Welcome to the (ISC)2 Certified Information Systems Security Professional (CISSP) Training Course

Course Agenda

Domain 1: Security and Risk Management

Domain 2: Asset Security

Domain 3: Security Architecture and Engineering

Domain 4: Communication and Network Security

Domain 5: Identity and Access Management (IAM)

Domain 6: Security Assessment and Testing

Course Agenda (continued)

Domain 7: Security Operations

Domain 8: Software Development Security

Domain 3

Security Architecture and Engineering

Domain Objectives

1. Implement engineering processes using secure design principles.
2. Manage engineering processes using secure design principles.
3. Identify the purpose of security models.
4. Identify common security models.
5. Differentiate between security requirements and security controls.
6. Identify types of controls.
7. Identify common or inheritable controls.

Domain Objectives (continued)

8. Select appropriate security controls.
9. Identify major control frameworks.
10. Tailor security controls.
11. Identify security control evaluation criteria.
12. Identify types of system security capabilities.
13. Employ integrated security elements.
14. Identify vulnerabilities and mitigations in client-based systems.
15. Identify vulnerabilities and mitigations in server-based systems.
16. Identify vulnerabilities and mitigations in database systems.

Domain Objectives (continued)

17. Identify vulnerabilities and mitigations in industrial control systems (ICSs).
18. Identify vulnerabilities and mitigations in cloud-based systems.
19. Identify vulnerabilities and mitigations in distributed systems.
20. Identify vulnerabilities and mitigations in Internet of Things (IoT).
21. Assess and mitigate vulnerabilities in web-based systems.
22. Assess and mitigate vulnerabilities in mobile systems.
23. Assess and mitigate vulnerabilities in embedded systems.
24. Understand key terms associated with cryptography.

Domain Objectives (continued)

25. Understand how security services such as confidentiality, integrity, authenticity, non-repudiation, and access control are addressed through cryptography.
26. Understand basic cryptography concepts of symmetric and asymmetric.
27. Describe hashing algorithms and digital signatures.
28. Understand the importance of key management.
29. Understand cryptanalysis methods.
30. Apply security principles to site and facility design.
31. Implement and manage physical security controls.

Domain Objectives (continued)

32. Implement and manage physical controls in wiring closets and intermediate distribution facilities.
33. Implement and manage physical controls in server rooms and data centers.
34. Implement and manage physical controls in media storage facilities.
35. Implement and manage physical controls for evidence storage.
36. Implement and manage physical controls in restricted areas.
37. Implement and manage physical controls in work areas.

Domain Objectives (continued)

38. Implement and manage environmental controls for utilities and power.
39. Implement and manage controls for heating, ventilation, and air conditioning (HVAC).
40. Implement and manage environmental controls.
41. Implement and manage environmental controls for fire prevention, detection, and suppression.

Domain Agenda

- Processes Using Secure Design Principles
- Fundamental Concepts of Security Models
- Select Controls Based upon Systems Security Requirements
- Security Capabilities of Information Systems
- Vulnerabilities of Security Architectures, Designs, and Solution Elements

Domain Agenda (continued)

- Cryptography
- Physical Security
- Domain Review

Module 1

Processes Using Secure Design Principles

Module Objectives

1. Implement engineering processes using secure design principles.
2. Manage engineering processes using secure design principles.

System and Security Engineering Processes

- Commonly accepted sources for engineering processes:
  - International Council on Systems Engineering (INCOSE)
  - NIST SP800-160 System Security Engineering
  - ISO/IEC 15026 series-Systems and Software Engineering
  - ISO/IEC/IEEE 15288 Systems and Software Engineering
- Systems and systems security engineering processes have converged across major sources:
  - NIST and INCOSE recognize system security engineering as a specialty engineering function

Technical Processes

- Business and mission analysis process
- Stakeholder needs and requirements definition process
- System requirements definition process
- Architecture definition process
- Design definition process
- System analysis process
- Implementation process
- Integration process
- Verification process
- Validation process
- Transition process
- Operation process
- Maintenance process
- Disposal process

Technical Management Processes

- Project planning process
- Project assessment and control process
- Decision management process
- Risk management process
- Configuration management process
- Information management process
- Measurement process
- Quality assurance process

Enabling Processes

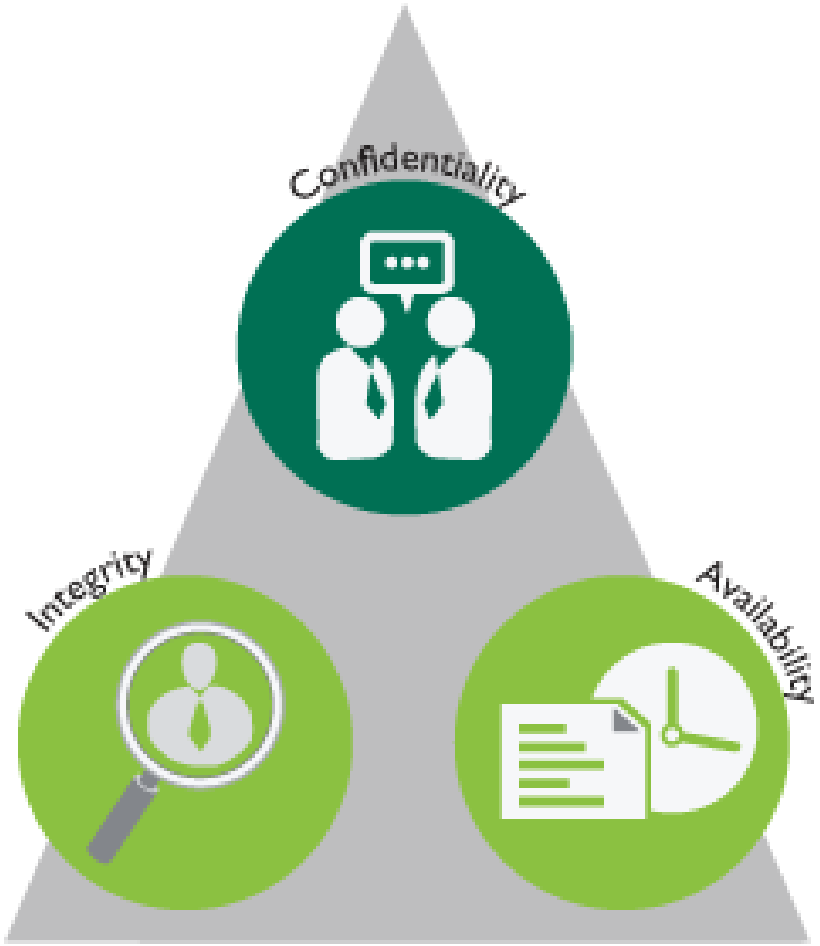
- Lifecycle model management process
- Infrastructure management process
- Portfolio management process
- Human resources management process
- Quality management process
- Knowledge management process

Agreement Processes

- Acquisition process
- Supply process

Key Principles of System Security

- Confidentiality
- Integrity
- Availability



Module 2

Fundamental Concepts of Security Models

Module Objectives

1. Identify the purpose of security models.
2. Identify common security models.

Security Models

Purpose: Security models define rules of behavior for an information system to enforce policies related to system security but typically involving confidentiality and/or integrity policies of the system.

Security Models Examples

- Bell–LaPadula (Confidentiality)
- Biba (Integrity)
- Brewer and Nash (Confidentiality)
- Clark–Wilson (Integrity)
- Graham–Denning (Confidentiality/Integrity)
- Harrison, Ruzzo, Ullman (Integrity)

Bell–LaPadula (BLP) (Confidentiality)

- State machine model
- Developed for Department of Defense (DoD)
- Used for multilevel security (MLS)
- Three properties defined:
  - No read up (simple security property)
  - No write down (star property)
  - Access matrix (discretionary security property)

Biba (Integrity)

- State transition model
- Focus on integrity vice confidentiality
- Opposite direction rules from Bell–LaPadula (BLP)
  - No Read down (simple integrity property)
  - No Write up (star integrity property)
  - Lower level process cannot request higher access (invocation property)

Brewer and Nash (Confidentiality)

- Designed to prevent conflict of interest
- Information flow control model
- Decomposes a company's information into discrete datasets based on potential conflicts of interest
- Defines rules for acceptable access to data objects by a particular subject (e.g., person or process)
- Accessing a data object excludes future access to potential conflict of interest objects

Clark–Wilson (Integrity)

- Introduces the concept of triples:
  - Subject
  - Program
  - Object
- Subjects can only manipulate data objects through the use of a defined program
- Set of rules designed to ensure data integrity for all operations

Graham–Denning (Confidentiality/Integrity)

- Set of rules for creation, assignment of access rights, and deletion of objects and subjects
- Eight rules (create/delete object/subject, assign: read, grant, delete, and transfer access rights)
- Often used in distributed systems

Harrison, Ruzzo, Ullman (HRU) (Integrity)

- Primarily for protection of access right integrity
  - Confidentiality is protected by access rights, so HRU does provide secondary confidentiality protection
- Extends Graham–Denning model
- Defines a set of primitive allowable operations involving subjects and objects

Modern Implementation

- Various components of security models are integrated into modern operating systems (OSs).
- The access control mechanisms discussed in Domain 5 implement key features of the security model in practical systems.
- Security models may not be implemented exactly in modern systems, but they provided the basis for most modern security implementation.

Module 3

Select Controls Based upon System Security Requirements

Module Objectives

1. Differentiate between security requirements and security controls.
2. Identify types of controls.
3. Identify common or inheritable controls.
4. Select appropriate security controls.
5. Identify major control frameworks.
6. Tailor security controls.
7. Identify security control evaluation criteria.

Security Controls

- Safeguards or countermeasures that mitigate risks to confidentiality, integrity, or availability in a system or operating environment.
- Controls may impact or modify the behavior of people, process, or technology.

Types of Controls

Control Action Types:

- Preventive controls:
  - Reduce likelihood or impact of an undesirable event occurring
- Detective controls:
  - Identify an undesirable event or collect information about it
- Corrective controls:
  - Reduce or eliminate the impact of an undesirable event that has occurred

Means of Application:

- Management:
  - Policy- or human-driven controls
- Operational:
  - Process-driven controls
- Technical
  - Controls applied to technology

Common/Inheritable Controls

- Common or Inheritable controls exist outside of a particular system but provide some confidentiality, integrity, or availability protection to the system
  - For example, enterprise firewall protections are inherited by systems behind the firewall
- May include management, operational, or technical controls

Control Selection

- Controls are selected to support the confidentiality, integrity, and availability needs of the system.
- Control frameworks are often utilized to select appropriate controls and define controls.
- Inheritable controls that support the system are identified.

Control Frameworks

- Control frameworks define controls and control elements.
- Frameworks allow for standardization of control implementation.
- Control frameworks often include evaluation criteria or mechanisms to verify controls are effective.

Example Control Frameworks and Standards

- ISO/IEC 27001
  - International Standard
- NIST (SP 800-53)
  - Required for US government use
- COBIT
  - Focused on business values
- ISA/IEC 62443 (ISA 99)
  - Industrial Automation and Control Systems

Tailoring Controls

- Control frameworks and standards are intended to be tailored to specific use-cases.
- Adjust control specifications or parameters to meet the needs of a specific system or environment.
- "Book" controls must be tailored to provide optimal value.

Important:
Controls are not intended to be checklist items but some organizations treat them as such.

Evaluation Criteria

Each control should include specific evaluation methods and expected results.

- Example evaluation methods from NIST:
  - Test: conduct a direct test of the control (usually used for technical type controls)
  - Interview: Interview or question staff (usually used for management or operational controls)
  - Examine: Examine documentation or artifacts for evidence that a control is properly employed (used for all control types)
- Controls may be evaluated by multiple methods

Module 4

Security Capabilities of Information Systems

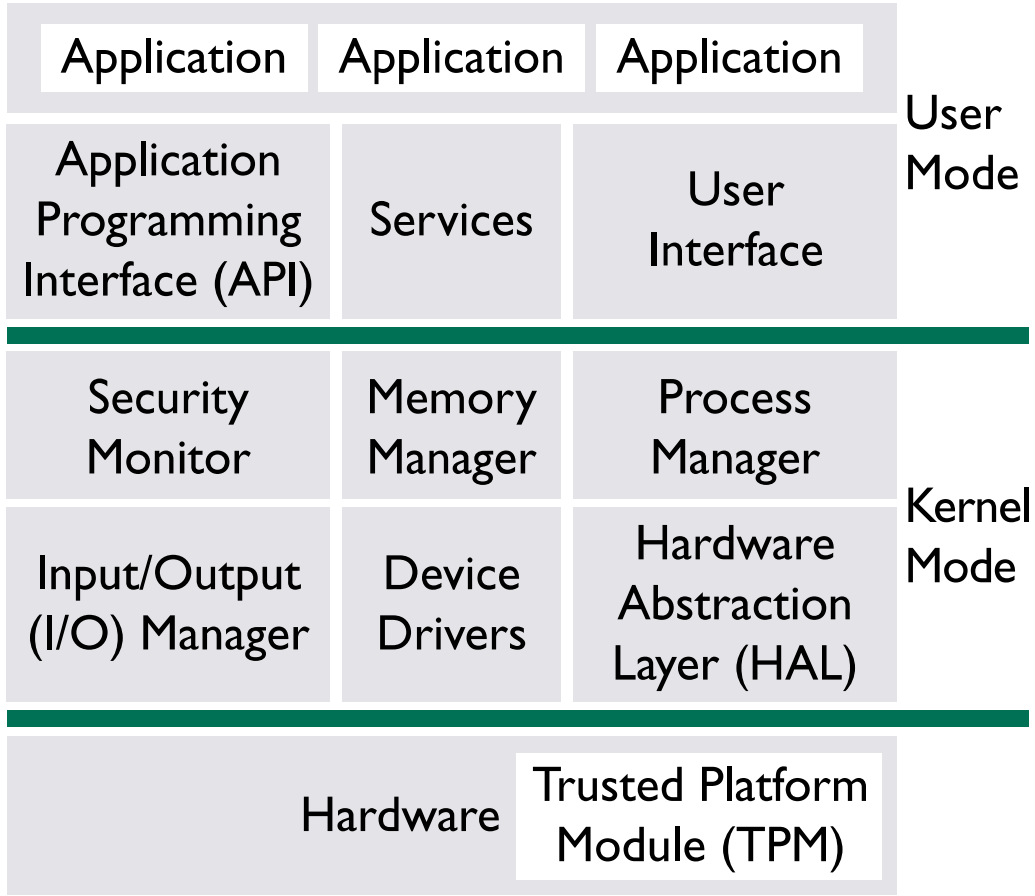
Module Objectives

1. Identify types of system security capabilities.
2. Employ integrated security elements.

System Security Capabilities

- Access control
- Processor states
- Memory management
- Process isolation
- Data hiding
- Abstraction layers
- Security kernel
- Encryption
- Code signing
- Audit and monitoring
- Virtualization/sandbox
- Hardware security Modules
- File system attributes

Generic Operating System (OS)/Computer Model



Access Control

- OS controls access to objects
- Rules define allowable behavior
- Security monitor or reference monitor enforces allowed behavior
- File systems typically support by assigning security attributes to objects/files
- Access control models are described in detail within Domain 5

Processor States

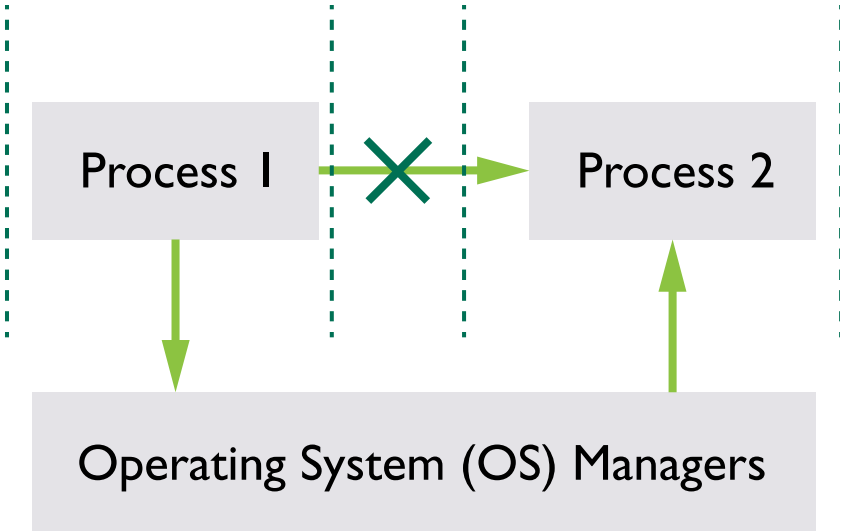
- Processors typically support at least two states of operation:
  - User mode
  - Kernel mode
- User mode has limited access to core functions or direct hardware access

Memory Management

- Direct application access to system memory is restricted
- Modern operating systems randomize memory locations (address space)
- Modern operating systems limit memory locations where code can execute
  - E.g., Data Execution Prevention (DEP) in Windows

Process Isolation

- Processes execute in separate memory spaces
- Direct exchange between processes is limited
- Operating system (OS) manages inter-process exchanges through controlled interfaces

