) develop a program to validate passwords, and more specifically, 2) validate the length of the password, 3) validate uppercase characters, and 4) validate a numeric character.*

*Prerequisite Knowledge: Students should be familiar with strings, booleans, user input, variables and conditionals.*

*Length of Completion: 3 to 5 class periods (based on 50 minutes)*

CRD-2.B.1 A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.B.2 A code segment refers to a collection of program statements that are part of a program.

CRD-2.B.3 A program needs to work for a variety of inputs and situations.

CRD-2.B.4 The behavior of a program is how a program functions during execution and is often described by how a user interacts with it.

CRD-2.C.1 Program input is data sent to a computer for processing by a program. Input can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.C.4 Inputs usually affect the output produced by a program.

CRD-2.C.6 Input can come from a user or other programs.

CRD-2.D.1 Program output is any data sent from a program to a device. Program output can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.D.2 Program output is usually based on a program's input or prior state (e.g., internal values).

CRD-2.J.1 In the development process, testing uses defined inputs to ensure that an algorithm or program is producing the expected outcomes. Programmers use the results from testing to revise their algorithms or programs.

CRD 2.J.2: Defined inputs used to test a program should demonstrate the different expected outcomes that are at or just beyond the extremes (minimum and maximum) of input data.

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP 1.A.3: Some programming languages provide types to represent data, which are referenced using variables. These types include: numbers, Booleans, lists, and strings.

AAP 1.B.1: The assignment operator allows a program to change the value represented by a variable.

AAP 1.B.3: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 1.C.4: A string is an ordered sequence of characters.

AAP 2.E.1: A Boolean value is either true or false.

AAP 2.H.1: Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP 2.K.1: Iteration statements change the sequential flow of control by repeating a set of statements zero or more times until a stopping condition is met.

Community Colleges Catalyzing Computing and Cybersecurity

Based on 2020-21 Framework

Computer Science Principles

Algorithms and Programming

AAP

Computing Systems and Networks

CSN

**Networking**

For determining the efficiency of an algorithm:
a. Explain the difference between algorithms that run in reasonable time and those that do not.
b. Identify situations where a heuristic solution may be more appropriate. (LO AAP-4.A)

Explain how computing devices work together in a network. (LO CSN-1.A)

For fault-tolerant systems, like the Internet:
a. Describe the benefits of fault tolerance.
b. Explain how a given system is fault-tolerant.
c. Identify vulnerabilities to failure in a system. (LO CSN-1.E)

# Cybersecurity Concept Lesson: Networking

*Overview: Students will: 1) explain that the Internet is a network of networks, 2) identify the OSI network layers and their functions, 3) recognize common network attacks, i.e., how networks can be misused, and specifically identify what layers of the OSI Model are attacked, and 4) investigate what attackers might be gaining and potential consequences of such misuse, ie., who can it affect and how.*

*Prerequisite Knowledge: It is suggested that students complete CCL 1: Personal Data Vulnerabilities.*

*Length of Completion: 5 class periods (based on 50 minutes)*

*AAP-4.A.2 A decision problem is a problem with a yes/no answer (e.g., is there a path from A to B?). An optimization problem is a problem with the goal of finding the "best" solution among many (e.g., what is the shortest path from A to B?).*

*CSN-1.A.3 A computer network is a group of interconnected computing devices capable of sending or receiving data.*

*CSN-1.A.4 A computer network is a type of a computing system.*

*CSN-1.A.5 A path between two computing devices on a computer network (a sender and a receiver) is a sequence of directly connected computing devices that begins at the sender and ends at the receiver.*

*CSN-1.A.6 Routing is the process of finding a path from sender to receiver.*

*CSN-1.E.3 One way to accomplish network redundancy is by having more than one path between any two connected devices.*

Computer Science Principles

DATA

DAT

Impact of Computing

IOC

# Cybersecurity Concept Lesson: Personal Data Vulnerabilities

*Overview: Students will: 1) describe what information can be extracted from data and metadata, 2) explain how the information may be susceptible to attack by an adversary, and 3) describe consequent risks to privacy from collecting and storing personal data on a computer system.*

*Prerequisite Knowledge: Students should have basic knowledge of how to use a web browser and how to access the pictures on their mobile phone.*

*Length of Completion: 2 to 3 class periods (based on 50 minutes)*

## Personal Data Vulnerabilities

Describe what information can be extracted from data. (LO DAT-2.A)

Describe what information can be extracted from metadata. (LO DAT-2.B)

Extract information from data using a program. (LO DAT-2.D)

Describe the risks to privacy from collecting and storing personal data on a computer system. (LO IOC-2.A)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

DAT-2.A.1: Information is the collection of facts and patterns extracted from data.

