Data Security Assessment Guide

How to use this Guide

This guide provides content and structure for the development of assessment items in data security. It is based on 7 learning objectives in data security. Each learning objective is organized into focal knowledge statements (see Table 1 and Figure 1). The focal knowledge statements are then broken down into the concepts and elements that could be used in assessing student learning (see Tables 2-8). Examples of assessment prompts are provided for each focal knowledge statement. The assessment prompts are representative and not an exhaustive list.

The knowledge statements provide a way to connect content to learning objectives in a structured manner that makes explicit what students should know or demonstrate. This guide can be used by educators or educational researchers to develop valid assessment items in data security.

This material is based upon work supported by the National Science Foundation under Grant No. 2117073.

Table 1

4.1.1: Students will understand how the characteristics and value of data impact data security.
411-01 Characteristics of data impact data security.
411-02 The value of data assets and corresponding risk(s) to data impact data security decisions.
4.1.2: Students will understand cybersecurity principles that restrict access to information and are implemented in data security protections.
412-01 The principles of least privilege, defense-in-depth, separation of duties, and minimization are security principles that restrict access to information and resources.
4.2.1: Students will identify data protection legislation, policies and procedures, and explain how they protect data.
421-01 Data protection laws, regulations, and standards impact organizational policies and procedures.
421-02 Data protection laws and organizational policies and procedures regulate the security of private and sensitive data by specifying security functions such as who has access, how data should be protected, and how long it should be retained.
4.3.1: Students will identify technical controls that are used to secure data.
431-01 Access control determines who can interact with an object.
431-02 Identification, authentication, authorization, and accounting (IAAA) are the four elements of the identity and access management (IAM) framework that ensures only legitimate and authorized users can access and use the system resources.
431-03 Other technical controls include network security devices such as firewalls and intrusion detection systems, encryption, configuration management, and data privacy controls.
4.3.2: Students will identify physical controls that are used to secure data.
432-01 Physical security controls are measures to protect data assets from physical harm, access, or disclosure.
432-02 Physical security controls provide protection from potential environmental threats and can include contingency planning for continued operation.
4.4.1: Students will define cryptography and explain how it is used in data security.
441-01 Cryptography uses an algorithm and a key to provide operations that can provide confidentiality and prevent unauthorized access to data.
441-02 Symmetric cryptography, asymmetric cryptography, and hashing are cryptographic processes.
441-03 Cryptographic mechanisms are used for data integrity by guarding against unauthorized modification or destruction of data and can ensure nonrepudiation and authenticity.
441-04 Cryptography evolves with technological advances and in response to cyber-attacks.
4.4.2: Students will understand how symmetric and asymmetric cryptography work.
442-01 Symmetric cryptography uses a shared secret key to transform plaintext to ciphertext and ciphertext to plaintext.
442-02 Asymmetric cryptography uses a pair of keys to encrypt and to decrypt messages.