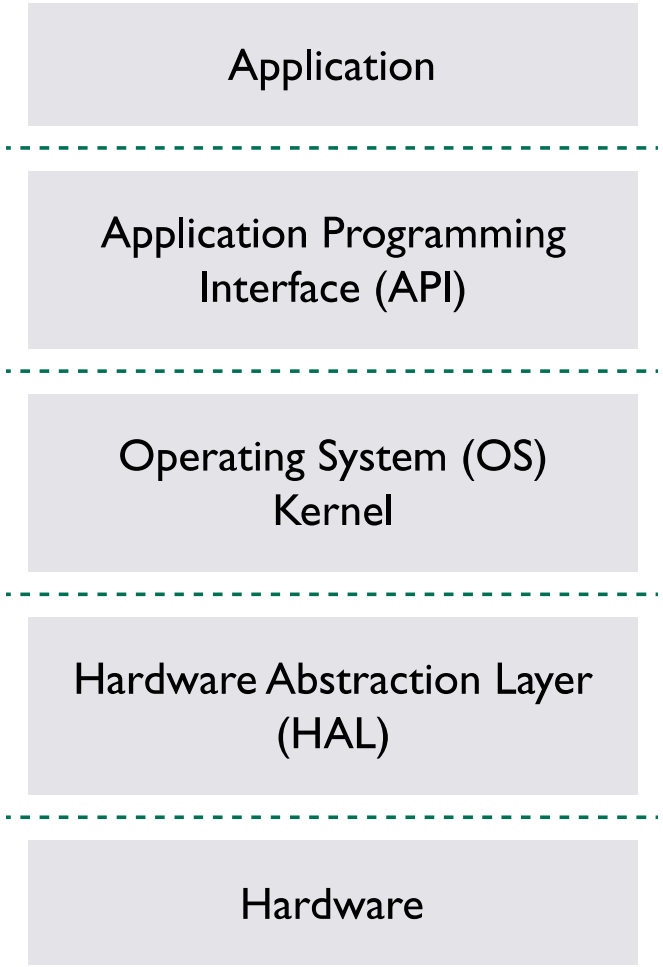


Data Hiding

- Typical with multilevel security (MLS) architectures using mandatory access control (MAC)
- Data or objects at a higher security level cannot be seen by objects at a lower security level
  - Associated to the Bell–LaPadula (BLP) security model
- Also a coding practice where raw data is hidden from access and can only be obtained from a standardized interface

Abstraction layers

- Limits direct access to objects or entities
- Defines allowable actions and interactions between layers
- Protects against improper behavior or access between layers



Security Kernel

- Also known as a reference monitor
- “Big Brother” of kernel mode
- Monitors and validates access control over system objects (e.g., files, network stack)
- Enforcement and validation component of all secure operating systems

Encryption

- Encryption can be applied to data at rest (e.g., files on hard drive) or data in transit (e.g., communication channel)
- May protect confidentiality and/or integrity of data
- Data cannot be read without the proper decryption key
- Protects data when OS features (e.g., security kernel) are not active or present
  - E.g., Windows Bitlocker protects data when the OS is not running and an attempt is made to physically remove and read the computer hard drive

Code Signing and Validation

- Cryptographic function
- Executable code is digitally signed
- OS validates signature before loading code
- Unsigned code or code with an invalid signature is prevented from executing
- May include OS internal code to prevent replacement of OS components

Audit and Monitoring

- System actions are recorded and stored in a protected location
  - Audit storage protection levels vary by system and must be enabled and validated
- Specific actions that are recorded are typically customizable
- Audit records MUST be reviewed or monitored to be an effective protection
- Monitoring and review may include both automated and manual elements
- Audit records are typically transferred off of a system for protection and long term storage

Virtualization/Sandbox

- Executing code is “wrapped” in a virtualization or sandbox layer
- Code executing within the environment is strictly limited from direct interaction outside the environment
- Permissions for system access may be restricted independently for each virtualized or sandboxed instance
- May be an OS native function or function provided by third-party software

Hardware Security Modules

- Hardware components that provide security services
- Trusted Platform Module (TPM)
  - Most common security module, present in most modern hardware platforms
  - Provides secure storage and cryptographic functions
  - Typically used to securely generate and store encryption keys
  - Keys or stored data cannot be extracted from the module without appropriate permissions
- Specialized devices (e.g., cell phone) may contain multiple hardware security modules

File System Attributes

- Various file systems may store security attributes or provide security functions
- A critical component to employing access control models in most operating systems
- File systems may include journaling that can protect data integrity

Host Protection Software

- Antivirus
- Host-based intrusion prevention (HIPS)
- Host firewall
- File integrity monitoring (FIM)
- Configuration and policy monitor

Module 5

Vulnerabilities of Security Architectures, Designs, and Solution Elements

Module Objectives

1. Identify vulnerabilities and mitigations in client-based systems.
2. Identify vulnerabilities and mitigations in server-based systems.
3. Identify vulnerabilities and mitigations in database systems.
4. Identify vulnerabilities and mitigations in Industrial Control Systems (ICS).
5. Identify vulnerabilities and mitigations in cloud-based systems.
6. Identify vulnerabilities and mitigations in distributed systems.
7. Identify vulnerabilities and mitigations in Internet of Things (IoT).

Module Objectives (continued)

8. Assess and mitigate vulnerabilities in web-based systems.
9. Assess and mitigate vulnerabilities in mobile systems.
10. Assess and mitigate vulnerabilities in embedded systems.

Vulnerabilities of Security Architectures, Designs, and Solution Elements

- This module introduces some common vulnerabilities and mitigation approaches
  - These are common among most system types
- It presents typical vulnerabilities and mitigation approaches for various system types
  - The vulnerabilities and mitigations are not intended to be comprehensive for each system type
- For each system type, consider which common vulnerabilities might exist in the various system components

Top Threat Actions/Mitigations

Top Threat Actions

- Hacking
- Social engineering
- Malware distribution
- Phishing

Top Mitigations

- Know what you have
- Patch and manage what you have
- Assess/monitor/log
- Educate users

Common System Vulnerabilities

Hardware

- Hardware components may fail at any time
  - Mean time between failure (MTBF) used to calculate expected life
  - Failure rates higher during initial system operation
- Supply chain issues may introduce technical flaws/vulnerabilities or malicious modification
- Old hardware may be difficult to repair/replace

Common System Vulnerabilities (continued)

Communications:

- Can fail
- Can be blocked (denial of service (DoS))
- Can be intercepted
- Can be counterfeited (replayed)
- Can be modified
- Characteristics can expose information about the sender/receiver (e.g., address, location, etc.)

Common System Vulnerabilities (continued)

Misuse by user

- Can be intentional or accidental
- Can degrade or bypass security controls
- Increases in likelihood as difficulty to operate increases
  - E.g., difficult security requirements increase likelihood of intentional misuse to “get the job done”

Common System Vulnerabilities (continued)

Code flaws

- Exist in all software products with more than trivial complexity
- May be introduced accidentally or intentionally
- Typical risk conditions:
  - Known flaws, patch available, systems not patched, exploit available
  - Known flaws, patch not available, exploit available
  - Unknown flaws, exploit available (zero-day attack possible)

Common System Vulnerabilities (continued)

Emanations

- Hardware/physical elements may radiate information
  - Radio frequency
  - Visible and non-visible spectrum
- Can be used to discern system functions
- Can be used to locate systems/components

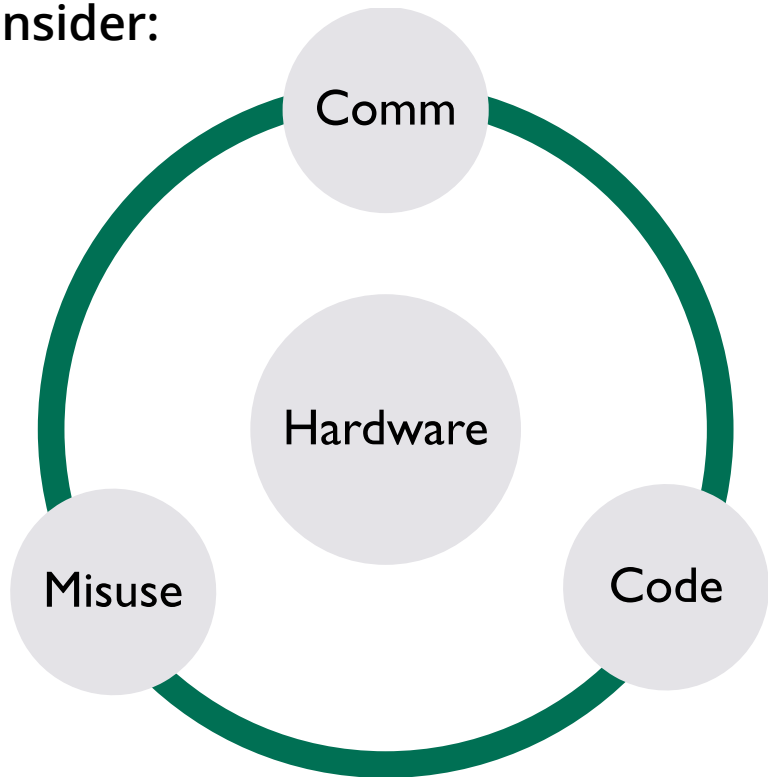
Client-based Systems

- Desktops, laptops, thin client terminals, etc.
- Typically present in large quantities
- Continuous state of adding new and decommissioning old in most organizations
- General purpose devices with inconsistent usage patterns across the install base

Client-based System Vulnerabilities

- Physically under user control
- Susceptible to user misuse (intentional or accidental)
- May be lost/stolen
- Monitoring may be difficult
- 100% update may be difficult

Consider:



Client-based System Mitigations

- Patch/update*: Continuous action
- General network protections: e.g. Network segmentation, firewall devices, network intrusion prevention or detection
- Host protections*: Antivirus, host IPS, host firewall, disk encryption
- Monitor*: Logs, alerts, track location
- Educate users: Anti-phishing campaign, detecting attacks

*Applied to all general purpose computing systems-servers, database, distributed, cloud-based, web-based

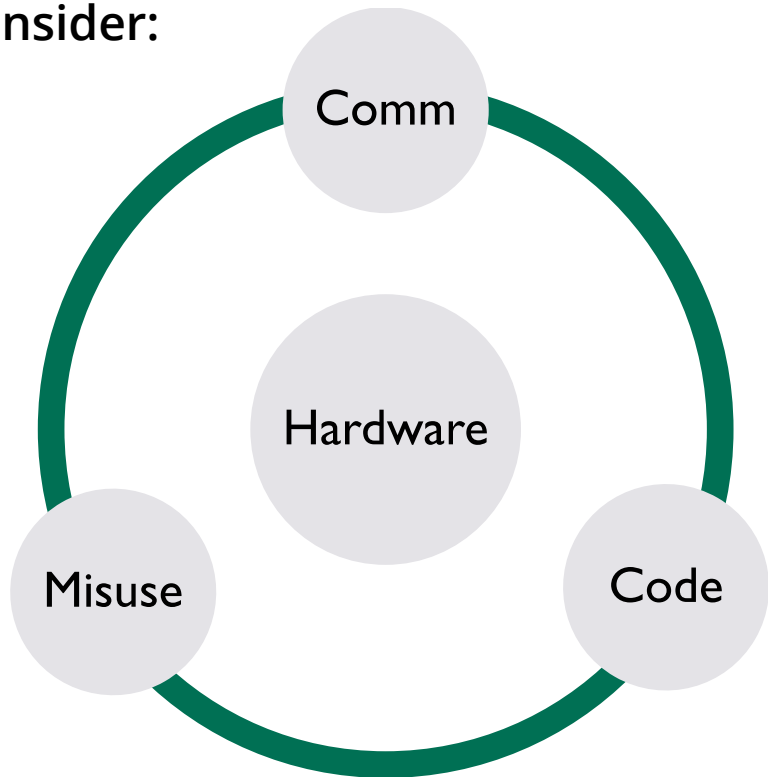
Server-based Systems

- Application servers, file servers, domain controllers, print servers, network service servers (e.g., DNS, DHCP, etc)
- Centrally managed/controlled
- Limited access/functionality
- Likely to be in a tightly controlled network segment

Server-based System Vulnerabilities

- May be exposed to external communication/services
- Updates may be delayed due to operational need
- May exist for long periods (risk of being outdated)
- High-traffic volume makes monitoring more difficult

Consider:



Server-based System Mitigations

- Targeted network protections (server specific rules, restricted ports/protocols)
- Strong remote access mechanisms
- Configuration and change management
- Monitor: Logs, alerts—targeted to server functions

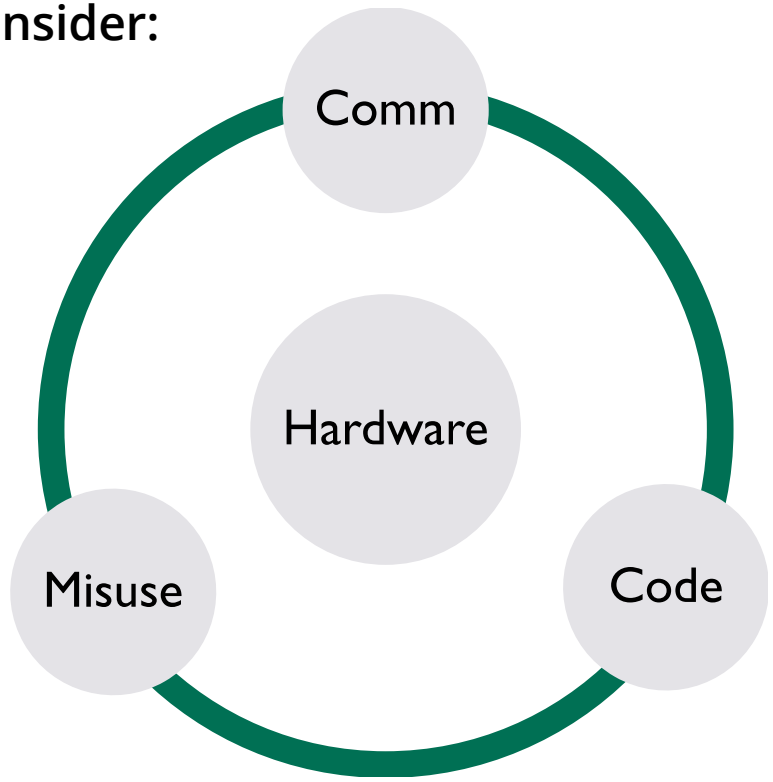
Database Systems

- Hosted on servers, cloud, distributed, etc.
  - Inherits platform vulnerabilities
- Typically contains large quantities of valuable information
- Typically requires high-speed operation with large number of transactions

Database System Vulnerabilities

- Inference
- Aggregation
- Data mining
- High-value target

Consider:



Database System Mitigations

- Input validation
- Robust authentication/access control
- Output throttling
- Anonymization
- Tokenization

Industrial Control Systems (ICSs)

- Typically embedded, limited function hardware
- Interfaces between logical (computer) space and the physical world
- Includes sensors, motors, actuators, valves, gauges, etc.

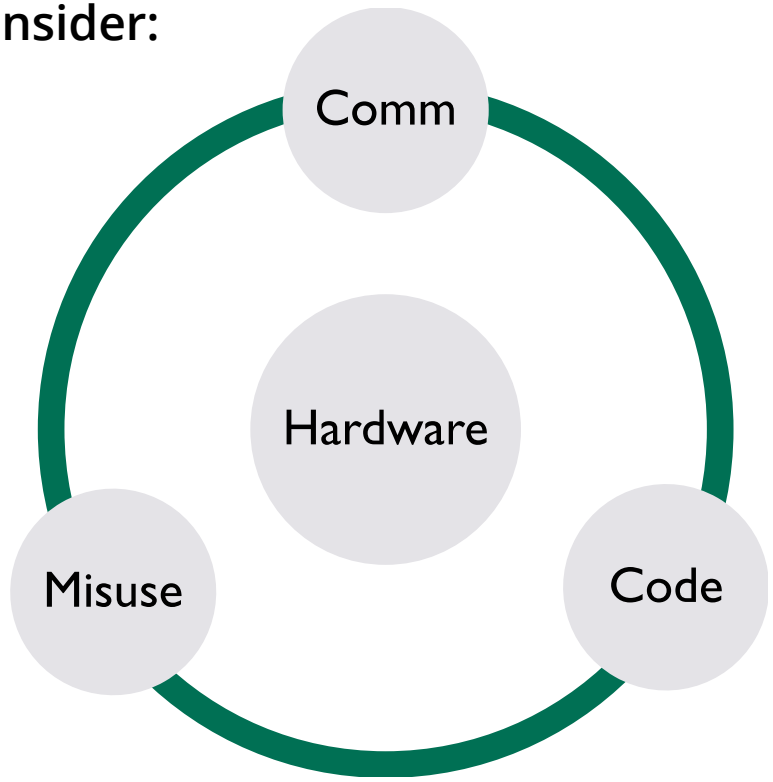
Industrial Control System Types

- Supervisory control and data acquisition (SCADA)
- Distributed control systems (DCSs)
- Programmable logic controllers (PLCs)

Industrial Control System Vulnerabilities

- Limited functionality
- Limited protections
- Long lifespan (become outdated)
- Susceptible to misuse/error
- Highly susceptible to denial of service (DoS) attacks
- Attacks can produce physical effects
- Often unattended in remote locations

Consider:



Industrial Control System Mitigations

- Isolated network infrastructure
- Robust network connection restrictions and monitoring
- Highly segmented network
- Protect communication channels
- Robust configuration control

Cloud-based Systems

- Components hosted by a cloud service provider (CSP)
- CSP assumes specific security responsibilities, the remainder stay with the data owner
- Typically high reliability, speed, capacities
- CSP to data owner relationship is governed by a contract and/or service-level agreements (SLAs)

Cloud-based System Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service
- Multi-Tenancy

Cloud-based System Types

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)
- Network as a service (NaaS)