DAT-2.A.2: Data provide opportunities for identifying trends, making connections, and addressing problems.

DAT-2.A.3: Digitally processed data may show correlation between variables. A correlation found in data does not necessarily imply a causal relationship exists. Often additional research is needed to understand the exact nature of the relationship.

DAT-2.A.4: Often a single data source does not contain the necessary data to draw a conclusion. It may be required to combine data from a variety of sources to formulate a conclusion.

DAT-2.B.1: Metadata are data about data. Metadata is associated with the primary data; the primary data may be an image, a Web page, or other complex object.

DAT-2.B.2: Changes and deletions made to metadata do not change the primary data.

DAT-2.B.3: Metadata are used for finding, organizing and managing information.

DAT-2.D.3 Search tools are useful for efficiently finding information.

IOC-2.A.1: Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.

IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.

IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.

IOC-2.A.12: PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

IOC-2.A.13: It is difficult to delete information once it has been placed online.

IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.

IOC-2.C.1: Phishing is a technique that is used to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Community Colleges Catalyzing Computing and Cybersecurity

Computer Science Principles

Computing Systems and Networks

CSN

Impact of Computing

IOC

# Risk

Describe the differences between the Internet and the World Wide Web. (LO CSN-1.D)

For fault-tolerant systems, like the Internet: a)Describe the benefits of fault tolerance. b)Explain how a given system is fault-tolerant. c)Identify vulnerabilities to failure in a system. (LO CSN-1.E)

IOC-2.A Describe the risks to privacy from collecting and storing personal data on a computer system. (LO IOC-2.A)

# Cybersecurity Concept Lesson: Risk

Students will: 1) discuss computing resources that can be misused, 2) identify how computing resources and information assets can be vulnerable to attack, 3) explain the role and types of protection mechanisms to achieve confidentiality, integrity, and availability of computing resources and information assets, and 4) summarize security and privacy risks from collecting and storying personal data on a computer system.

Prerequisite Knowledge: Students should be familiar with Internet concepts, the CIA Triad, and Identification, Authentication, and Authorization concepts.

Length of Completion: 4 to 6 class periods (based on 50 minutes)

CSN-1.D.1 The World Wide Web is a system of linked pages, programs, and files.

CSN-1.D.3 The World Wide Web uses the Internet.

CSN-1.E.2 Redundancy is the inclusion of extra components that can be used to mitigate failure of a system if other components fail.

CSN-1.E.3 One way to accomplish network redundancy is by having more than one path between any two connected devices.

CSN-1.E.5 When a system can support failures and still continue to function, it is called fault-tolerant. This is important because elements of complex systems fail at unexpected times, often in groups, and fault tolerance allows users to continue to use the network.

IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.

IOC-2.A.2 Search engines can record and maintain a history of searches made by users.

IOC-2.A.3 Websites can record and maintain a history of individuals who have viewed their pages.

IOC-2.A.4 Devices, websites, and networks can collect information about a user's location.

IOC-2.A.5 Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.

IOC-2.A.6 Search engines can use search history to suggest websites or for targeted marketing.

IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.

IOC-2.A.8 PII and other information placed online can be used to enhance a user's online experiences.

IOC-2.A.9 PII stored online can be used to simplify making online purchases.

IOC-2.A.10 Commercial and governmental curation of information may be exploited if privacy and other protections are ignored.

IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.

IOC-2.A.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

IOC-2.A.13It is difficult to delete information once it has been placed online.

IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.

Computer Science Principles

Computing Systems and Networks

CSN

Impact of Computing

IOC

## Risk

Explain how computing resources can be protected and can be misused. (LO IOC-2.B)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Risk

Students will: 1) discuss computing resources that can be misused, 2) identify how computing resources and information assets can be vulnerable to attack, 3) explain the role and types of protection mechanisms to achieve confidentiality, integrity, and availability of computing resources and information assets, and 4) summarize security and privacy risks from collecting and storying personal data on a computer system.

Prerequisite Knowledge: Students should be familiar with Internet concepts, the CIA Triad, and Identification, Authentication, and Authorization concepts.

Length of Completion: 4 to 6 class periods (based on 50 minutes)

IOC-2.B.1 Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.

IOC-2.B.2 A strong password is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.

IOC-2.B.3 Multifactor authentication is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge, possession, and inheritance.

IOC-2.B.4 Multifactor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.