Graphical representation of learning objectives and focal knowledge statements

Figure 1

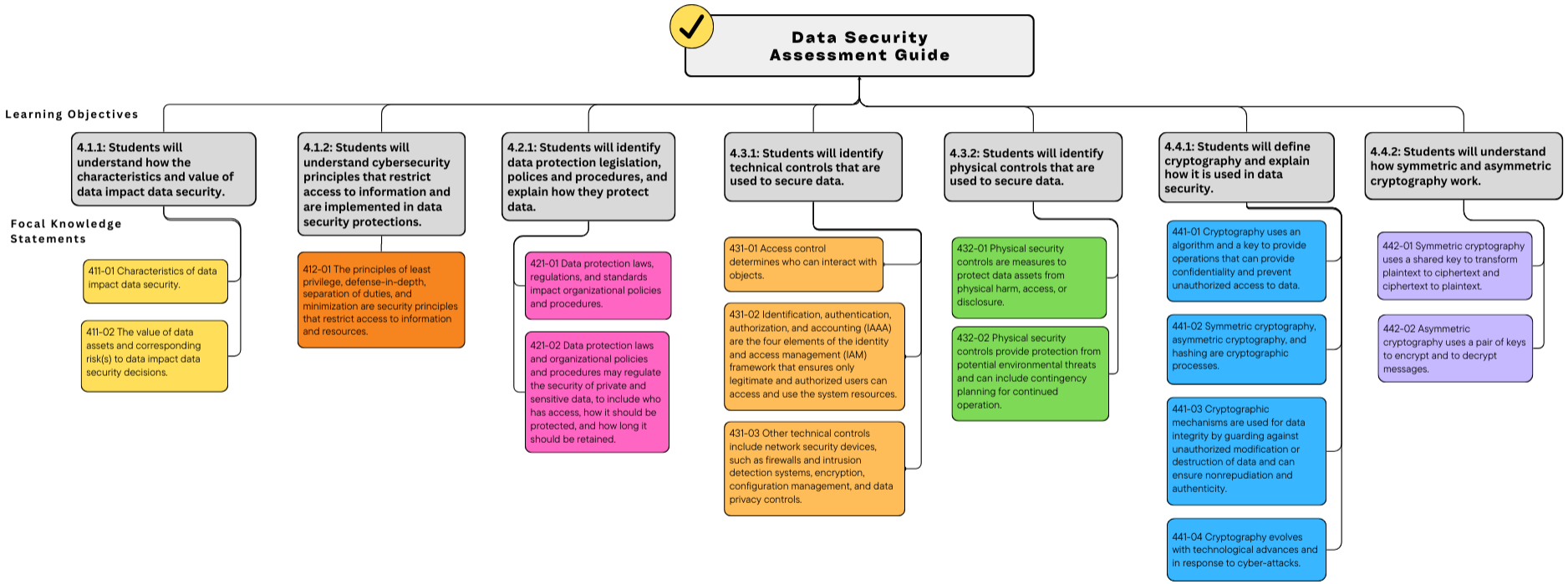

Table 2

4.1.1: Students will understand how the characteristics and value of data impact data security.	
Focal Knowledge	411-01 Characteristics of data impact data security.
Knowledge Statements	• Data is a subset of information in an electronic format that allows it to be retrieved or transmitted; whereas information is a meaningful expression of data. • Data can exist in one of three states in a computational environment: data at rest (storage), data in transit, or data in process (use). • Data at rest resides on a storage media. • Data in transit is the transmission of data from one place to another. • Data in use is data that is in the process of being transformed in format (e.g. computation, compression, encryption). • The data states can be combined in a sequence of operations, for example from transit to processing to storage. • Security requirements change with the state of the data and the requirements for confidentiality, integrity, and/or availability. • Confidentiality means to preserve authorized restrictions on information access and disclosure. • Integrity means to guard against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. • Availability refers to the timely and reliable access to and use of information. • Authentication is the verification of the source (user, process, or device) of data. • Data velocity is the speed at which data is generated, collected, processed, and shared. High velocity makes it more challenging to monitor and respond to security threats. • The sheer volume of data creates challenges for classifying and securing data. • Data storage is often distributed across multiple systems. • Data veracity is the quality, accuracy, integrity, and credibility of data. • Data variety refers to data that is structured, unstructured, or semi structured depending upon the sources of data. Unstructured data is more difficult to assess its sensitivity and to provide appropriate levels of access control. • Metadata is data about data. For example, in a file system metadata provides information about a file's contents such as ownership, format, characteristics. Metadata can contain sensitive information such as a user's location. • Security tools generate metadata that can contain private data. • Data security includes physical security, access controls, and organizational policies and procedures. • The "loss" of data to an unauthorized party is irreparable. Data is readily copied and shared, which can increase the impact of the data loss. • Threats to data confidentiality include: exfiltration by a malicious insider, exfiltration by an external adversary, ransomware, misconfiguration, human error, misplaced hardware or theft. • Data integrity attacks include unauthorized insertion, deletion, or modification of data.