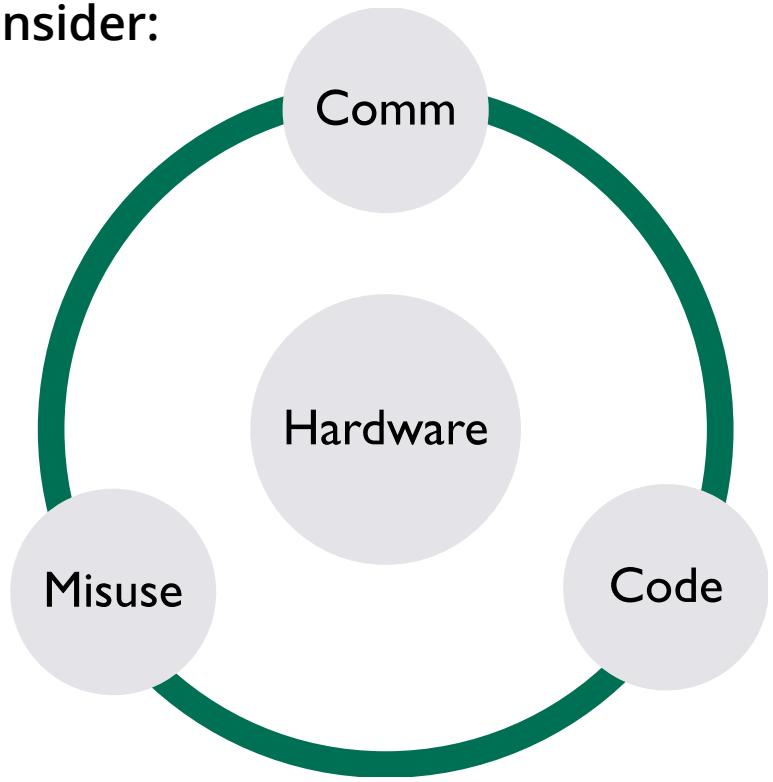
Cloud-based System Deployment

- Private
  - Exclusive use by a single organization
  - On or off premises
- Community
  - Provisioned for exclusive use by a community of users
- Public
  - Open use by general public
- Hybrid
  - Combination of two or more deployment models

Cloud-based System Vulnerabilities

- Inherently exposed to external communication/access
- Misconfiguration a major risk
- May exist for long periods (risk of being outdated)
- Gap between CSP and data owner security controls

Consider:



Cloud-based System Mitigations

- Reputable cloud service provider that supplies security information/testing results
- Well trained system administrators
- Robust configuration control/change control
- File and communication encryption
- Well managed identity and access controls

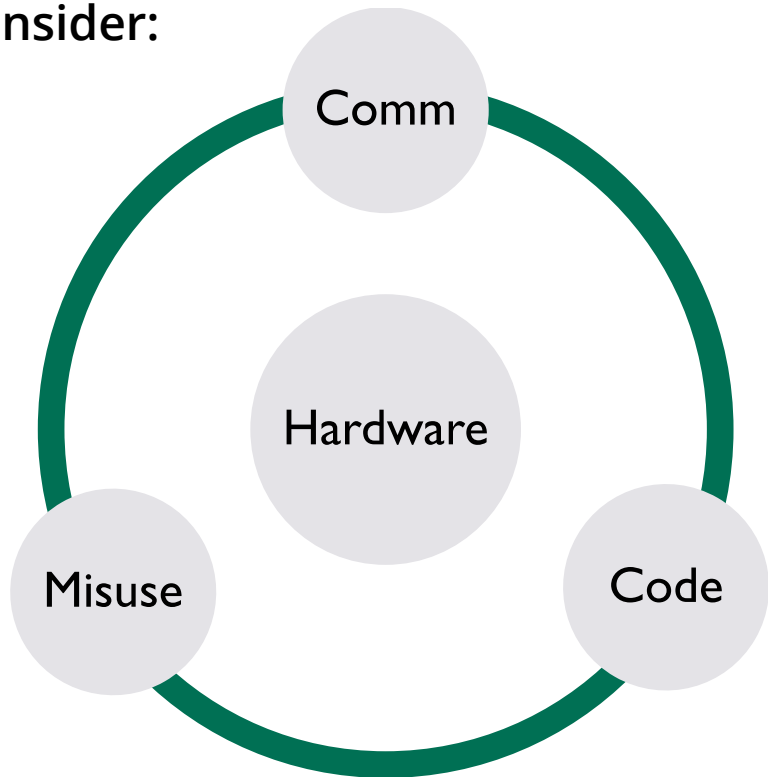
Distributed Systems

- Nodes and processors operate independently
- Storage and processing spread across multiple components
- Nodes "pass messages" to coordinate and communicate
- Example: traditional telephone
  - Switches operate independently
  - Coordinate to pass calls between them

Distributed System Vulnerabilities

- Lack of central control/monitoring
- Data elements may be lost if nodes fail
- Inconsistent security levels between nodes is possible
- Susceptible to communication failures, compromise, or denial of service (DoS)

Consider:



Distributed System Mitigations

- Standard security rules for nodes to enter distributed network
- Communication control, encryption, and redundancy
- Node backup and data sharing between nodes

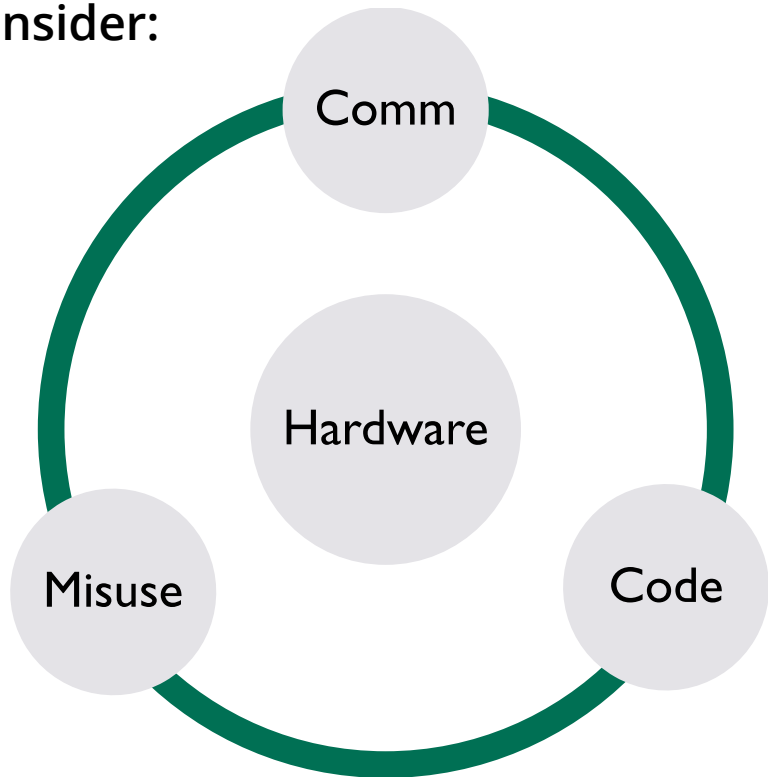
Internet of Things (IoT) Systems

- Generally small form factor, embedded hardware
- Limited functionality OS
- May interface with the physical world
- Pervasive and often connected to general purpose networks
- Functions/accessibility may be unclear to owner/user

Internet of Things (IoT) Vulnerabilities

- Limited vendor support for updates
- Little to no onboard security capability
- Poor code management due to rapid development cycles
- May contain limited or weak security implementations on standard protocols (e.g., Bluetooth, WiFi)

Consider:



Internet of Things (IoT) Mitigations

- Isolated on private networks with controlled access
- Products selected for security features and updatability
- Product security/penetration testing
- Disable unneeded functions

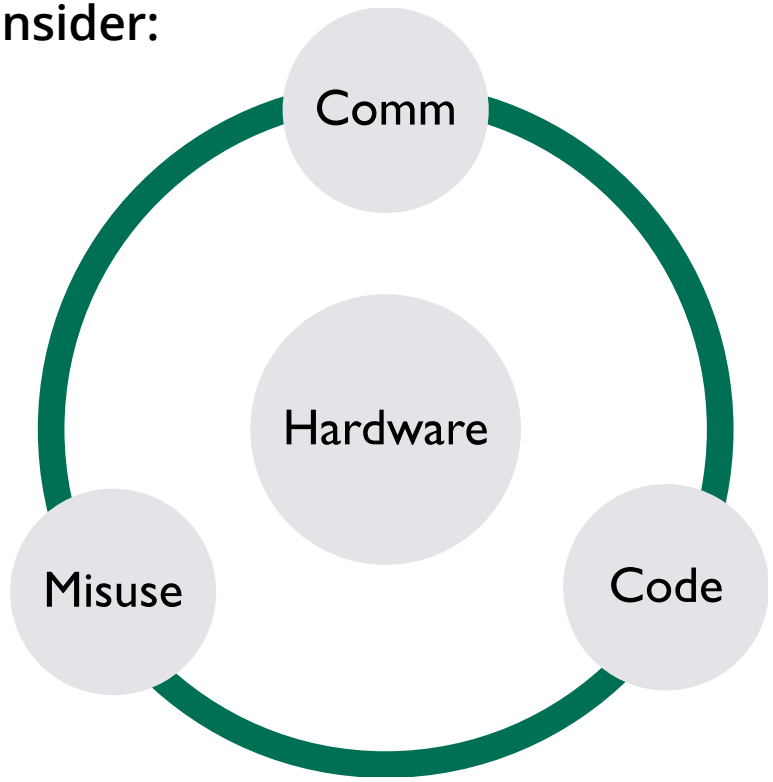
Web-based Systems

- Applications or data accessible and manipulated through a web browser or web service
- Often connects to a data source (database) that may be on or off platform
- Uses standard protocols and interface languages
- Connections are typically dynamic

Web-based System Vulnerabilities

- Accessibility to network communications/access
- Use of obsolete protocols/encryption
- Code/configuration errors that expose components or data

Consider:



Web-based System Mitigations

- Protect system behind firewalls and access controls
- Limit and monitor communication protocols
- Scan, evaluate, and assess interfaces and code (HTML, Java, scripts, etc)
- Tightly control configuration and change management
- Ensure platform is security configured

Mobile Systems

Phones, tablets, wearable devices

- Portable, small form factor
- Limited functionality
- Embedded OS
- Typically contains limited amounts of data
- Connected (cellular, WiFi, Bluetooth, tethering)
- Designed for single user

Mobile Systems (continued)

Laptops, personal computers

- Portable, medium form factor
- Full featured operating system
- Capabilities similar to a desktop
- May contain large amounts of data
- Multi-user capable
- Connected (WiFi, Bluetooth, tethering, possibly cellular)

Mobile Systems (continued)

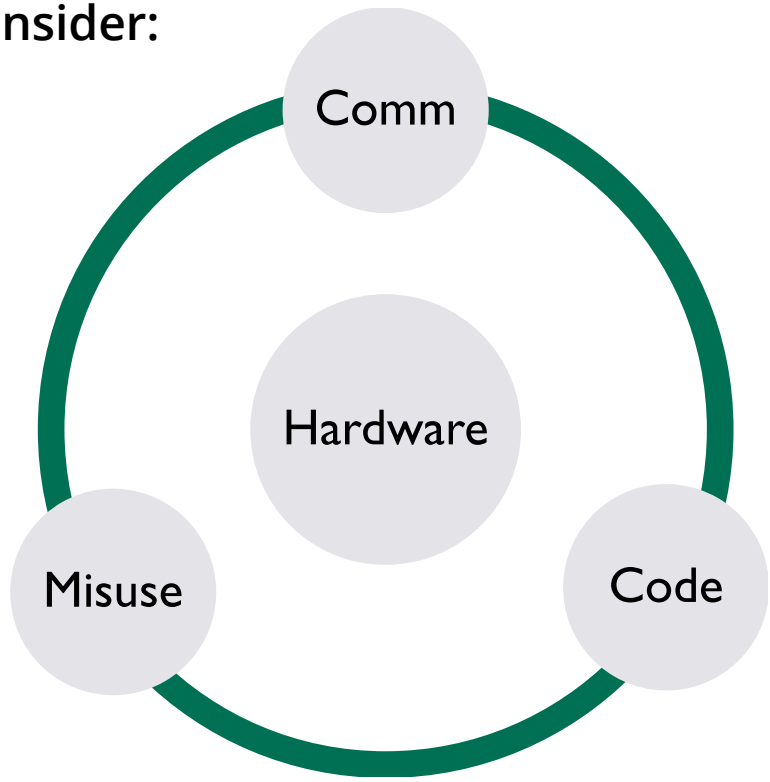
Are laptops mobile systems?

- Opinions may vary, wide gray area depending on the particular capabilities and configuration of a device
- Share physical vulnerabilities with other device types
- Capable of more onboard controls (e.g., traditional computer host protections, logging, monitoring, access controls)
- Mitigation mechanisms are different from other device types
- Some tablets cross the line between laptop characteristics and embedded mobile device characteristics

Mobile System Vulnerabilities

- Loss or theft
- Weak access controls configured
- Unencrypted data
- Communication interception or eavesdropping
- Limited onboard security services and monitoring

Consider:



Mobile System Mitigations

- Mobile device management (MDM) installed
  - Device tracking, wiping, software control, policy enforcement
- Activate screen lock and high complexity passcodes or biometrics
- Ensure device is encrypted
- Tunnel communications through VPN architecture
- Limit software/apps installed to trusted packages
- Prevent jailbreak or rooting devices
- Do not connect to public networks (e.g., coffee shop, hotel)

Mobile System Mitigations (continued)

For laptops:

- Apply all traditional computer system protections (e.g., AV, FW, Host IPS, etc.)
- Ensure encryption is activated
- Ensure strong passwords, biometrics, or two factor authentication on all user accounts
- Activate anti-theft function or tracking functions if available
- Tunnel mobile communications through VPN
- Do not connect to public networks (e.g., coffee shop, hotel)

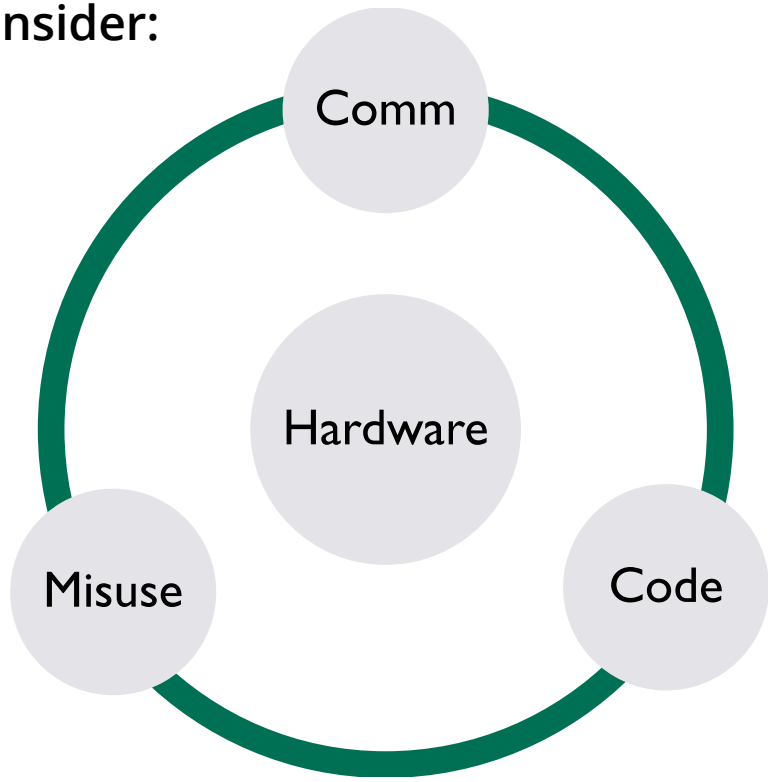
Embedded Systems

- Computing platform with a dedicated function
- Limited function/specialized OS
- Limited processing power
- Long service life in many applications
- Includes System on a Chip (SoC) architectures
- Typically includes special device categories:
  - IoT, ICS, mobile devices
- Highly diverse in nature
  - Specialized computing vs general purpose computing

Embedded System Vulnerabilities

- Limited function design does not include all full monitoring and security control implementation
- Limited access controls
- Limited ability to update, vendor support often time limited

Consider:



Embedded System Mitigations

- Limit access to devices
- Limit communications to devices
- Disable unnecessary/unneeded components/features/communications
- Isolate on dedicated networks if connected
- Monitor external communications with exterior sensors (e.g., network taps, sensors)
- Apply vendor updates when available

Activity: Designing Security into an Architecture Scenario

The National Federal Amalgamated Corporation (NFAC) is developing a new customer facing application for amalgamated data. The initial design includes the following elements:

- Database servers within the NFAC data center that store customer private and sensitive data elements
- Application servers within the NFAC data center that access the database servers and are accessed by NFAC employee workstations
- Employee workstations (some desktop, some laptop) are used by NFAC employees to access the Application servers to access, upload, modify, and delete sensitive customer data

Activity: Designing Security into an Architecture Scenario (continued)

- Web servers located with a cloud provider that access NFAC databases and applications to deliver data to external customers through a web browser
- Mobile applications distributed to customers for installation on Android and Apple devices that provide customer access via a Mobile Application Service hosted by the same cloud provider hosting the web servers

Activity: Designing Security into an Architecture-Instructions

INSTRUCTIONS

Consider the scenario and the vulnerabilities, mitigations, and controls discussed in the preceding modules. Each of the system types listed in the scenario have inherent strengths and weaknesses. For each item, identify potential risks or weakness and one or more controls or mitigation consistent with the access requirements listed in the scenario.