IOC-2.B.5 Encryption is the process of encoding data to prevent unauthorized access to information. Decryption is the process of decoding the data.

IOC-2.B.6 Certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.

IOC-2.B.7 Computer virus and malware scanning software can help protect a computing system against infection.

IOC-2.B.8 A computer virus is a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.

IOC-2.B.9 Malware is software intended to damage a computing system or to take partial control over its operation.

IOC-2.B.10 All real-world systems have errors or design flaws that can be exploited to compromise them. Regular software updates help fix errors that could compromise a computing system.

IOC-2.B.11 Users can control the permissions programs have for collecting user information. Users should review the permission settings of programs to protect their privacy.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.

IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.

IOC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.

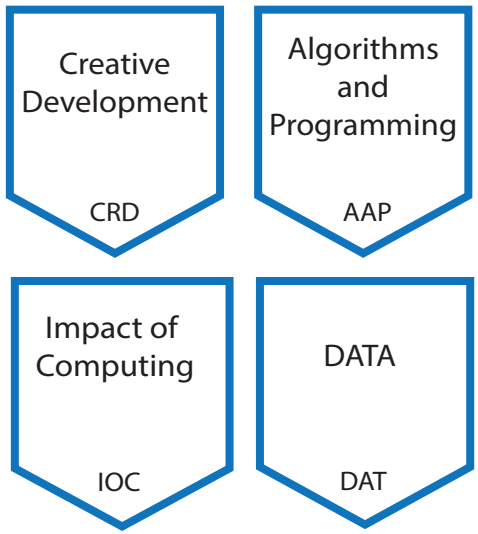
IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.

IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.

IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.

IOC-2.C.7 Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.

Computer Science Principles




## Steganography

Identify input(s) to a program. (LO CRD-2.C)

Identify output(s) produced by a program. (LO CRD-2.D)

Compare data compression algorithms to determine which is best in a particular context. (LO DAT-1.D)

Identify the challenges associated with processing data. (LO DAT-2.C)

Extract information from data using a program. (LO DAT-2.D)

Explain how programs can be used to gain insight and knowledge from data. (LO DAT-2.E)

# Cybersecurity Concept Lesson: Steganography

Students will: 1) investigate how Steganography can hide information inside of a file, message, photograph, or video, 2) write a series of programs which advance a starting photograph file and a starting secret message file into a Steganographic photograph, c) decode a secret message in a photograph, and 4) explore how secret codes are used in government surveillance.

Prerequisite Knowledge: Students should be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. This CCL works best as a lead-in to the Caesar Cipher CCL, the Vigenère Cipher CCL, and the Symmetric and Public Key Cryptography CCL.

Length of Completion: 4 or 5 class periods (based on 50 minutes)

CRD-2.C.1 Program input is data sent to a computer for processing by a program. Input can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.C.4 Inputs usually affect the output produced by a program.

CRD-2.C.6 Input can come from a user or other programs.

CRD-2.D.1 Program output is any data sent from a program to a device. Program output can come in a variety of forms, such as tactile, audio, visual, or text.

CRD-2.D.2 Program output is usually based on a program's input or prior state (e.g., internal values).

DAT-1.D.1 Data compression can reduce the size (number of bits) of transmitted or stored data.

DAT-1.D.2 Fewer bits does not necessarily mean less information.

DAT-1.D.3 The amount of size reduction from compression depends on both the amount of redundancy in the original data representation and the compression algorithm applied.

DAT-1.D.4 Lossless data compression algorithms can usually reduce the number of bits stored or transmitted while guaranteeing complete reconstruction of the original data.

DAT-1.D.5 Lossy data compression algorithms can significantly reduce the number of bits stored or transmitted but only allow reconstruction of an approximation of the original data.

DAT-1.D.6 Lossy data compression algorithms can usually reduce the number of bits stored or transmitted more than lossless compression algorithms.

DAT-1.D.7 In situations where quality or ability to reconstruct the original is maximally important, lossless compression algorithms are typically chosen.

DAT-1.D.8 In situations where minimizing data size or transmission time is maximally important, lossy compression algorithms are typically chosen.

DAT-2.C.1 The ability to process data depends on the capabilities of the users and their tools.

DAT-2.D.1 Programs can be used to process data to acquire information.

DAT-2.E.1 Programs are used in an iterative and interactive way when processing information to allow users to gain insight and knowledge about data.

DAT-2.E.2 Programmers can use programs to filter and clean digital data, thereby gaining insight and knowledge.