	• Malware, ransomware, malicious insiders, and human error are threats to data integrity.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the data state and related confidentiality and/or integrity concerns given a scenario. • Describe characteristics of data and how that impacts the security of data.
Focal Knowledge	411-02 The value of data assets and the corresponding risk(s) to data impact data security decisions.
Knowledge Statements	• A data asset is any information-based resource, including databases, systems, and services, as well as the data/information itself. • The value of data to an organization can indicate the impact to the organization if the data is lost/breached, leaked, stolen, or modified in an unauthorized manner. • The value of data to the adversary could be: financial gain, takeover, espionage, revenge, etc. • The value of data impacts how quickly an organization will need to respond to a security incident. • Data breaches can impact operations, finances, and the reputation of an organization. • Data "loss" is the exposure of proprietary, sensitive, or classified information through theft or leakage. • Data manipulation attacks occur when an adversary does not take data, but instead makes subtle, stealthy tweaks to data for some type of gain or effect. • Data availability attacks have the aim of making data unavailable to users when they need it. • Data can be accidentally or intentionally deleted, overwritten, or misplaced. • A data breach is the unauthorized access, disclosure, compromise, or loss of control of personally identifiable information. • Data exfiltration is the stealing or exporting of data from an organization. • Data "loss" can be the result of misconfigurations, errors, unpatched or outdated software, or insider attacks. • Data classification is the process of assigning a value to information, labeling it, and determining the requirements for handling of information. Not all information is of equal importance. • Data label examples include public, private, sensitive, confidential, critical, and proprietary data. • The data classification standard for NIST has three categories: low impact, moderate impact, and high impact. The categories represent the potential damage on operations, assets, or individuals from unauthorized disclosure or modification or destruction of the data. • Risk includes the potential harm to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. • Data security involves the process and measures to maintain confidentiality, integrity, and availability of data in a manner consistent with the organization's risk strategy. • Context impacts the security of data. For example, private health information should be confidential, but it must also be shared with the attending caregiver. Contextual information can determine when a user should be granted access to data. Enabling both confidentiality and availability/appropriate use of data requires security controls. • Risk assessment involves determining the likelihood and impact of an attack on data security given threats, vulnerabilities and controls.

Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Describe the purpose of data classification standards. • Demonstrate the use of a risk assessment matrix. • In a given scenario, describe the likely consequences of a data security incident in terms of confidentiality, integrity, and/or availability.

Table 3

4.1.2: Students will understand cybersecurity principles that restrict access to information and are implemented in data security protections.	
Focal Knowledge	412-01 The principles of least privilege, defense-in-depth, separation of duties, and minimization are security principles that restrict access to information and resources.
Knowledge Statements	• Least privilege is a security principle that a system should restrict the access privileges of users (or processes) to the minimum necessary to accomplish assigned tasks. • Non-privileged users should be prevented from executing functions reserved for system administrators or privileged accounts. • Privileged accounts should be restricted to organization-defined compelling operational needs. • Separation of duties is a principle that no user should be given enough privileges to misuse the system on their own. • Defense-in-depth uses a series of layered, redundant defensive measures to protect sensitive data. • The principle of minimization is the idea of keeping the least functionality necessary in a program or device in order to decrease the attack vectors. • Data minimization is the principle of limiting the collection of personal information to that which is necessary to accomplish a specific purpose. • Data minimization techniques include data masking, anonymization, and tokenization.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Explain how a given security principle relates to technical controls and to physical controls. • Explain how layering of security controls mitigates data security risk.

Table 4

4.2.1: Students will identify data protection legislation, policies, and procedures and explain how they protect data.	
Focal Knowledge	421-01 Data protection laws, regulations, and standards impact organizational policies and procedures.
Knowledge Statements	• Society influences the development of law and law influences the behavior and actions of individuals and organizations. • The sources of laws can be constitutional, statutes, common law, or administrative regulations.