Activity: Designing Security into an Architecture- Instructions (continued)

Example:

- Database Servers:
  - Risk: Database servers contain bulk sensitive data and may be targeted by adversaries.
  - Control: Database servers will be placed on a protected network segment and network access controls will prevent access to the database server for any connection except from authorized application servers.

Module 6

Cryptography

Module Objectives

1. Understand key terms associated with cryptography.
2. Understand how security services such as confidentiality, integrity, authenticity, non-repudiation, and access control are addressed through cryptography.
3. Understand basic cryptography concepts of symmetric and asymmetric.
4. Describe hashing algorithms and digital signatures.
5. Understand the importance of key management.
6. Understand cryptanalysis methods.

Cryptography Services

- Confidentiality
- Integrity
- Authenticity
- Non-repudiation
- Access control

Data Protection

Data at Rest

Backup tapes, off-site storage, password files

Data in Transit

Provides secure and confidential methods to transmit data

Allows the verification of the integrity of the message so that any changes to the message itself can be detected

End-to-end Encryption

- Generally performed by the end user within an organization
- The data is encrypted at the start of the communications channel or before and remains encrypted until it is decrypted at the remote end

Link Encryption

- Encrypts all of the data along a communications path
- Communications nodes need to decrypt the data to continue routing

Cryptographic Evolution

Cryptographic techniques:

- Manual
- Mechanical
- Electro-mechanical
- Electronic
- Quantum cryptography

Key Encryption Concepts and Definitions

Plaintext or cleartext	Ciphertext or cryptogram	Cryptosystem	Algorithm
Encryption	Decryption	Key or Cryptovariable	Non-Repudiation
Cryptanalysis	Cryptology	Collision	Key space

Key Encryption Concepts and Definitions (continued)

Initialization vector (IV)	Encoding/decoding
Substitution	Transposition or permutation
Confusion/diffusion Avalanche	Key clustering

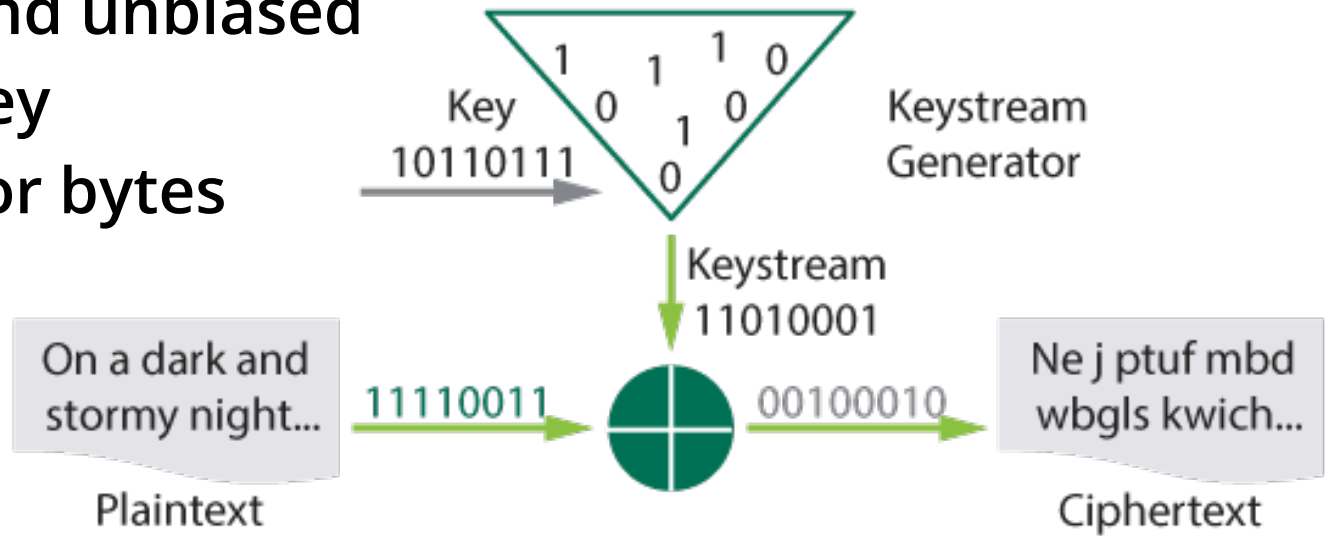
Key Encryption Concepts and Definitions (continued)

Synchronous Each encryption or decryption request is performed immediately	Asynchronous Encrypt/Decrypt requests are processed in queues	Hash function
Digital signatures	Symmetric	Asymmetric
Digital Certificate	Certificate authority (CA)	Registration authority (RA)

Stream-based Ciphers

A keystream (sequence of bits used as a key) is generated and combined with the plaintext using an exclusive-or (XOR) operation:

- Statistically unpredictable and unbiased
- Not linearly related to the key
- Operates on individual bits or bytes
- Functionally complex
- Long periods with no repeats



Cryptographic Operation for a Stream-based Cipher

- Plaintext is XORed with a seemingly random keystream to generate ciphertext
- It is seemingly random because the generation of the keystream is usually controlled by the key

Exclusive-Or (XOR)

Crypto XOR Operation

1 **Convert letters into binary values**

C = ASCII 67
67 Binary = 01000011
A = ASCII 65
65 Binary = 01000001

2 **XOR Values**

```
01000011
01000001
--------
00000010
```

XOR calculation
- Compare two binary values
- If both values are same the output is 0
- If they are different the output is 1

Transmit = 00000010

Block Ciphers

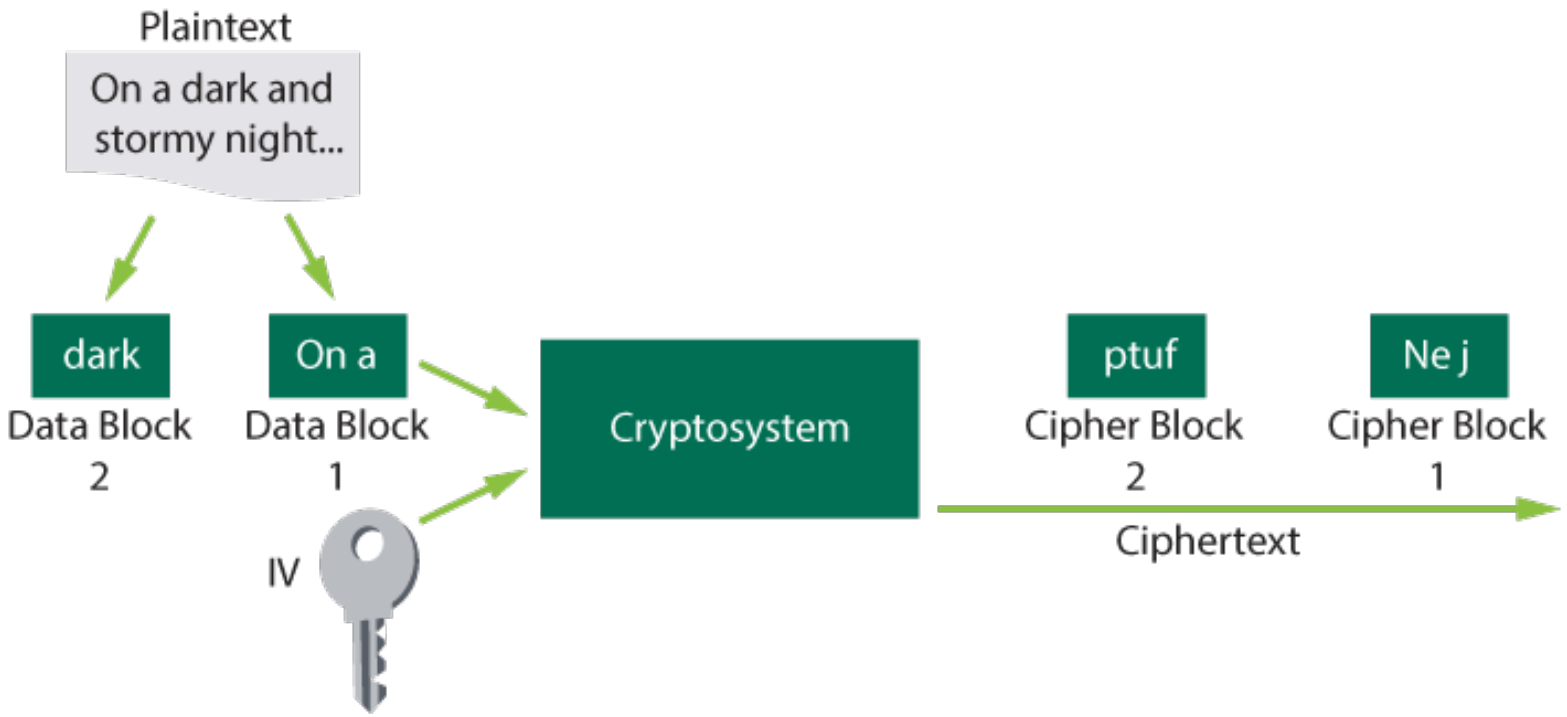
- A block cipher operates on fixed-size blocks of text
- The size of the block affects the strength of the cryptographic implementation
- As plaintext is fed into the cryptosystem, it is divided into blocks of a preset size
- Often a multiple of the ASCII character size — 64, 128, 192 bits, etc.

Block Ciphers (continued)

Operate on fixed size blocks of plain text

More suitably implemented in software to execute on general-purpose computer

Overlap when block operated as stream



Key Length

- Important aspect of key management to consider when generating and using cryptographic keys
- The longer the key, the more keyspace it represents

Block Size

- Block ciphers operate on a fixed length string of bits
- Typically 64 bits, or multiples of 64 bits

Initialization Vectors (IV) – Why They Are Needed

- Encrypting the same plaintext using the same key always produces the same ciphertext
- Encrypting the same message with different keys may produce discernable patterns
- An IV is a random value added to the plaintext message before encrypting so that each ciphertext will be substantially different

Kerckhoff's Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

High Work Factor

- Measured in units such as:
  - Hours of computing time
  - Cost in dollars of breaking the encryption
- If the work factor is sufficiently high, the encryption system is considered to be practically or economically unbreakable

Substitution Ciphers

- The process of substituting one letter for another based upon a cryptovariable
- Involves shifting positions in the alphabet of a defined number of characters (Caesar cipher and Vigenere cipher)
- Involves using a scrambled alphabet to substitute one letter for another (Enigma machine)

Transposition Ciphers

- Cryptosystems that use transposition or permutation
- Rely on concealing the message through the transposing of or interchanging the order of the letters

T	H	I	S	I
S	A	N	E	X
A	M	P	L	E
O	F	T	R	A
N	S	P	O	S
I	T	I	O	N

Rectangular Substitution Tables

Monoalphabetic and Polyalphabetic Ciphers

- Monoalphabetic Cipher
- Polyalphabetic Cipher
  - Developed Circa 15th Century

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
2	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
3	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
4	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
...																										

Encrypt the plaintext 'FEEDBACK' using a key of 3241 CCACYYYJ

Running Key Cipher

- Use the value of plaintext letters and a value of key based on a shared book

Value of Message
'THIS message …'

+ Value of Key
'on periodic …'

= Value of Ciphertext

T	H	I	S
19	7	8	18
O	N	P	E
14	13	15	5
33	20	23	22
-26			
7	20	23	22
H	U	X	W

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

One-Time Pads

- The only cipher system asserted as unbreakable
- Both sides have same pad of key values
  - Truly random key values
  - Keys are only used once

Steganography

- Plaintext hidden/disguised
- Prevents a third party from knowing that a secret message exists
- Traditionally accomplished in a number of ways:
  - Physical techniques
  - Modern steganography
  - Null ciphers

E1089197693F6C4C26E0033F8C8AF00C

57694B77DCB55C543C6C0BA8E1FF2D17

Null Cipher

- Plaintext is mixed with large amounts of non-cipher material
- A simple form of steganography

Example:

Closed inspection specific security process integrate security governance really easily and timely

CISSP is great

Null Cipher – Are You Deaf, Father William, William

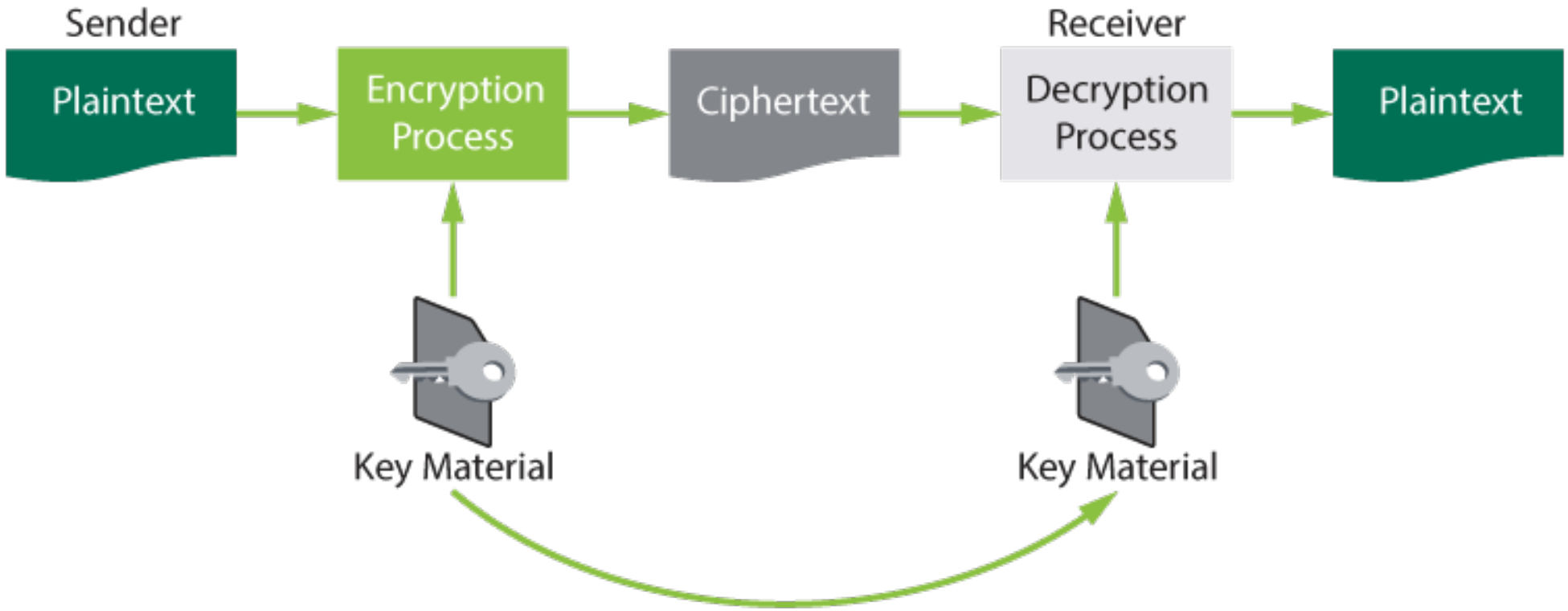
Carroll - 1876

"Are you deaf, Father William!" the young man said,
"Did you hear what I told you just now?
"Excuse me for shouting! Don't waggle your head
"Like a blundering, sleepy old cow!
"A little maid dwelling in Wallington Town,
"Is my friend, so I beg to remark:
"Do you think she'd be pleased if a book were sent down
"Entitled 'The Hunt of the Snark?'"
"Pack it up in brown paper!" the old man cried,
"And seal it with olive-and-dove.
"I command you to do it!" he added with pride,
"Nor forget, my good fellow, to send her beside
"Easter Greetings, and give her my love."