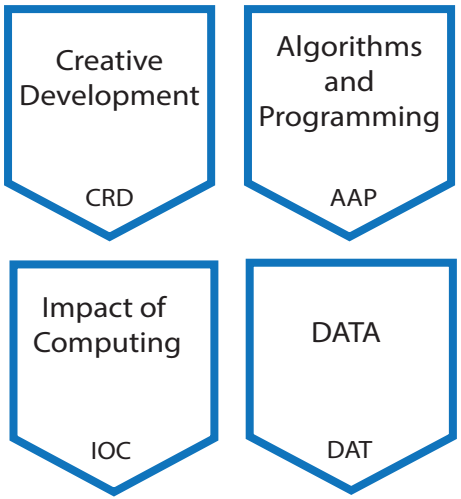
DAT-2.E.4 Insight and knowledge can be obtained from translating and transforming digitally represented information.

DAT-2.E.5 Patterns can emerge when data are transformed using programs.



Based on 2020-21 Framework

Computer Science Principles




# Cybersecurity Concept Lesson: Steganography

Students will: 1) investigate how Steganography can hide information inside of a file, message, photograph, or video, 2) write a series of programs which advance a starting photograph file and a starting secret message file into a Steganographic photograph, c) decode a secret message in a photograph, and 4) explore how secret codes are used in government surveillance.

Prerequisite Knowledge: Students should be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. This CCL works best as a lead-in to the Caesar Cipher CCL, the Vigenère Cipher CCL, and the Symmetric and Public Key Cryptography CCL.

Length of Completion: 4 or 5 class periods (based on 50 minutes)

## Steganography

Represent a value with a variable. (LO AAP-1.A)

Represent a list or string using a variable. (LO AAP-1.C)

Evaluate expressions that use arithmetic operators. (LO AAP-2.C)

Evaluate expressions that manipulate strings. (LO AAP-2.D)

Express an algorithm that uses selection without using a programming language. (LO AAP-2.G)

For selection:
a. Write conditional statements.
b. Determine the result of conditional statements. (LO AAP-2.H)

For iteration:
a. Write iteration statements.
b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

For algorithms:
a. Create algorithms.
b. Combine and modify existing algorithms. (LO AAP-2.M)

For list operations:
a. Write expressions that use list indexing and list procedures.
b. Evaluate expressions that use list indexing and list procedures. (LO AAP-2.N)

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP-1.A.3 Some programming languages provide types to represent data, which are referenced using variables. These types include numbers, Booleans, lists, and strings.

AAP-1.A.4 Some values are better suited to representation using one type of data rather than another.

AAP-1.C.1 A list is an ordered sequence of elements. For example, [value1, value2, value3, …] describes a list where value1 is the first element, value2 is the second element, value3 is the third element, and so on.

AAP-1.C.3 An index is a common method for referencing the elements in a list or string using natural numbers.

AAP-1.C.4 A string is an ordered sequence of characters.

AAP-2.C.1 Arithmetic operators are part of most programming languages and include addition, subtraction, multiplication, division, and modulus operators.

AAP-2.C.2 The exam reference sheet provides a MOD b, which evaluates to the remainder when a is divided by b. Assume that a is an integer greater than or equal to 0 and b is an integer greater than 0. For example, 17 MOD 5 evaluates to 2.

AAP-2.D.1 String concatenation joins together two or more strings end-to-end to make a new string.

AAP-2.G.1 Selection determines which parts of an algorithm are executed based on a condition being true or false

AAP-2.H.1 Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP-2.K.1 Iteration statements change the sequential flow of control by repeating a set of statements zero or more times, until a stopping condition is met.

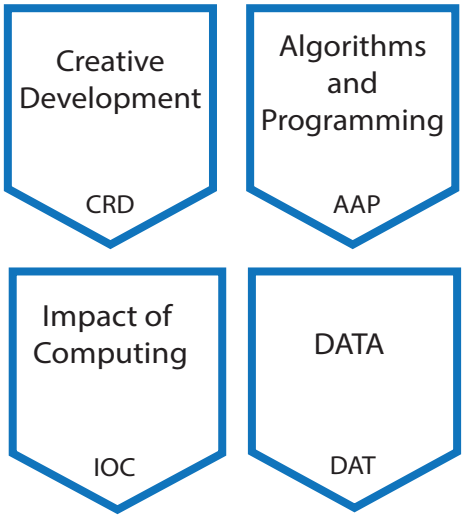
AAP-2.M.1 Algorithms can be created from an idea, by combining existing algorithms, or by modifying existing algorithms.