	• Data security and privacy are interrelated. Privacy and confidentiality of information depends upon the establishment and maintenance of protective measures (security). • Privacy is the right to control how your information is viewed and used, while security is protection against danger. • Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to data. • Data security standards are guidelines and practices to protect information from unauthorized access, use, modification, disclosure, or destruction. • NIST Special Publication 800-53, "Guide for Assessing Security Controls in Federal Information Systems and Organization" is the standard required for U.S. federal agencies. • A security framework defines processes for the development of policies and procedures, and the implementation of security controls. • The NIST Cybersecurity Framework (CSF) is a set of guidelines and best practices to help organizations develop a cybersecurity program. It is a voluntary guide. • Internet transactions across state and international borders creates jurisdiction problems for enforcement of laws. Jurisdiction is the scope of authority to enforce laws.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the level of government involved in specific cybersecurity policies. • Describe how data protection laws impact organizational policies and practices. • Analyze how acceptable use policies impact data security.
Focal Knowledge	421-02 Data protection laws and organizational policies and procedures may regulate the security of private and sensitive data, to include who has access, how it should be protected, and how long it should be retained.
Knowledge Statements	• Data protection legislation (e.g. GDPR, PCI DSS, HIPAA, COPPA) may define data labels and compliance requirements for organizations. • Sensitive information is defined as information in which the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974. • Personally identifiable information (PII) is information that can be used to distinguish an individual's identity, either alone or when combined with other information that is linked to a specific individual. • Privacy is the right of a party to maintain control over and confidentiality of information about itself. • The impact of technology on privacy concerns has caused governments to address privacy concerns through new or updated laws and regulations. • The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards to protect individuals' medical records and other personal health information (PHI) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. • Protected health information (PHI) includes demographic data related to past, present, or future physical or mental health conditions, the provision of heath care, or the past, present, or future payment for the provision of health care to an individual.

	• The General Data Protection Regulation (GDPR) is a European data protection law that applies to any "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." • The Payment Card Industry Data Security Standard (PCI DSS) is mandated by credit card companies to secure and protect credit card data provided by cardholders and transmitted through card processing transactions. • The Children's Online Privacy Protection Act (COPPA) is a federal law requiring online services and websites to obtain parental consent before collecting, using, or disclosing personal information from children under age 13. • Data governance establishes standards and policies to manage the availability, retention, usability, integrity and security of data in an organization.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Describe how privacy intersects with data security laws. • Identify laws intended to protect PII and PHI. • Describe how changes in technology impact data protection laws.

Table 5

4.3.1: Students will identify technical controls that are used to secure data.	
Focal Knowledge	431-01 Access control determines who can interact with objects.
Knowledge Statements	• Access control is the granting or denying of specific requests to 1) obtain and use data and related information processing services; and 2) enter physical facilities. • Access is the ability to interact with an object or a resource. An object or resource is defined here as a device, file, program or process, and implies access to the information contained in the objects. • An access control list is a mechanism to implement access control for a system resource by enumerating the identities that are permitted to access the resource. • An access control request can come from a human, a machine, a process, or an application. • Access rights are described as permissions or privileges. • File permissions are the ability to view, modify, access, use, or delete resources. • Linux file permissions are defined as read, write, and execute. • Operating systems have access permissions for system administration, also known as a system administrator or a root user. These privileged users are authorized to perform security-related functions that are not authorized to ordinary users. • Role-based access control (RBAC) involves the assignment of roles to users. The role permissions reflect the permissions needed to perform defined functions within an organization. • Rule-based access control (RBAC) establishes a set of rules granting access to use resources. • Mandatory access control (MAC) restricts access to objects based on the sensitivity (security attributes) of the information contained in the object. • Discretionary access control (DAC) gives control to the owner of an object. The owner can determine who gets access rights and what those rights should be.

Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify examples of access control in a given scenario. • Implement Linux file permissions, change file permissions, and view file permissions.
Focal Knowledge	431-02 Identification, authentication, authorization, and accounting (IAAA) are the four elements of the identity and access management (IAM) framework that ensures only legitimate and authorized users can access and use the system resources.
Knowledge Statements	• Identification is the process of verifying the user or entity attempting to access a system or resource. • Identification is done through various means such as usernames, passwords, biometrics, security tokens, smartcards. • Attributes are distinctive features, characteristics or properties of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means. • Identification enables authentication and authorization in a system. • Identification management systems are responsible for the creation, use, and termination of electronic identities. • Authentication is the process of verifying identity to one previously established in the system. • User authentication is often based on passwords or biometric authentication. • Authentication can use a device, such as a token or an app on a smartphone. • Multifactor authentication is the combination of two or more types of authentications. • Categories of authentication may include: something you are, something you know, something you have, somewhere you are, or something you do. • User accounts, devices, network-capable devices, and computer processes use identification and authentication measures. • Authorization is the process of permitting or denying access to a specific resource. • User accounts are a means of managing user privileges. • Users are often grouped to manage privileges in a system. • Users may be assigned roles to manage privileges in a system. • Accounting is the process of tracking resource utilization by accounts. • Logging of events and auditing of logs for signs of a cyber-attack are accountability measures. • Intrusion detection is the process of monitoring events in a computer system or network and analyzing them for signs of possible incidents.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Distinguish between identification, authentication, and authorization. • Describe how logging, monitoring and auditing are used to detect data security events. • Explain why password strength is important to access control.
Focal Knowledge	431-03 Other technical controls include network security devices such as firewalls and intrusion detection systems, encryption, configuration management, and data privacy controls.
Knowledge Statements	• Technical controls are security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in hardware, software, or firmware components.

	• Firewalls safeguard the network from intentional or unintentional intrusion by filtering incoming and outgoing traffic based on predetermined rules. • Intrusion detection systems monitor and analyze network or system events by providing a warning of attempts to access system resources in an unauthorized manner. • Encryption protects sensitive information by making it unreadable to unauthorized parties. • Encryption protocols safeguard passwords and secure communications through technologies such as SSL/TLS. • Configuration management involves compliance with security policies. It can prevent vulnerabilities such as open/unused ports, default credentials, and misconfiguration of access controls. • Data backups are a corrective technical control providing protection against loss from errors, hardware failure, environmental and natural hazards, and cyber-attacks. • Data backups are just one component of a disaster recovery plan. • Data masking hides personal or sensitive data by substituting altered values. • Data anonymization protects private or sensitive information by removing identifiers that connect the stored data to an individual.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify data security technical controls. • Describe the role of detection, response, and recovery in data security.

Table 6

4.3.2: Students will identify physical controls that are used to secure data.	
Focal Knowledge	432-01 Physical security controls are measures to protect data assets from physical harm, access, or disclosure.
Knowledge Statements	• Physical security control are measures, policies, and procedures to protect an organization's information systems and physical structures from natural events, environmental hazards, and unauthorized intrusion. • Physical security facilities are the buildings and structures housing computer systems and networks. • Mobile and portable systems may be installed in vehicles or carried by humans and do not have a fixed position. • Physical access controls restrict the entry and exit of personnel, equipment, and media. • Measures to protect physical access include walls, fences, doors, bollards, barricades, locks, and lighting. • Access control vestibules, badges, signs, cameras, alarms, security guards, reception areas provide physical security and screening at entry points. • Closed-circuit television cameras and motion detectors can provide detection capability. • Physical security controls include protecting computer monitors from direct observation by unauthorized persons, interception of data transmission on tapped lines, and wireless signal interception. • Mobile devices have an increased risk of theft, and encryption of data files is a security measure to protect confidential information.

Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify physical security controls in a given scenario. • Describe how physical security relates to data security.
Focal Knowledge	432-02 Physical security controls provide protection from potential environmental threats and can include contingency planning for continued operation.
Knowledge Statements	• The geographic location of facilities determines the risk of natural threats to include earthquakes, flooding, high winds, etc. • The geographic location determines exposure to man-made threats such as burglary, chemical spills, explosions, fires, etc. • Measures to detect natural and environmental hazards include: fire detection and suppression; sensors for moisture detection and temperature; and motion detection systems. • Hot and cold aisle layouts control airflow. Excessive heat is an environmental hazard. • Power generators, uninterruptible power supply (UPS) and power redundancy supply backup are used in the event of power interruptions. • Restoration sites can be used to restore operation if a facility sustains physical damage. • Redundant servers and network connections provide the ability to continue operations in the event of hardware failure. • Redundant array of inexpensive disks (RAID) spreads data across several disks for recovery purposes. • A contingency plan is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failures or destruction of facilities.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Describe how environmental controls protect systems and the information contained on them. • Describe the role of contingency planning in a security plan.