Advantages and Disadvantages of Symmetric Algorithms

Advantages	Disadvantages
• Fast • Secure • Confidentiality	• Key distribution is very difficult • Not able to provide integrity, authenticity, non-repudiation of origin, access control, and digital signatures • Require both sender and receiver to share the same key • Challenges with secure key distribution • Scalability

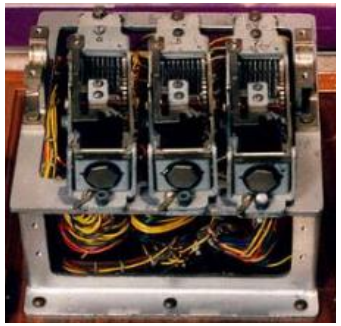
Out-of-Band Key Distribution



Out-of-Band Key Distribution

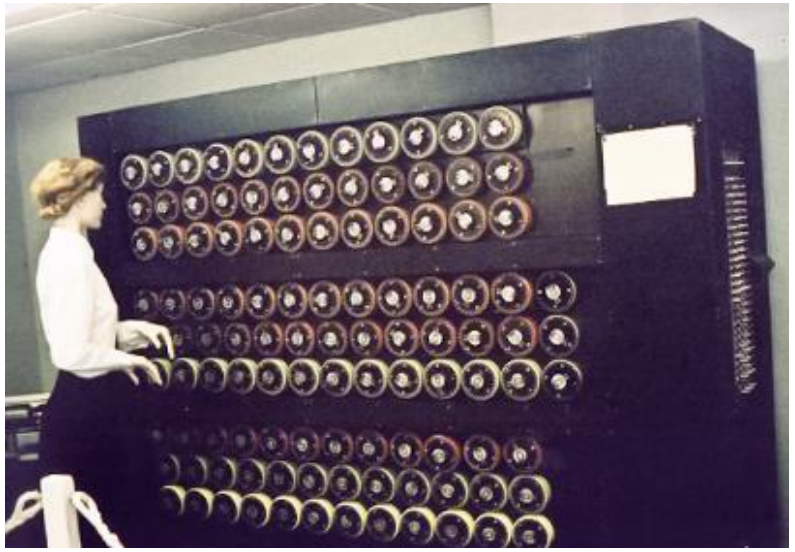
Examples of Symmetric Algorithms

- Caesar cipher
- The Spartan scytale
- The Enigma machine



System 97 Printing Machine for European Characters

Codename “Purple”



Basic Block Cipher Modes

Mode	Usage
Electronic Code Book (ECB)	Very short messages (less than 64 bits in length), such as transmission of a DES key.
Cipher Block Chaining (CBC)	Authentication
Cipher Feedback (CFB)	Authentication
Output Feedback (OFB)	Authentication
Counter (CTR)	Used in high-speed applications such as IPSec and ATM

Basic Block Cipher Modes

- Electronic Codebook (ECB) Mode
- Cipher Block Chaining (CBC) Mode

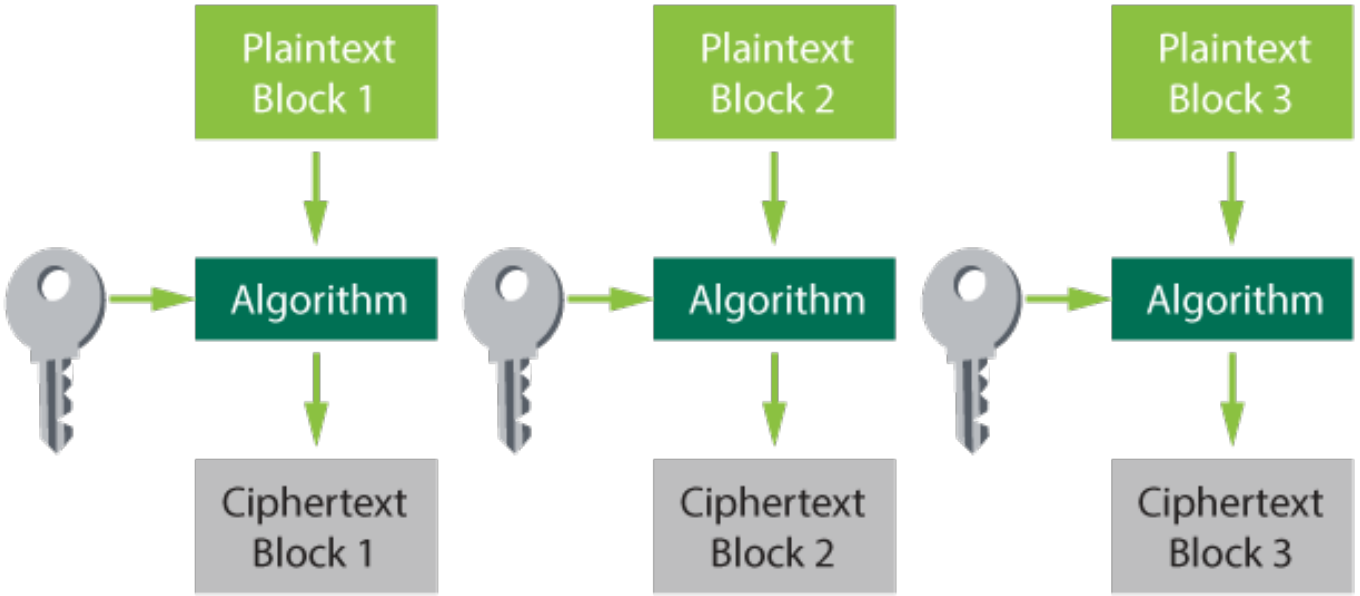
Using Symmetric Block Cyphers to Simulate Stream

Ciphers

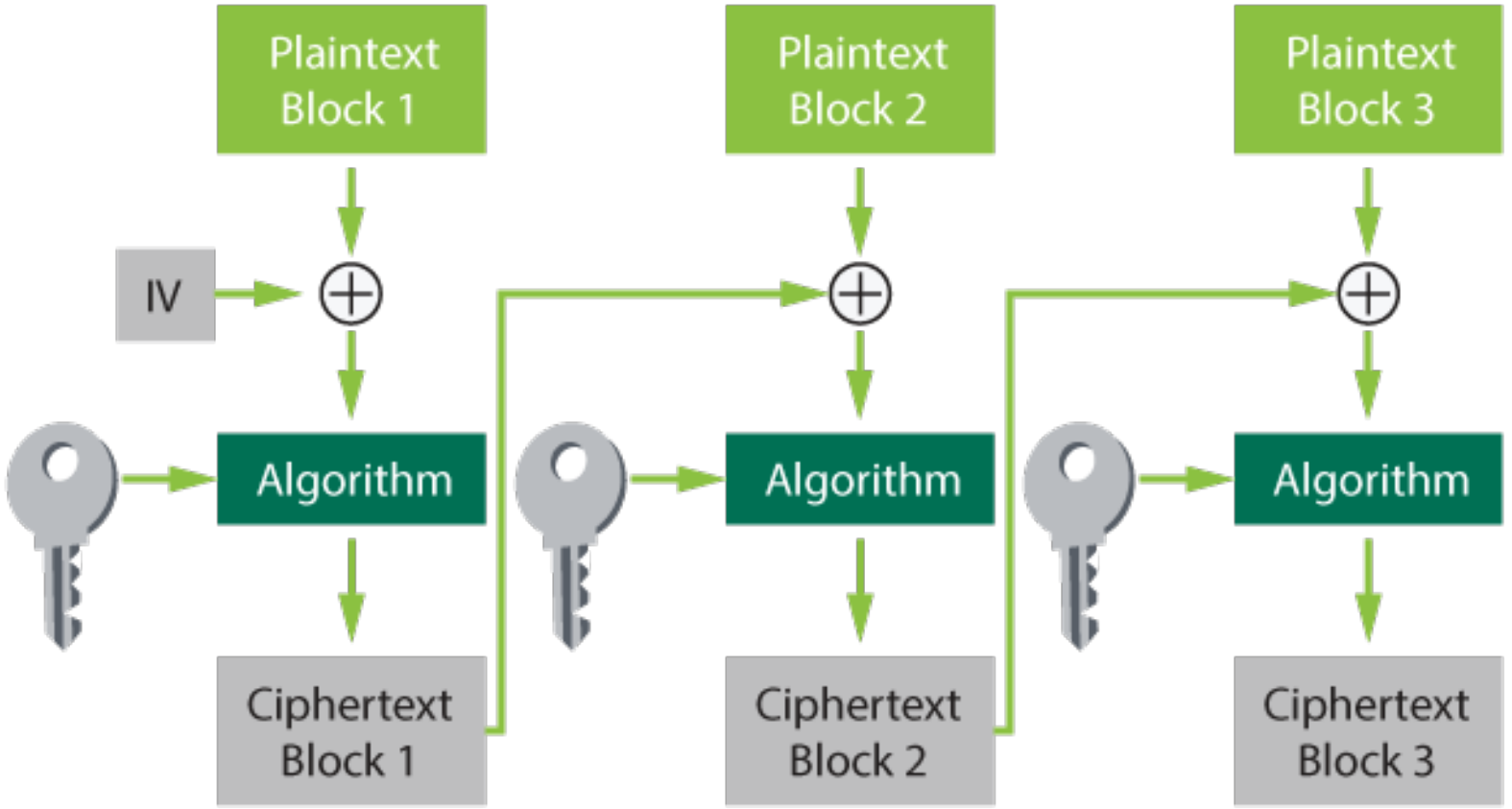
- Cipher Feedback (CFB) Mode
- Output Feedback (OFB) Mode
- Counter (CTR) Mode

Electronic Codebook (ECB) Mode

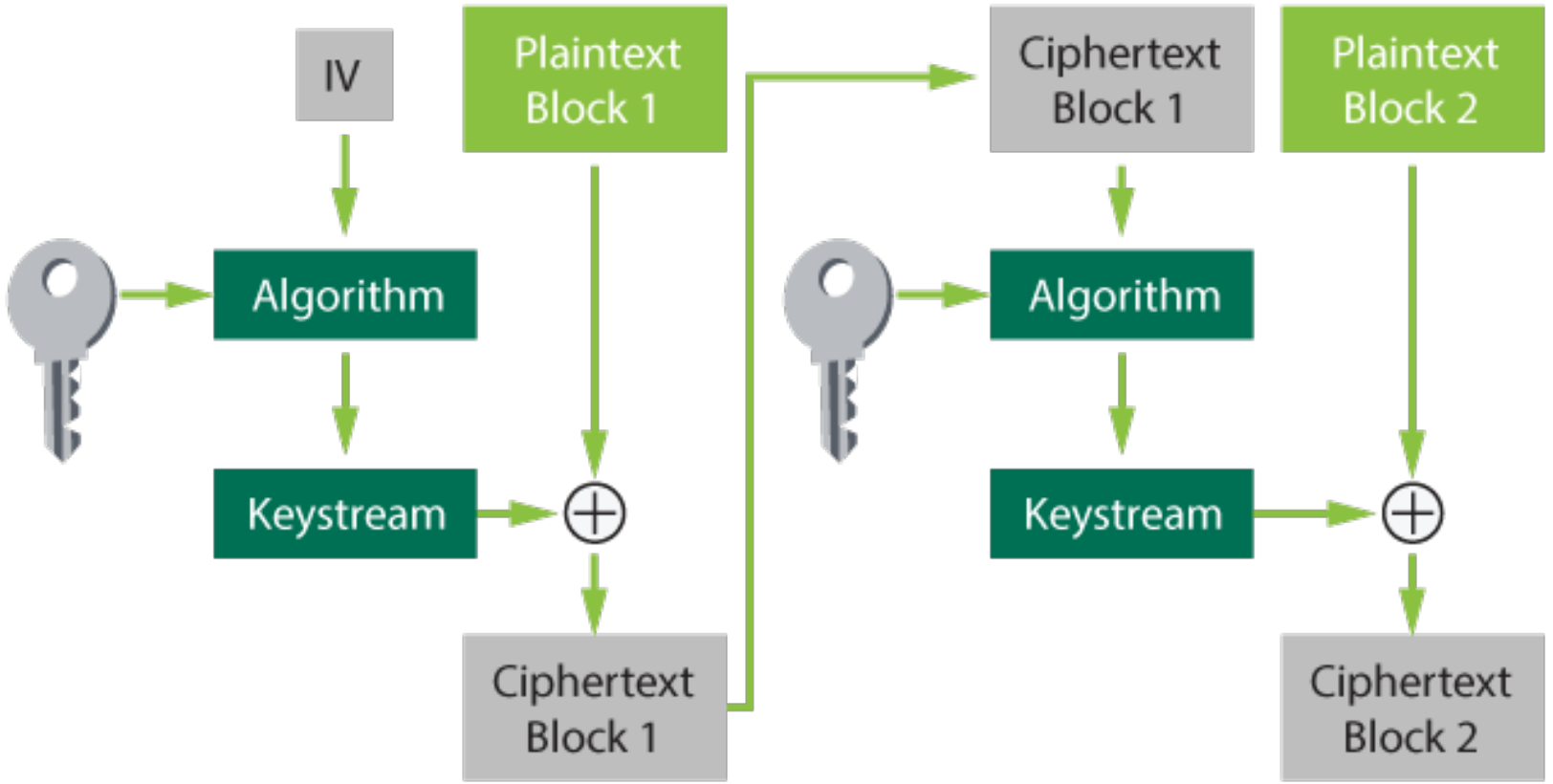
- Each block of plaintext is encrypted independently using the same key
- Only used for small messages – smaller than 64 bits



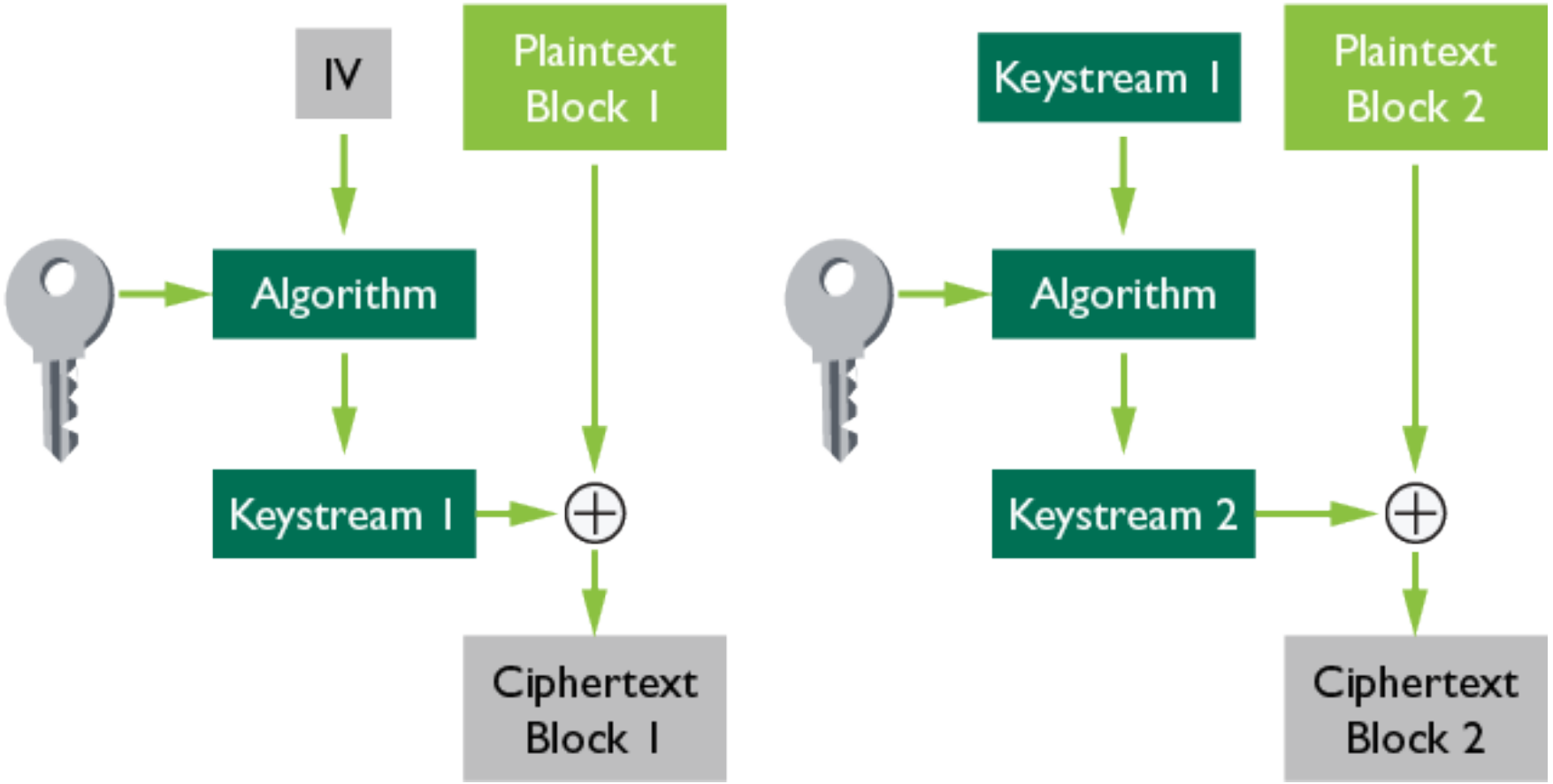
Cipher Block Chaining (CBC) Mode



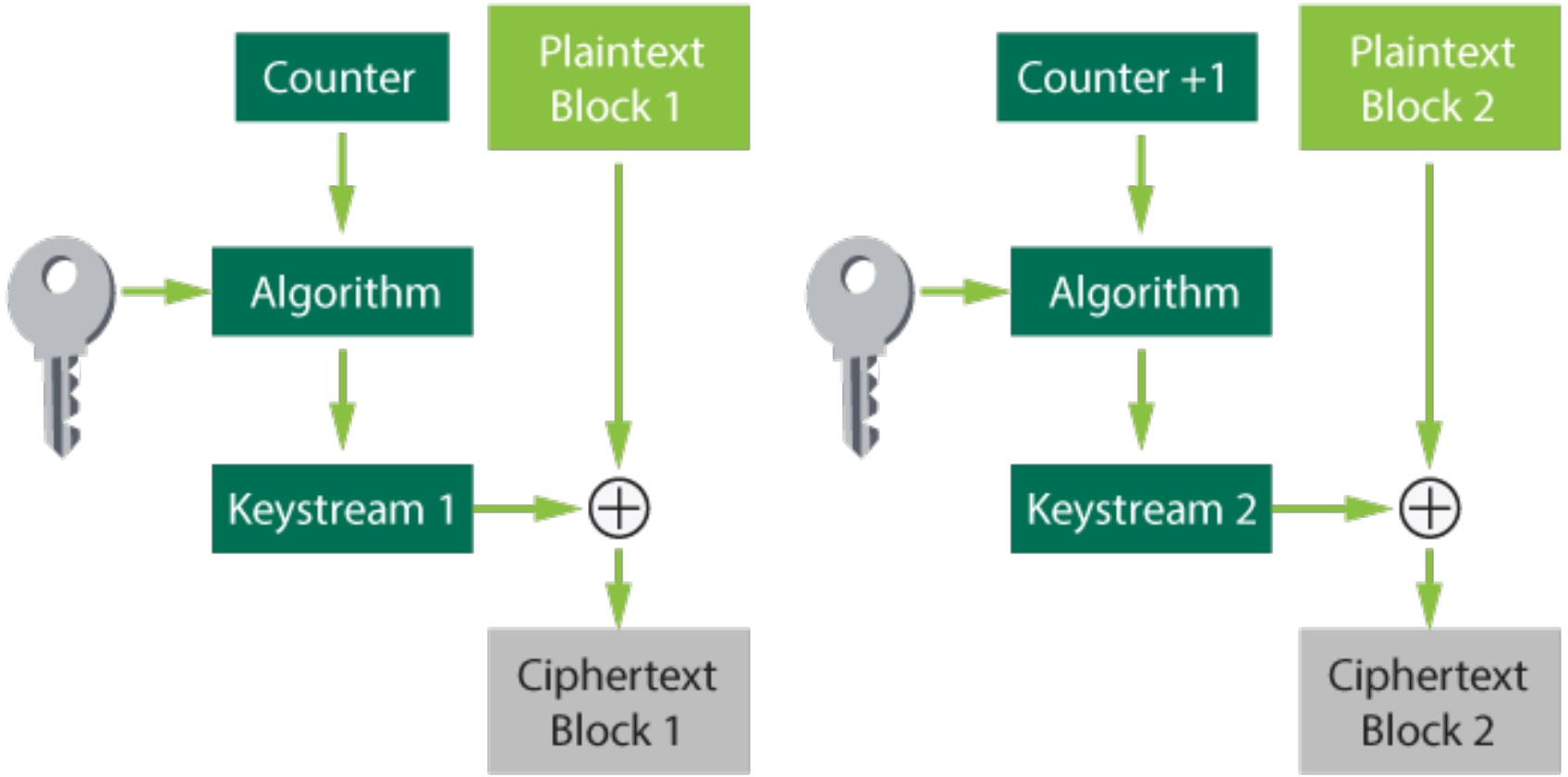
Cipher Feedback (CFB) Mode



Output Feedback (OFB) Mode



Counter Mode (CTR)