AAP-2.N.1 The exam reference sheet provides basic operations on lists, including: accessing an element by index, assigning a value of an element of a list to a variable, assigning a value to an element of a list, inserting elements at a given index, adding elements to the end of the list, removing elements, and determining the length of a list.



Based on 2020-21 Framework

Computer Science Principles




## Steganography

For algorithms involving elements of a list:
a. Write iteration statements to traverse a list.
b. Determine the result of an algorithm that includes list traversals. (LO AAP-2.O)

For procedure calls:
a. Write statements to call procedures.
b. Determine the result or effect of a procedure call. (LO AAP-3.A)

Explain how the use of procedural abstraction manages complexity in a program. (LO AAP-3.B)

For generating random values:
a. Write expressions to generate possible values.
b. Evaluate expressions to determine the possible results (LO AAP-3.E)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Steganography

Students will: 1) investigate how Steganography can hide information inside of a file, message, photograph, or video, 2) write a series of programs which advance a starting photograph file and a starting secret message file into a Steganographic photograph, c) decode a secret message in a photograph, and 4) explore how secret codes are used in government surveillance.

Prerequisite Knowledge: Students should be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. This CCL works best as a lead-in to the Caesar Cipher CCL, the Vigenère Cipher CCL, and the Symmetric and Public Key Cryptography CCL.

Length of Completion: 4 or 5 class periods (based on 50 minutes)

AAP-2.O.1 Traversing a list can be a complete traversal, where all elements in the list are accessed, or a partial traversal, where only a portion of elements are accessed.

AAP-2.O.2 Iteration statements can be used to traverse a list.

AAP-3.A.1 A procedure is a named group of programming instructions that may have parameters and return values.

AAP-3.A.2 Procedures are referred to by different names, such as method or function, depending on the programming language.

AAP-3.A.3 Parameters are input variables of a procedure. Arguments specify the values of the parameters when a procedure is called.

AAP-3.A.4 A procedure call interrupts the sequential execution of statements, causing the program to execute the statements within the procedure before continuing. Once the last statement in the procedure (or a return statement) has executed, flow of control is returned to the point immediately following where the procedure was called.

AAP-3.B.1 One common type of abstraction is procedural abstraction, which provides a name for a process and allows a procedure to be used only knowing what it does, not how it does it.

AAP-3.B.2 Procedural abstraction allows a solution to a large problem to be based on the solution of smaller subproblems. This is accomplished by creating procedures to solve each of the subproblems.

AAP-3.B.5 Using parameters allows procedures to be generalized, enabling the procedures to be reused with a range of input values or arguments.

AAP-3.E.1 The exam reference sheet provides RANDOM(a, b) which generates and returns a random integer from a to b, inclusive. Each result is equally likely to occur. For example, RANDOM(1, 3) could return 1, 2, or 3.

AAP-3.E.2 Using random number generation in a program means each execution may produce a different result.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.



Based on 2020-21 Framework

Computer Science Principles

Creative Development
CRD

Algorithms and Programming
AAP

Impact of Computing
IOC

## Symmetric & Public Key Cryptography

Explain how computing innovations are improved through collaboration. (LO CRD-1.A)

Demonstrate effective interpersonal skills during collaboration. (LO CRD-1.C)

Explain how a program or code segment functions. (LO CRD-2.B)

For errors in an algorithm or program:
a. Identify the error.
b. Correct the error. (LO CRD-2.I)

Represent a value with a variable. (LO AAP-1.A)

Represent a list or string using a variable. (LO AAP-1.C)

Evaluate expressions that use arithmetic operators. (LO AAP-2.C)

Evaluate expressions that manipulate strings. (LO AAP-2.D)

# Cybersecurity Concept Lesson: Symmetric & Public Key Cryptography

Students will: 1) investigate how Symmetric and Public Key Encryption work to achieve the goals of confidentiality of information and integrity/authentication of sender, 2) explain the difference between Symmetric and Public Key Encryption methodologies, 3) explain how a one-way function (which underlies both Symmetric and Public Key Encryption) can create a public secret and the difficulty with which the process can be reversed, and 4) write a program that models the public key exchange mechanism of the Diffie-Hellman Symmetric Key Exchange algorithm thereby advancing their programming capabilities by using more advanced mathematical operators (e.g., modulus, exponents).

Prerequisite Knowledge: Students should be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. For students who have not completed their study of programming a pseudo-code version of the programming exercise has been included.