Table 7

4.4.1: Students will define cryptography and explain how it is used in data security.	
Focal Knowledge	441-01 Cryptography uses an algorithm and a key to provide operations that can provide confidentiality and prevent unauthorized access to data.
Knowledge Statements	• Encryption is the process of hiding or coding information so that only the person a message was intended for can read it (confidentiality).Confidentiality is the property that sensitive information is not disclosed to unauthorized entities. • As a discipline, cryptography embodies the principles and techniques for making plain information unintelligible and for restoring encrypted information to intelligible form. • A cryptographic algorithm (also known as a cipher) is a well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. • Some examples of cryptographic algorithms are Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), and Secure Hash Algorithm (SHA-256). • The same algorithm must be used in order for two parties to communicate.

	• A cryptographic key is a parameter used with a cryptographic algorithm. An entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. • In some cases, the two parties use a single, shared key. In other cases, a pair of keys are generated with one key kept private and the other is public. • Encryption of stored information is a means for implementing access enforcement.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the role of cryptography in providing confidentiality. • Define key terms used in cryptography.
Focal Knowledge	441-02 Symmetric cryptography, asymmetric cryptography, and hashing are cryptographic processes.
Knowledge Statements	• Symmetric cryptography requires that two parties share the same key. The key is used to encrypt and to decrypt data. • Asymmetric cryptography (also known as public key cryptography) uses a pair of related keys. One of the keys is “public” and the other is “private.” • In asymmetric cryptography the private key is confidential, i.e., known only to the owner of it. The public key is shared with other parties. • A computer system can use both symmetric and asymmetric cryptography in order to use the advantages of each type. • Plaintext refers to intelligible data, and ciphertext refers to its unintelligible form. • Encryption is the process of transforming plaintext into ciphertext. The reversed process is called decryption. • Decryption is the process of transforming ciphertext into plaintext using a cryptographic algorithm and key. • Hashing algorithms are a mathematical function that makes data unreadable through a one-way function. • Hashing algorithms are one-way functions and can protect data at rest because they are nearly impossible to reverse. This makes hashing algorithms well-suited to password storage. • Cryptographic hash functions have several important properties: 1) deterministic, 2)resistant to collision (meaning no two inputs produce the same hash), 3) computationally infeasible to reverse the process, and 4) resistant to pre-image attacks.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the correct use of keys in symmetric cryptography. • Identify how keys are used in asymmetric cryptography. • Describe the use of hash functions as a one-way cryptographic function. • Identify properties of cryptographic hash functions. • Students will identify how hash functions are used.
Focal Knowledge	441-03 Cryptographic mechanisms are used for data integrity by guarding against unauthorized modification or destruction of data and can ensure nonrepudiation and authenticity.

Knowledge Statements	• Data encryption is often thought of in terms of providing confidentiality. It can also ensure integrity, authenticity, and nonrepudiation. • Integrity is a property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. • Authenticity is the property that data originated from its purported source. • Non-repudiation is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. • Hashing algorithms can be used to authenticate data by hashing a file and sharing the hash along with the file. The recipient of the file can generate a hash using the same algorithm and compare the hashes to ensure that the file has not been modified in transit. • Some popular hashing algorithms are the SHA and MD family of algorithms. SHA-256 is a cryptographic hash algorithm that produces a 256-bit value from an input string of text. MD-5 creates a 128-bit string value from a string of any length. • Authenticity of an electronic document and the identity of the sender of the document can be established through a digital signature. • Digital signatures are the result of a cryptographic transformation of data that provides origin authentication, data integrity, and signer non-repudiation. • Digital signatures use asymmetric cryptography and hashing. • The digital signature process involves hashing the message and then encrypting the hash with the sender's private key. Upon receipt the hash can be decrypted using the sender's public key. The message is hashed and the two hashes are compared. If the hashes are identical then the message was not altered in transit. The decryption using the sender's public key ensures that the sender possessed the private key and they are presumably the same person. The digital signature process can ensure integrity of the message and non-repudiation of the signer of the message. • The digital signature process does not ensure confidentiality of the message. Encryption of the message or of the channel used in transmission is needed as an additional step. • A Certificate Authority (CA) is a trusted third-party organization that issues and revokes digital certificates, which serve to validate the identities of entities (organizations, websites). • A root certificate is a self-signed certificate and verifies the identity of the root certificate authority.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Explain how hashing is used to authenticate data. • Explain the role of nonrepudiation in the signing and exchanging of documents. • Explain the process of a digital signature. • Describe the role of digital certificates in verifying identity.
Focal Knowledge	441-04 Cryptography evolves with technological advances and in response to cyber-attacks.
Knowledge Statements	• The desire to communicate in secret by hiding information began thousands of years ago. • Early cryptographic methods involved the shifting of letters to make text unreadable. • The Caesar cipher (or shift cipher) is a simple substitution cipher. Each plaintext letter is replaced by a letter some fixed number of positions down the alphabet.