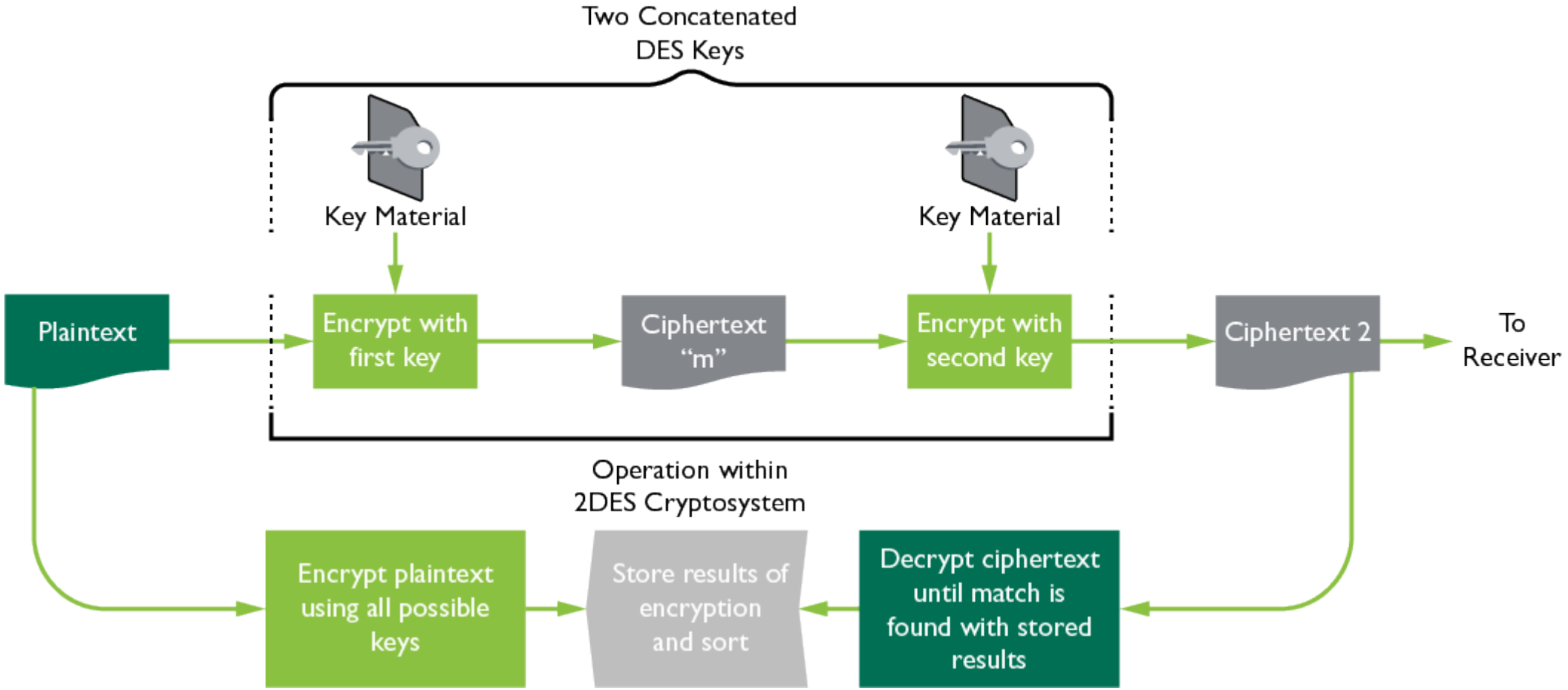
The Data Encryption Standard (DES)

- Horst Feistel had developed a family of algorithms that had a core principle of taking the input block of plaintext and dividing it in half
- Then, each half was used several times through an exclusive-or operation to alter the other half — providing a type of permutation as well as substitution
- A Feistal algorithm became the data encryption algorithm used for DES
- DEA Algorithm is Symmetric Block Cipher, 64-bit blocks, 16 rounds, 56-bit effective key length

Double-DES (2DES)

- Given today's technology, DES key is too short to provide adequate protection
- One of the first alternatives to create a stronger version of DES was to double the encryption process

Meet-in-the-Middle Attack on 2DES



Triple DES (3DES)

- Triple DES was designed to operate at a relative strength of 2^{112} using two, or three, different keys to perform the encryption
- This effectively rendered a key with a 168-bit strength, as there are always three iterations done with the keys

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

CCMP is an authentication protocol that forms part of the 802.11i standard for wireless local area networks.

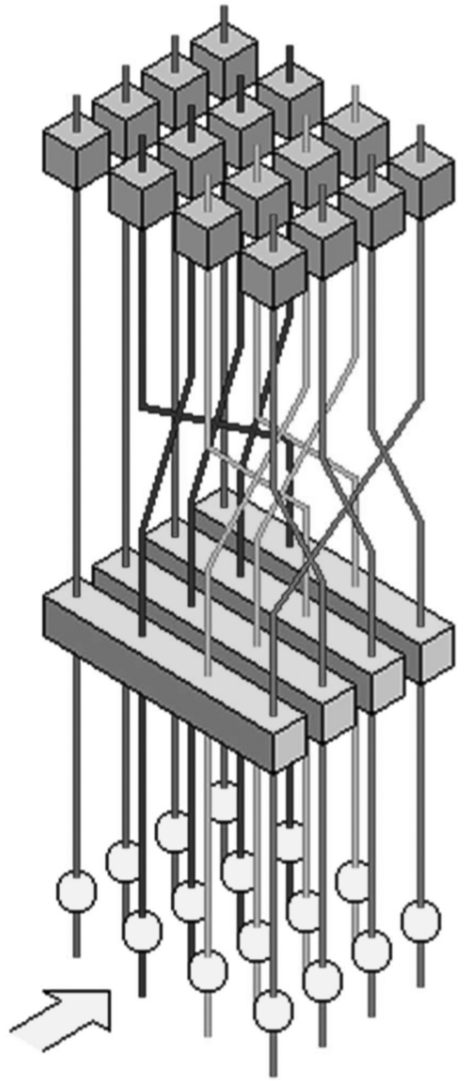
How CCMP Works

- AES processing in CCMP must use AES 128-bit key and 128-bit block size
- CCMP use of 128-bit keys and a 48-bit IV minimizes vulnerability to replay attacks; the CTR component provides data privacy
- The Cipher Block Chaining Message Authentication Code component produces a MIC that provides data origin authentication and data integrity for the packet payload data

Rijndael

- The Rijndael algorithm can be used with block sizes of 128, 192, or 256 bits
- Four major operations:

Substitute bytes	Shift rows
Mix columns	Add round key



Byte Sub

Shift Row

Mix Column

Add Round Key

Other Symmetric Algorithms

- International Data Encryption Algorithm (IDEA) 128-bit key 64-bit blocks
- CAST-128 key length between 40 and 128 bits. 12 and 16 rounds
- SAFER uses 64-bit (SAFER-SK64) or 128-bit blocks (SAFER-SK128)
- Blowfish uses variable key sizes, from 32 up to 448 bits on 64-bit blocks

Other Symmetric Algorithms (continued)

- Twofish can operate with keys of 128, 192, or 256 bits on blocks of 128 bits
- RC4 commonly used stream-based cipher
- RC5/RC6 key size can vary from 0 to 2,040 bits; the number of rounds 0 to 255

International Data Encryption Algorithm

(IDEA)

- IDEA uses a 128-bit key and operates on 64-bit blocks
- IDEA does eight rounds of transposition and substitution using modular addition and multiplication and bitwise XOR

CAST

CAST-128 can use keys between 40 and 128 bits in length and will do between 12 and 16 rounds of operation, depending on key length

Secure and Fast Encryption Routine (SAFER)

- All of the algorithms in SAFER are patent-free
- The algorithms work on either 64-bit input blocks (SAFER-SK64) or 128-bit blocks (SAFER-SK128)

Blowfish

- Extremely fast cipher and can be implemented in as little as 5K of memory
- Operates with variable key sizes, from 32 up to 448 bits on 64-bit input and output blocks

Twofish

- Was one of the finalists for the AES
- Can operate with keys of 128, 192, or 256 bits on blocks of 128 bits
- Performs 16 rounds during the encryption/decryption process

Rivest Cipher 5 (RC5)

- Very adaptable product useful for many applications
- The key for RC5 can vary from 0 to 2,040 bits
- The number of rounds it executes can be adjusted from 0 to 255
- The length of the input words can also be chosen from 16-, 32-, and 64-bit lengths
- The algorithm operates on two words at a time in a fast and secure manner

Rivest Cipher 4 (RC4)

- If RC4 is used with a key length of at least 128 bits, there are currently no practical ways to attack it
- The published successful attacks against the use of RC4 in WEP applications are related to problems with the implementation of the algorithm, not the algorithm itself

Symmetric Algorithms

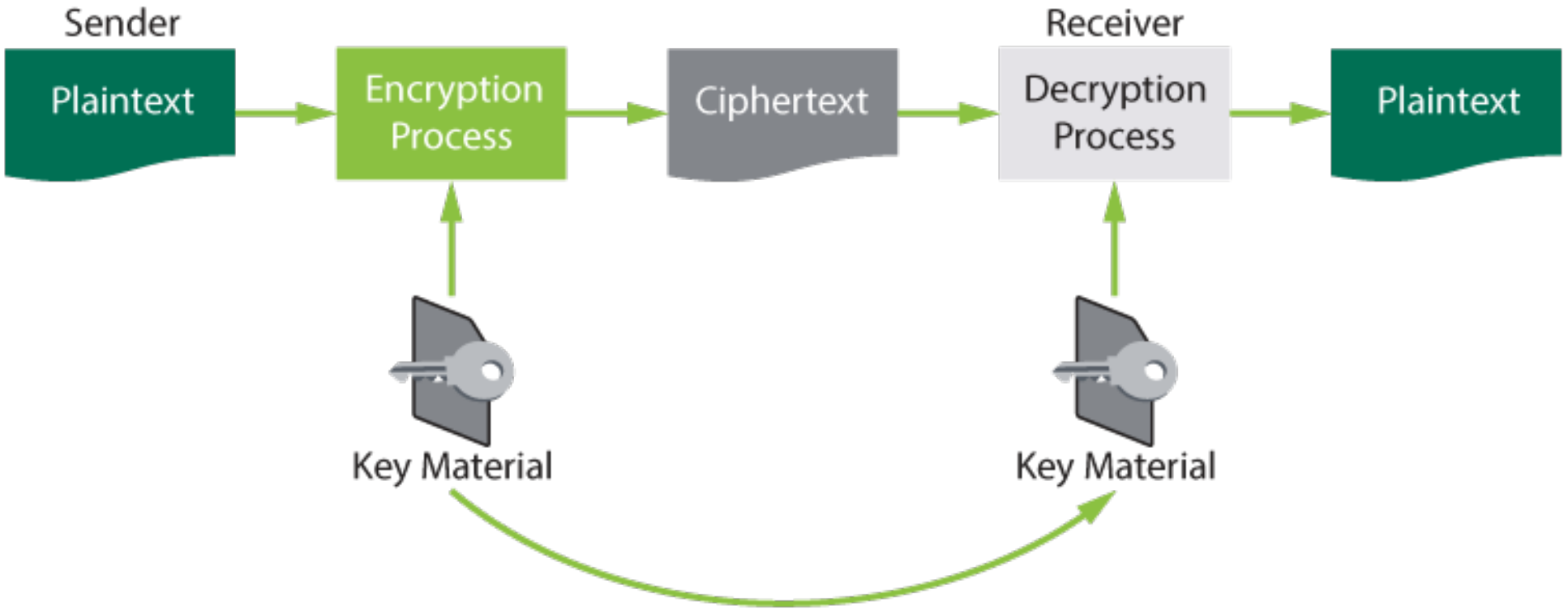
Strength	Name	Key Size
Weak	RC2-40	40
	DES	56
	RC5-64/16/7	56
Medium	RC5-64/16/10	80
	Skipjack	80
Strong	RC2-128	128
	RC5-64/12/16	128

Strength	Name	Key Size
	IDEA	128
	Blowfish	128
	3DES	168
Very Strong	RC5-64/12/32	256
	Twofish	256
	RC6	256
	Rijndael	256

Advantages and Disadvantages of Symmetric Algorithms

Advantages	Disadvantages
• Fast • Secure • Confidentiality	• Key distribution is very difficult • Not able to provide integrity, authenticity, non-repudiation of origin, access control, and digital signatures • Require both sender and receiver to share the same key • Challenges with secure key distribution • Scalability

Out-of-Band Key Distribution



Out-of-Band Key Distribution
Cryptovariable

Asymmetric Algorithms

- Asymmetric algorithms:
  - Based on the use of a pair of mathematically related keys
  - Relies on hard mathematical problems and one-way functions
    - A process that is much simpler to go in one direction (forward) than to go in the other direction (backward or reverse engineering)
- The process to generate the public key (forward) is fairly simple
  - To learn the private key from knowledge of the public key in computationally infeasible

Asymmetric Algorithms (continued)

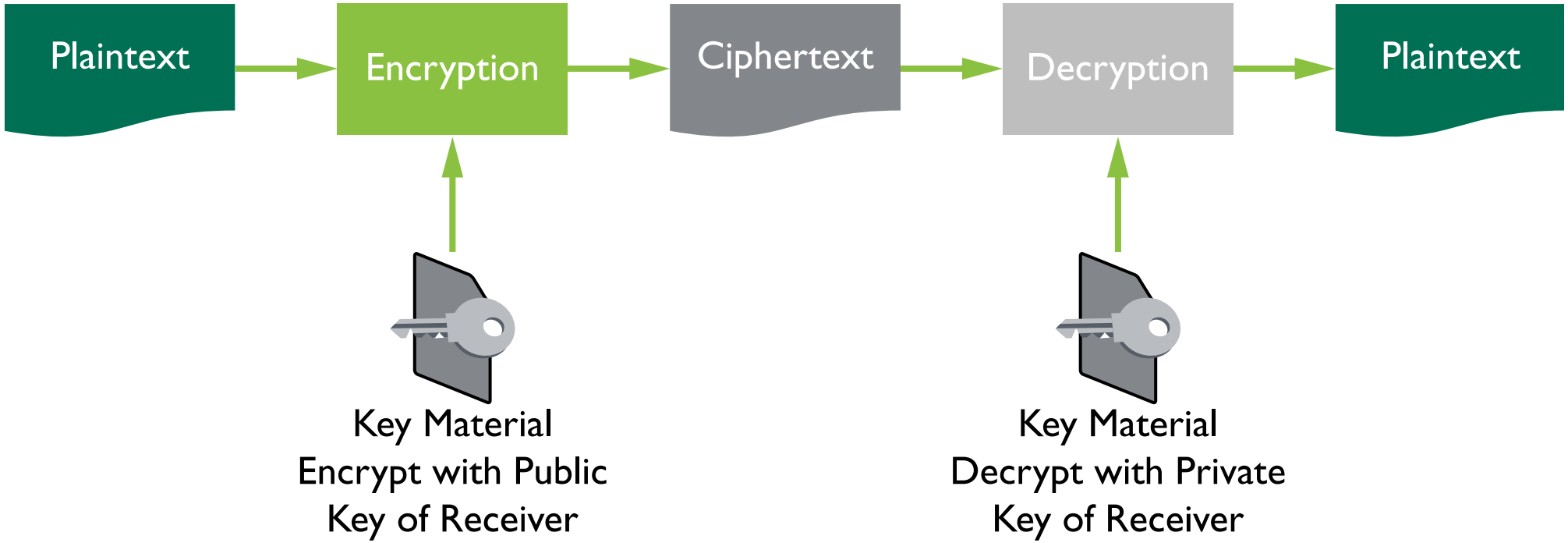
Factoring

- Given P and Q, it is easy to compute P*Q
- Given the product N = P*Q, it is not easy to compute P and Q
- Pick E (encrypt number)
- Compute D so that D*E = 1, MOD (P-1)*(Q-1)
- E and N together are the public key, and D and N are the private key