Length of Completion: 2 to 3 class periods (based on 50 minutes)

CRD-1.A.3 Effective collaboration produces a computing innovation that reflects the diversity of talents and perspectives of those who designed it.

CRD-1.C.1 Effective collaborative teams practice interpersonal skills, including but not limited to: communication, consensus building, conflict resolution, and negotiation.

CRD-2.B.1 A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.I.1 A logic error is a mistake in the algorithm or program that causes it to behave incorrectly or unexpectedly.

CRD-2.I.2 A syntax error is a mistake in the program where the rules of the programming language are not followed.

CRD-2.I.3 A run-time error is a mistake in the program that occurs during the execution of a program. Programming languages define their own run-time errors.

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP-1.A.3 Some programming languages provide types to represent data, which are referenced using variables. These types include numbers, Booleans, lists, and strings.

AAP-1.A.4 Some values are better suited to representation using one type of data rather than another.

AAP-1.C.1 A list is an ordered sequence of elements. For example, [value1, value2, value3, ...] describes a list where value1 is the first element, value2 is the second element, value3 is the third element, and so on.

AAP-1.C.3 An index is a common method for referencing the elements in a list or string using natural numbers.

AAP-1.C.4 A string is an ordered sequence of characters.

AAP-2.C.1 Arithmetic operators are part of most programming languages and include addition, subtraction, multiplication, division, and modulus operators.

AAP-2.C.2 The exam reference sheet provides a MOD b, which evaluates to the remainder when a is divided by b. Assume that a is an integer greater than or equal to 0 and b is an integer greater than 0. For example, 17 MOD 5 evaluates to 2.

AAP-2.D.1 String concatenation joins together two or more strings end-to-end to make a new string.



Based on 2020-21 Framework

Computer Science Principles

Creative Development (CRD) | Algorithms and Programming (AAP) | Impact of Computing (IOC)

## Symmetric & Public Key Cryptography

Express an algorithm that uses selection without using a programming language. (LO AAP-2.G)

For selection:
a. Write conditional statements.
b. Determine the result of conditional statements. (LO AAP-2.H)

For iteration:
a. Write iteration statements.
b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

For algorithms:
a. Create algorithms.
b. Combine and modify existing algorithms. (LO AAP-2.M)

For list operations:
a. Write expressions that use list indexing and list procedures. b. Evaluate expressions that use list ndexing and list procedures. (LO AAP-2.N)

For algorithms involving elements of a list:
a. Write iteration statements to traverse a list.
b. Determine the result of an algorithm that includes list traversals. (LO AAP-2.O)

For procedure calls:
a. Write statements to call procedures.
b. Determine the result or effect of a procedure call. (LO AAP-3.A)

Explain how the use of procedural abstraction manages complexity in a program. (LO AAP-3.B)

For generating random values:
a. Write expressions to generate possible values.
b. Evaluate expressions to determine the possible results (LO AAP-3.E)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Symmetric & Public Key Cryptography

Students will: 1) investigate how Symmetric and Public Key Encryption work to achieve the goals of confidentiality of information and integrity/authentication of sender, 2) explain the difference between Symmetric and Public Key Encryption methodologies, 3) explain how a one-way function (which underlies both Symmetric and Public Key Encryption) can create a public secret and the difficulty with which the process can be reversed, and 4) write a program that models the public key exchange mechanism of the Diffie-Hellman Symmetric Key Exchange algorithm thereby advancing their programming capabilities by using more advanced mathematical operators (e.g., modulus, exponents).

Prerequisite Knowledge: Students should be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. For students who have not completed their study of programming a pseudo-code version of the programming exercise has been included.

Length of Completion: 2 to 3 class periods (based on 50 minutes)

AAP-2.G.1 Selection determines which parts of an algorithm are executed based on a condition being true or false

AAP-2.H.1 Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP-2.K.1 Iteration statements change the sequential flow of control by repeating a set of statements zero or more times, until a stopping condition is met.

AAP-2.M.1 Algorithms can be created from an idea, by combining existing algorithms, or by modifying existing algorithms.

AAP-2.N.1 The exam reference sheet provides basic operations on lists, including: accessing an element by index, assigning a value of an element of a list to a variable, assigning a value to an element of a list, inserting elements at a given index, adding elements to the end of the list, removing elements, and determining the length of a list.

AAP-2.N.2 List procedures are implemented in accordance with the syntax rules of the programming language.

AAP-2.O.1Traversing a list can be a complete traversal, where all elements in the list are accessed, or a partial traversal, where only a portion of elements are accessed.

AAP-2.O.2 Iteration statements can be used to traverse a list.