	• The Vigenère cipher is a polyalphabetic substitution cipher. It encrypts each letter of plaintext with a different Caesar cipher. The increment is determined by a key (text). • Cryptographic methods have evolved and used advanced transposition and substitution ciphers. • Ciphers became automated through the use of mechanical and electromechanical devices. • The German Enigma machine in World War II is an example of an electromechanical encryption machine. • Cryptanalysis is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. • Frequency analysis is the study of the frequency of letters or groups of letters in ciphertext. • Frequency analysis is a common method used in cracking a substitution cipher. • Commercial transactions over the Internet in the 1990s increased interest in standards for encryption. • Key length refers to the length of a key in bits used by an algorithm. In general, longer keys provide stronger encryption.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the ciphertext when given the plaintext using a transposition cipher. • Identify the ciphertext when given the plaintext using a shift cipher. • Identify the ciphertext when given the plaintext using a substitution cipher. • Identify the encrypted message when given the decrypted message and a Vigenère Cipher table. • Students will identify the symmetric key used in a Rail Fence Cipher • Recognize cryptanalysis techniques and tools used against classical cryptography methods.

Table 8

4.4.2: Students will understand how symmetric and asymmetric cryptography work.	
Focal Knowledge	442-01 Symmetric cryptography uses a shared key to transform plaintext to ciphertext and ciphertext to plaintext.
Knowledge Statements	• Symmetric key cryptography uses a single key, and the sender and receiver must share the same key. • The sharing of the same key means that the channel used to share the key must be secure. • Data encryption provides confidentiality provided the key is kept secret. • The Data Encryption Standard (DES) published by NIST is a symmetric key system. • Symmetric key cryptography is faster than asymmetric key cryptography. • Symmetric cryptography is used to encrypt credit card information, personally identifiable information used in banking transactions, and data that is stored on a device (data at rest). • Symmetric and asymmetric cryptography are combined in some cases to improve the speed and the security of communication. For example, SSL/TLS use both symmetric and asymmetric cryptography.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Describe the advantages and disadvantages of symmetric key cryptography. • Identify implementations of symmetric key cryptography.
Focal Knowledge	442-02 Asymmetric cryptography uses a pair of keys to encrypt and to decrypt messages.

Knowledge Statements	• Asymmetric encryption uses a pair of related keys. The key pair is generated by a one-way function to create mathematically related keys. • The private key must be kept secret and the public key can be shared with other parties. • Asymmetric encryption solves the problem of sharing a single key (symmetric cryptography). • RSA (Rivest Shamir Adelman) is a commonly used asymmetric key encryption algorithm. • Public key infrastructure (PKI) is a framework established to issue, maintain, and revoke keys and certificates. • PKI certificates verify the owner of a private key and the authenticity of the exchange of keys. • Asymmetric encryption is slower than symmetric encryption. • Asymmetric encryption is implemented in SSL/TLS, S/MIME encrypted email, code signing, digital signatures, and end-to-end private messaging services.
Assessment Prompts	• Given questions about any of the knowledge statements above, select the correct answer. • Identify the role of the public and private keys in asymmetric cryptography. • Describe how public and private keys are mathematically linked. • Describe the process of encrypting a message, sending it to a recipient, and decrypting the message. • Describe advantages and disadvantages of asymmetric cryptography.