Discrete Logs

- Exponentiation is easy: if you have G and X, it is easy to compute S = G to the power of X
- Logarithms are hard: if you have S and G, it is hard to find X such that G to the power of X = S
- There are better attacks against discrete logs than brute force
- Parameters have to be as large as factoring (512, 1024, 2048 bits)

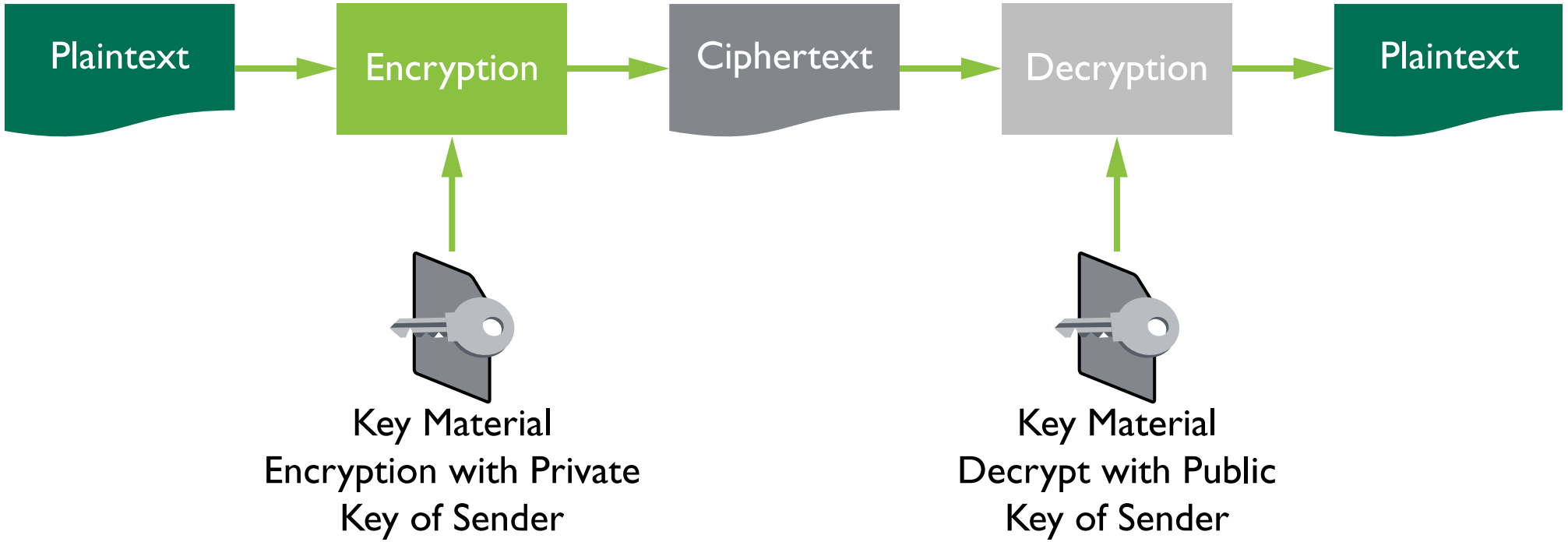
Using Public Key Cryptography to Send a Confidential Message



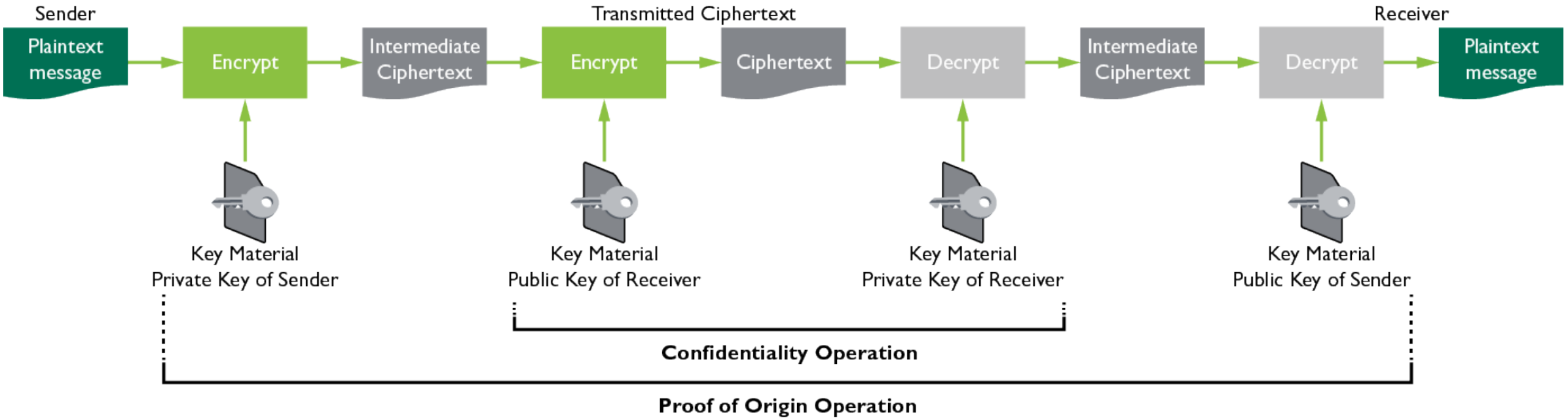
Open Message

- When a message is encrypted with the private key of a sender, it can be opened or read by anyone who possesses the corresponding public key
- When a person needs to send a message and provide proof of origin (non-repudiation), he can do so by encrypting it with his own private key
- The recipient then has some guarantee that the message did originate with the sender

Using Public Key Cryptography to Send a Message with Proof of Origin



Confidential Messages with Proof of Origin



Rivest-Shamir-Adleman (RSA) Algorithm

- RSA is based on the mathematical challenge of factoring the product of two large prime numbers
- Three primary attack approaches:

Brute force	Mathematical attacks	Timing attacks

Diffie-Hellman Algorithm

- Used to enable two users to exchange or negotiate a secret symmetric key that will be used subsequently for message encryption
- Does not provide for message confidentiality, but it is extremely useful for applications such as TLS and IPSEC
- Based on discrete logarithms

ElGamal

- Included the ability to provide message confidentiality and digital signature services
- Based on the same mathematical functions of discrete logs

Elliptic Curve Cryptography (ECC)

- The ability to use much shorter keys for ECC implementations provides savings on computational power and bandwidth
- This makes ECC especially beneficial for implementation in smart cards, wireless, and other similar application areas
- Elliptic curve algorithms provide confidentiality, digital signatures, and message authentication services

Advantages and Disadvantages of Asymmetric Key Algorithms

Advantages	Disadvantages
Possible to send a message across an untrusted medium in a secure manner without the overhead of prior key exchange or key material distribution • Access control • Confidentiality • Integrity • Non-repudiation • Authenticity • No scalability problem	Mathematically intensive and, therefore, becomes extremely slow compared with its symmetric counterpart

Activity: Asymmetric Cryptography

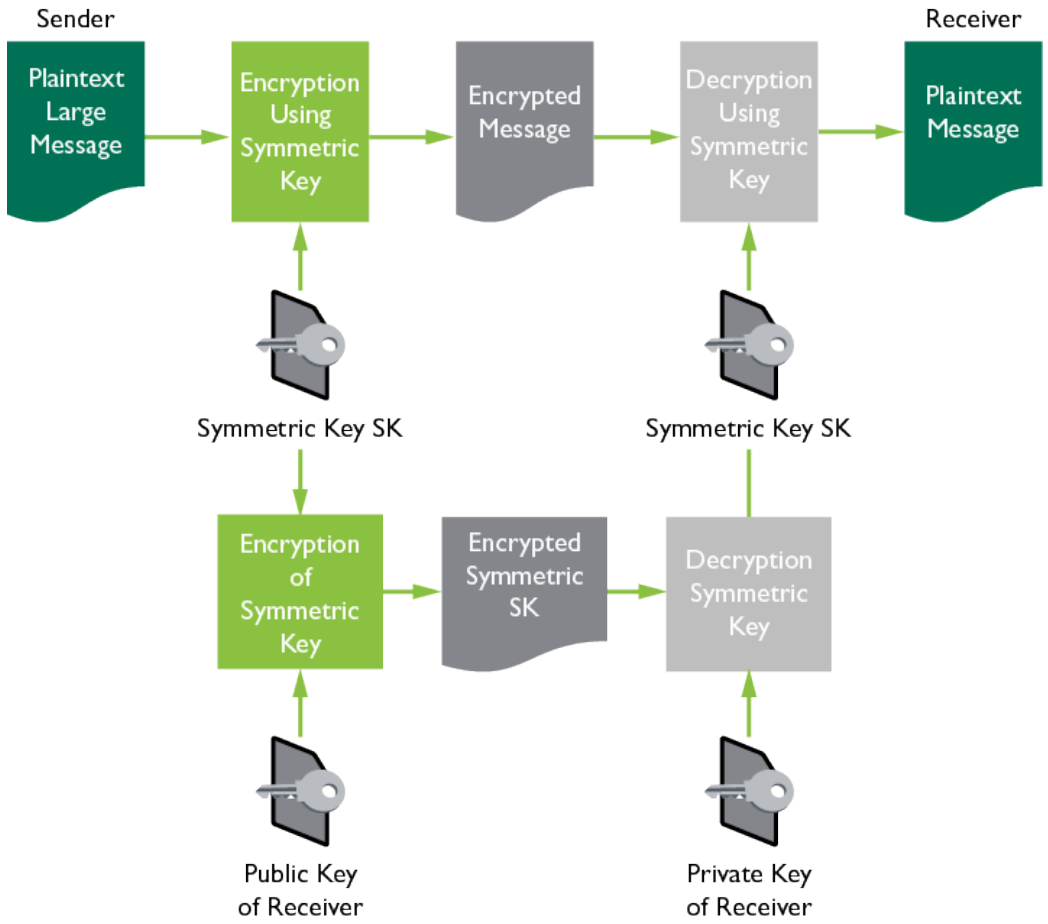
1. What must the key holder do to allow for the transmission of a confidential message?
2. Identify one or more advantages of asymmetric cryptography.
3. Identify one or more disadvantages of asymmetric cryptography.
4. Describe RSA.

Activity: Asymmetric Cryptography (continued)

ANSWERS

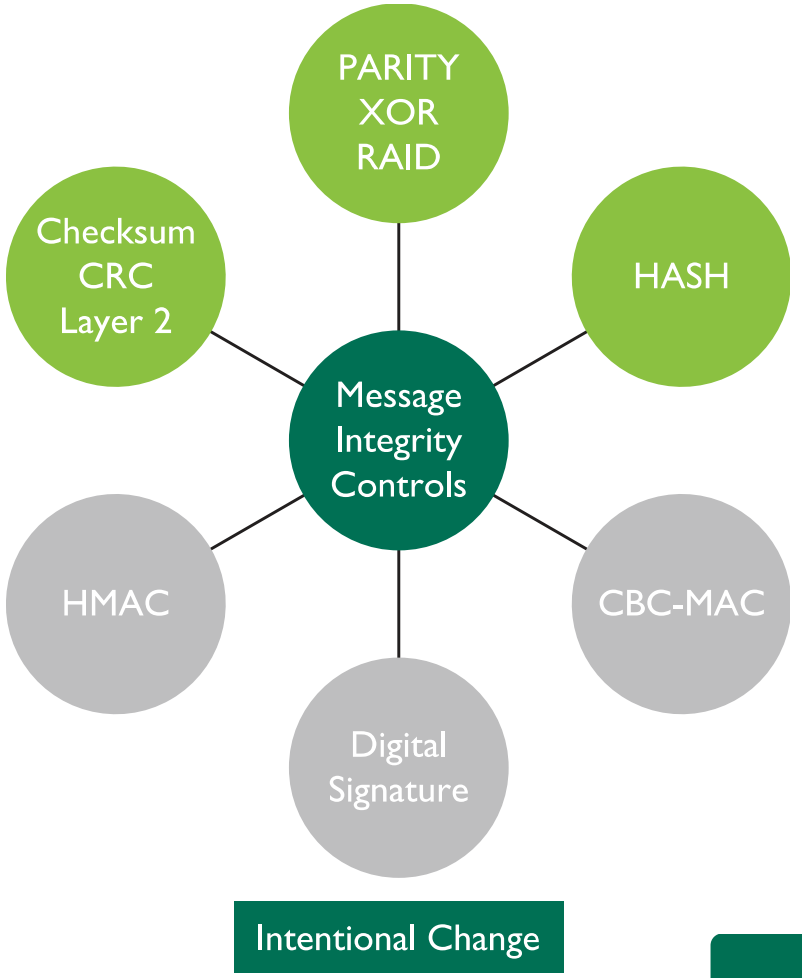
1. Keep their private key confidential.
2. It makes it possible to send a message across an untrusted medium in a secure manner without the overhead of prior key exchange or key material distribution.
3. Extremely slow
4. RSA is based on the mathematical challenge of factoring the product of two large prime numbers.

Hybrid Cryptography and Cryptographic Systems



Message Integrity Controls (MICs)

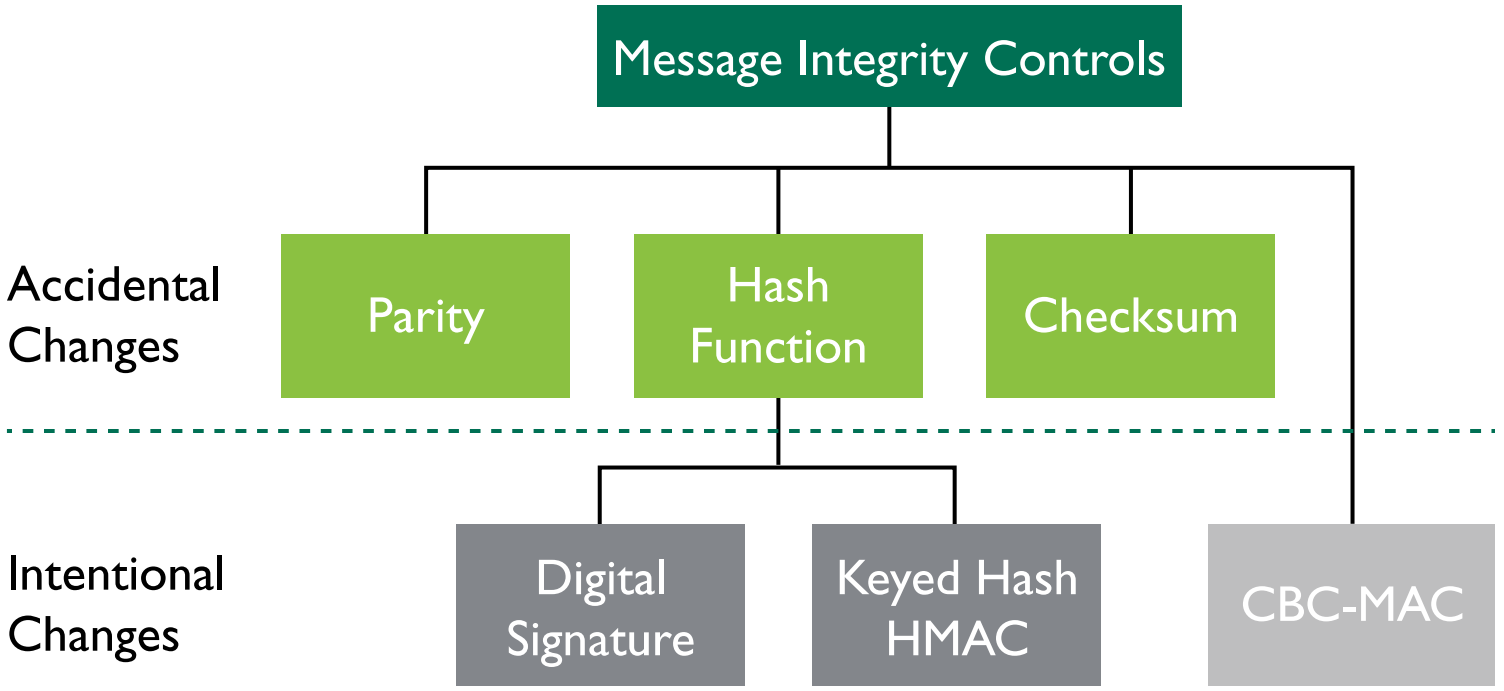
- MICs detect alterations (whether intentional or accidental) to a message during transmission
- A MIC is a special value that is calculated based on the message contents and added to the message to be sent



Message Integrity Controls (MICs) (continued)

Accomplished through cryptographic functions that perform in several manners, depending on the business needs and level of trust between the parties and systems

Message Integrity Controls (MICs) (continued)



Message Digests

- A small representation of a larger message
- Used to ensure the authentication and integrity of information, not the confidentiality

Message Authentication Code (MAC)

- A small block of data that is generated using a secret key and then appended to the message
- When the message is received, the recipient can generate his/her own MAC using the secret key and know the message has not changed