AAP-3.A.1 A procedure is a named group of programming instructions that may have parameters and return values.

AAP-3.A.2 Procedures are referred to by different names, such as method or function, depending on the programming language.

AAP-3.A.3 Parameters are input variables of a procedure. Arguments specify the values of the parameters when a procedure is called.

AAP-3.A.4 A procedure call interrupts the sequential execution of statements, causing the program to execute the statements within the procedure before continuing. Once the last statement in the procedure (or a return statement) has executed, flow of control is returned to the point immediately following where the procedure was called.

AAP-3.B.1 One common type of abstraction is procedural abstraction, which provides a name for a process and allows a procedure to be used only knowing what it does, not how it does it.

AAP-3.B.2 Procedural abstraction allows a solution to a large problem to be based on the solution of smaller subproblems. This is accomplished by creating procedures to solve each of the subproblems.

AAP-3.B.5 Using parameters allows procedures to be generalized, enabling the procedures to be reused with a range of input values or arguments.

AAP-3.E.1 The exam reference sheet provides RANDOM(a, b) which generates and returns a random integer from a to b, inclusive. Each result is equally likely to occur. For example, RANDOM(1, 3) could return 1, 2, or 3.

AAP-3.E.2 Using random number generation in a program means each execution may produce a different result.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.



Based on 2020-21 Framework

Computer Science Principles

Creative Development
CRD

Algorithms and Programming
AAP

Impact of Computing
IOC

## Vigenère Cipher

Explain how computing innovations are improved through collaboration. (LO CRD-1.A)

Demonstrate effective interpersonal skills during collaboration. (LO CRD-1.C)

Explain how a program or code segment functions. (LO CRD-2.B)

For errors in an algorithm or program:
a. Identify the error.
b. Correct the error. (LO CRD-2.I)

Represent a value with a variable. (LO AAP-1.A)

Represent a list or string using a variable. (LO AAP-1.C)

Evaluate expressions that use arithmetic operators. (LO AAP-2.C)

Evaluate expressions that manipulate strings. (LO AAP-2.D)

# Cybersecurity Concept Lesson: Vigenère Cipher

Students will: 1) investigate how Vigenère Ciphers work to achieve the goals of confidentiality of information and integrity/authentication of sender, their historical context, and strengths and weaknesses, 2) encrypt and decrypt text using Vigenère Ciphers, c) implement a Vigenère Cipher in a programming language, and 4) ascertain the correctness of their program as a functional program to protect information assets and computing resources.

Prerequisite Knowledge: Students will need to be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. For students who have not completed their study of programming a pseudo-code version of the programming exercise has been included.

Length of Completion: 2 to 3 class periods (based on 50 minutes)

CRD-1.A.3 Effective collaboration produces a computing innovation that reflects the diversity of talents and perspectives of those who designed it.

CRD-1.C.1 Effective collaborative teams practice interpersonal skills, including but not limited to: communication, consensus building, conflict resolution, and negotiation.

CRD-2.B.1 A program is a collection of program statements that performs a specific task when run by a computer. A program is often referred to as software.

CRD-2.I.1 A logic error is a mistake in the algorithm or program that causes it to behave incorrectly or unexpectedly.

CRD-2.I.2 A syntax error is a mistake in the program where the rules of the programming language are not followed.

CRD-2.I.3 A run-time error is a mistake in the program that occurs during the execution of a program. Programming languages define their own run-time errors.

AAP-1.A.1 A variable is an abstraction inside a program that can hold a value. Each variable has associated data storage that represents one value at a time, but that value can be a list or other collection that in turn contains multiple values.

AAP-1.A.2 Using meaningful variable names helps with the readability of program code and understanding of what values are represented by the variables.

AAP-1.A.3 Some programming languages provide types to represent data, which are referenced using variables. These types include numbers, Booleans, lists, and strings.

AAP-1.A.4 Some values are better suited to representation using one type of data rather than another.

AAP-1.C.1 A list is an ordered sequence of elements. For example, [value1, value2, value3, ...] describes a list where value1 is the first element, value2 is the second element, value3 is the third element, and so on.

AAP-1.C.3 An index is a common method for referencing the elements in a list or string using natural numbers.

AAP-1.C.4 A string is an ordered sequence of characters.

AAP-2.C.1 Arithmetic operators are part of most programming languages and include addition, subtraction, multiplication, division, and modulus operators.

AAP-2.C.2 The exam reference sheet provides a MOD b, which evaluates to the remainder when a is divided by b. Assume that a is an integer greater than or equal to 0 and b is an integer greater than 0. For example, 17 MOD 5 evaluates to 2.

AAP-2.D.1 String concatenation joins together two or more strings end-to-end to make a new string.



Based on 2020-21 Framework

Computer Science Principles

Creative Development CRD

Algorithms and Programming AAP

Impact of Computing IOC

## Vigenère Cipher

Express an algorithm that uses selection without using a programming language. (LO AAP-2.G)

For selection:
a. Write conditional statements.
b. Determine the result of conditional statements. (LO AAP-2.H)

For iteration:
a. Write iteration statements.
b. Determine the result or side-effect of iteration statements. (LO AAP-2.K)

For algorithms:
a. Create algorithms.
b. Combine and modify existing algorithms. (LO AAP-2.M)

For list operations:
a. Write expressions that use list indexing and list procedures.
b. Evaluate expressions that use list indexing and list procedures. (LO AAP-2.N)

For algorithms involving elements of a list:
a. Write iteration statements to traverse a list.
b. Determine the result of an algorithm that includes list traversals. (LO AAP-2.O)

For procedure calls:
a. Write statements to call procedures.
b. Determine the result or effect of a procedure call. (LO AAP-3.A)

Explain how the use of procedural abstraction manages complexity in a program. (LO AAP-3.B)

For generating random values:
a. Write expressions to generate possible values.
b. Evaluate expressions to determine the possible results (LO AAP-3.E)

Explain how unauthorized access to computing resources is gained. (LO IOC-2.C)

# Cybersecurity Concept Lesson: Vigenère Cipher

**Students will: 1) investigate how Vigenère Ciphers work to achieve the goals of confidentiality of information and integrity/authentication of sender, their historical context, and strengths and weaknesses, 2) encrypt and decrypt text using Vigenère Ciphers, c) implement a Vigenère Cipher in a programming language, and 4) ascertain the correctness of their program as a functional program to protect information assets and computing resources.**

**Prerequisite Knowledge: Students will need to be familiar with the following programming fundamentals: conditional statements, iteration, arrays, array processing, strings, modulus mathematics, and string processing. For students who have not completed their study of programming a pseudo-code version of the programming exercise has been included.**

**Length of Completion: 2 to 3 class periods (based on 50 minutes)**

AAP-2.G.1 Selection determines which parts of an algorithm are executed based on a condition being true or false

AAP-2.H.1 Conditional statements or "if-statements" affect the sequential flow of control by executing different statements based on the value of a Boolean expression.

AAP-2.K.1 Iteration statements change the sequential flow of control by repeating a set of statements zero or more times, until a stopping condition is met.

AAP-2.M.1 Algorithms can be created from an idea, by combining existing algorithms, or by modifying existing algorithms.

AAP-2.N.1 The exam reference sheet provides basic operations on lists, including: accessing an element by index, assigning a value of an element of a list to a variable, assigning a value to an element of a list, inserting elements at a given index, adding elements to the end of the list, removing elements, and determining the length of a list.

AAP-2.O.1Traversing a list can be a complete traversal, where all elements in the list are accessed, or a partial traversal, where only a portion of elements are accessed.

AAP-2.O.2 Iteration statements can be used to traverse a list.

AAP-3.A.1 A procedure is a named group of programming instructions that may have parameters and return values.

AAP-3.A.2 Procedures are referred to by different names, such as method or function, depending on the programming language.

AAP-3.A.3 Parameters are input variables of a procedure. Arguments specify the values of the parameters when a procedure is called.

AAP-3.A.4 A procedure call interrupts the sequential execution of statements, causing the program to execute the statements within the procedure before continuing. Once the last statement in the procedure (or a return statement) has executed, flow of control is returned to the point immediately following where the procedure was called.

AAP-3.B.1 One common type of abstraction is procedural abstraction, which provides a name for a process and allows a procedure to be used only knowing what it does, not how it does it.

AAP-3.B.2 Procedural abstraction allows a solution to a large problem to be based on the solution of smaller subproblems. This is accomplished by creating procedures to solve each of the subproblems.

AAP-3.B.5 Using parameters allows procedures to be generalized, enabling the procedures to be reused with a range of input values or arguments.

AAP-3.E.1 The exam reference sheet provides RANDOM(a, b) which generates and returns a random integer from a to b, inclusive. Each result is equally likely to occur. For example, RANDOM(1, 3) could return 1, 2, or 3.

AAP-3.E.2 Using random number generation in a program means each execution may produce a different result.

IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.