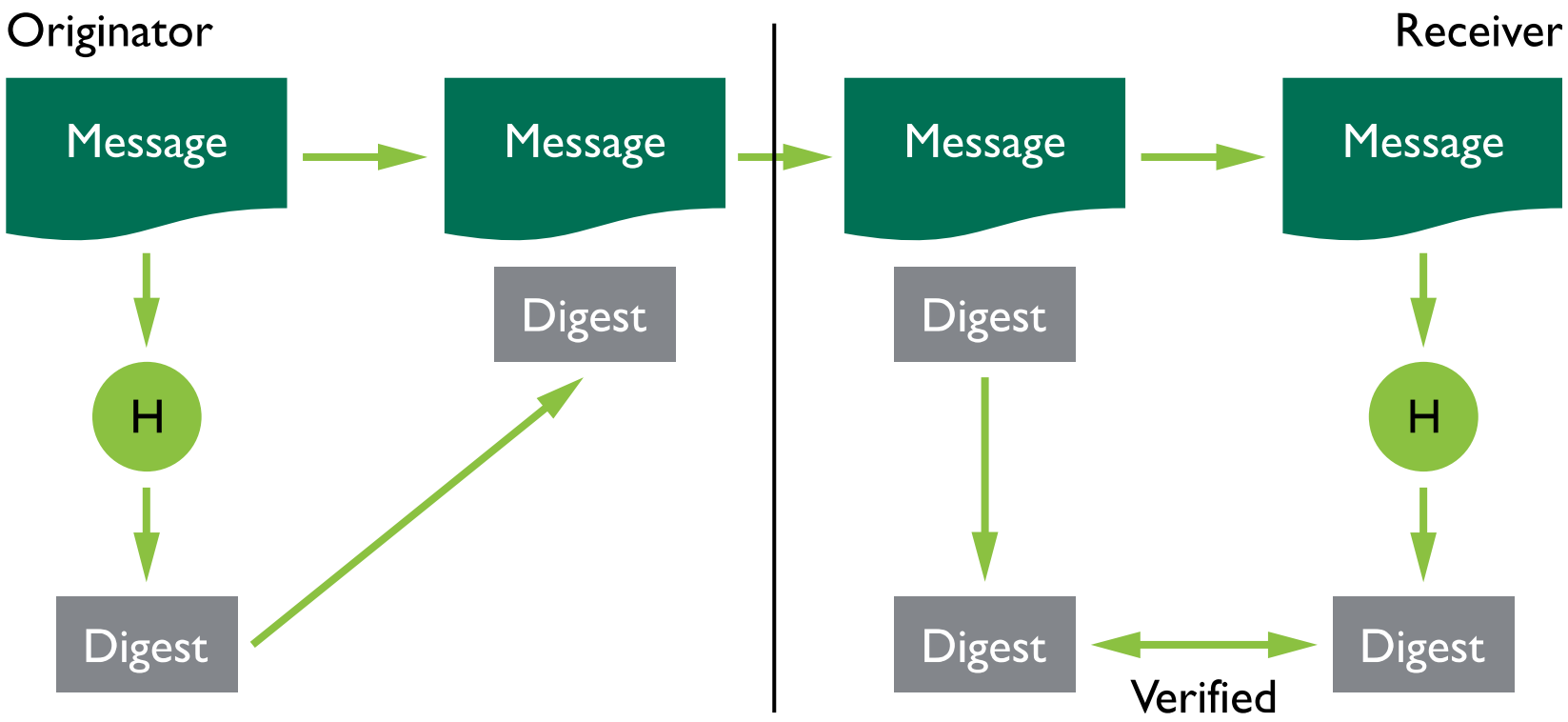
Hash Message Authentication Code (HMAC)

- Hashed MACing implements a freely available hash algorithm as a component (black box) within the HMAC implementation
- This allows ease of the replacement of the hashing module if a new hash function becomes necessary

Hashing

Accepts an input message of any length and generates a fixed-length output

Operation of Hash Functions



Five Key Properties of a Hash Function

- Uniformly distributed
- Collision resistant
- Difficult to invert
- Computed on entire message
- Deterministic (same input always produces same digest)

MD5 Message Digest Algorithm

- The most widely used hashing algorithm and is described in RFC 1321 but no longer considered secure
- MD5 generates a 128-bit digest from a message of any length
- It processes the message in 512-bit blocks and does four rounds of processing

Secure Hash Algorithm (SHA) and SHA-1

- SHA was developed by NIST.
- SHA-1 operates on 512-bit blocks and can handle any message up to 2^{64} bits in length.
- The output of SHA-1 is 160 bits in length – not considered good practice. Recommended use of SHA-512.
- The processing includes four rounds of operations of 20 steps each.

Secure Hash Standard – SHA-3

The new hash algorithm is based on the KECCAK algorithm and will be named SHA-3. It will be described in FIPS 202 (draft as of April 2015) and will augment the hash algorithms currently specified in FIPS 180-4, the Secure Hash Standard.

Other Hash Algorithms

- HAVAL – variable length output
- RIPEMD-160 – European Standard
- The output may be 128, 160, 192, 224, or 256 bits, and the number of rounds may vary from three to five
- HAVAL operates 60% faster than MD5 when only three rounds are used and is just as fast as MD5 when it does five rounds of operation

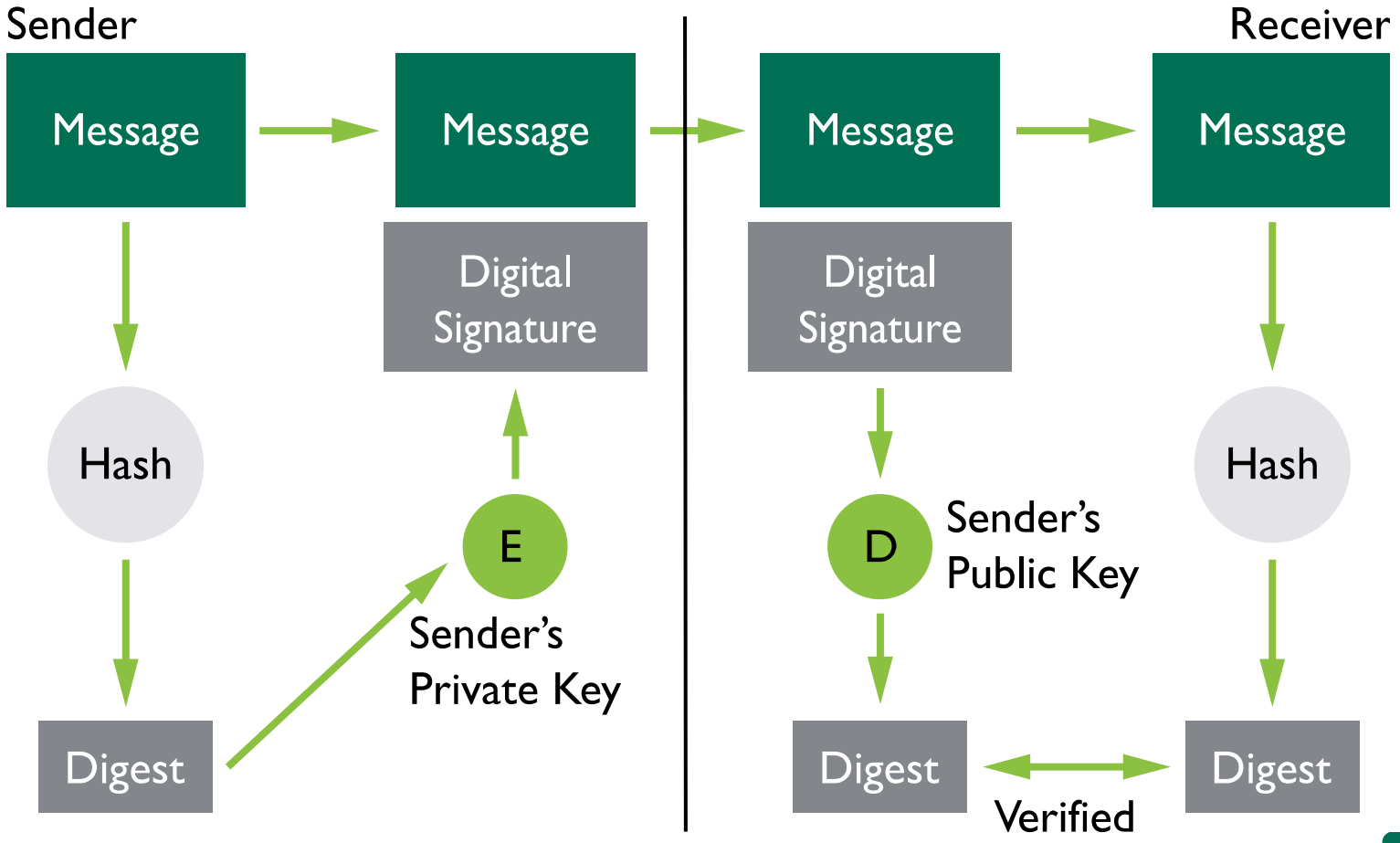
The Birthday Paradox/Birthday Attack

- Once there are more than 23 people together, there is a greater than 50% probability that two of them share the same birthday
- The likelihood of finding a collision for two messages and their hash values may be a lot easier than may have been believed
- It would be very similar to the statistics of finding two people with the same birthday
- Rainbow table uses this predictability against hashing systems

Digital Signatures – Non-Repudiation

- Provides assurance that the message comes from the person who claims to have sent it
- Has not been altered, both parties have a copy of the same document
- The sender cannot claim that he/she did not send it
- Digital Signature Standard (DSS)
  - A digital signature is based on a public key (asymmetric) algorithm
  - Does not provide for confidentiality of the message through encryption and is not used for key exchange

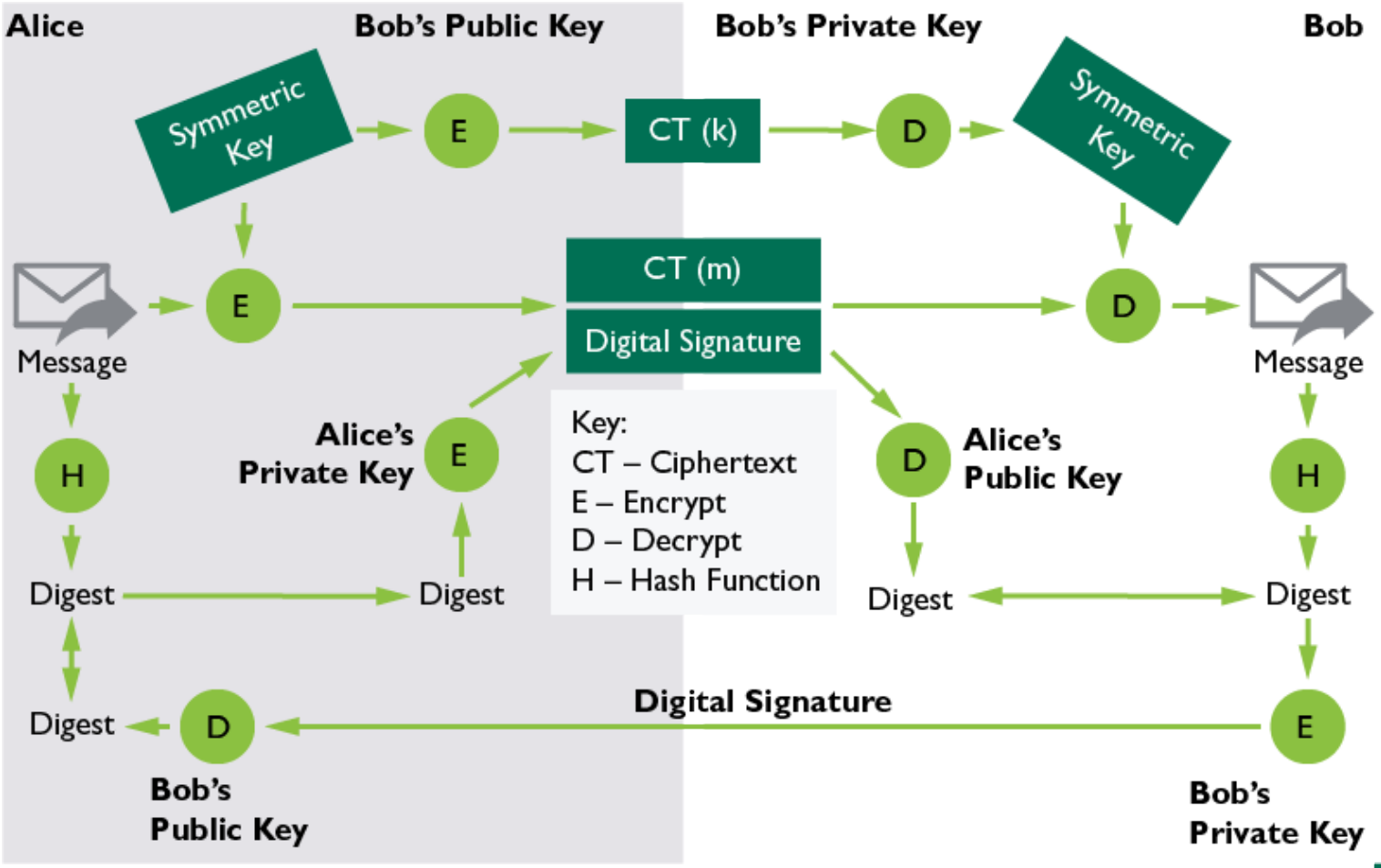
Digital Signatures



Uses of Digital Signatures

- A digital certificate is an electronic document that asserts authenticity and data integrity that is tied to a sender
- Digital signatures are used to sign emails, ecommerce transactions, software and software patches, and digital certificates
- Many governments and courts recognize digital signatures as a verifiable form of authentication

Combine Everything



Applying Cryptography and Key Management

Cryptographic Lifecycle

A cryptographic function is “broken” when one of the following conditions is met:

For a Hashing Function:	For an Encryption System:
• Collisions or hashes can be reliably reproduced in an economically feasible fashion without the original source • When an implementation of a hashing function allows a side channel attack	• A cipher is decoded without access to the key in an economically feasible fashion • When an implementation of an encryption system allows unauthorized disclosure or alteration of information • Private key has been compromised

Algorithm/Protocol Governance

Cryptography policies, standards, and procedures should minimally address:

- Approved cryptographic algorithms and key sizes
- Transition plans for weakened or compromised algorithms and keys
- Procedures for the use of cryptographic
- Key generation, escrow, and secure destruction
- Incident reporting

Issues Surrounding Cryptography

- As part of risk analysis, it is important to understand how cryptography can be misused so that appropriate security mitigation can be applied
- Cryptographic protection is implemented for preventing software and media piracy or corruption of software (digitally signed software and software patches)
- Digital rights management systems (DRMS) require a design and governance to protect intellectual property and individual privacy while ensuring an individual's fair use of the intellectual property

International Export Controls

- Most countries regulate the use of cryptographic tools used by their citizens
- Most laws that control the use of cryptography are based on key length
- Dual use good (can be used for both commercial and military purposes)
- This is because key length is one of the most understandable methods of gauging the strength of a cryptosystem

Public Key Infrastructure (PKI)

- A set of system, software, and communication protocols required to use, manage, and control public key cryptography
- It has core primary purposes:
  - Publish public keys/certificates
  - Certify that a key is tied to an individual or entity
  - Provide verification of the validity of a public key
  - Provide services such as confidentiality, integrity, authenticity, non-repudiation and access control

Certification/Certificate Authority (CA)

- Binds entities to their public keys
- "Signs" an entity's digital certificate to certify that the certificate content accurately represents the certificate owner

X-509 Certificate

Field	Description of
Algorithim used for the signature	Algorithm used to sign the certificate
Issuer name	X.500 name of CA
Period of validity	
Start date/end date	
Subject's name	Owner of the public key
Subject's public key information (algorithm, parameters, key)	Public key and algorithm used to create it
Issuer unique identifier	Optional field in case the CA used more than one X.500 name
Subject's unique identifier	Optional field in case the public key owner has more than one X.500 name
Extensions	
Digital signature of CA	Hash of the certificate encrypted with the private key of the CA

Certificate Revocation

- Certificate revocation is required if private key has been compromised
- Provides updates on non-valid certificates, in other words, tells certificate holders not to use public key

Key Management and Key Management Practices

Key generation	Key distribution	Key change
Key disposition	Key recovery	Key storage

Key Recovery

Dual Control

Two or more people required working in cooperation

Split Knowledge

Specific information known only to one individual that must be combined with knowledge held by another individual

Key Escrow

Storing key with a trusted party

Creation of Keys

Automated key generation

Truly random

Random

Asymmetric key length

Key Wrapping and Key Encrypting Keys (KEKs)

- KEKs are used as part of key distribution or key exchange
- The process of using a KEK to protect session keys is called key wrapping
- Key wrapping uses symmetric ciphers to securely encrypt a plaintext key with associated integrity information and data

Key Distribution

- Keys can be distributed in a number of ways
- Example:
  - Out-of-band key exchange
  - Key wrapping

Key Storage and Destruction

Methods for protecting stored keying material include:

- Trusted, tamperproof hardware security modules
- Passphrase protected smart cards
- Key wrapping the session keys using long-term storage KEKs
- Splitting cipher keys and storing in physically separate storage locations
- Protecting keys using strong passwords/passphrases, key expiry, and the like
- At the end of lifecycle of keys, they must be securely destroyed

Cryptanalysis – Methods of Cryptanalytic Attacks

Activity: Cryptanalytic Attacks

INSTRUCTIONS

As we discuss each of the attacks, complete the table.

Brute Force Attacks

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Key Size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

If you assume:

- *Every person on the planet owns 10 computers.*
- *There are 7 billion people on the planet.*
- *Each of these computers can test 1 billion key combinations per second.*
- *On average, you can crack the key after testing 50% of the possibilities.*

Then the earth's population can crack one encryption key in 77,000,000,000,000,000,000,000,000 years!

Supercomputer: No. of combination checks per second = $(10.51 \times 10^{15}) / 1000 = 10.51 \times 10^{12}$

https://www.eetimes.com/document.asp?doc_id=1279619

Ciphertext-only Attack

- One of the most difficult because the attacker has so little information to start with
- All the attacker starts with is some unintelligible data that he suspects may be an important encrypted message
- The attack becomes simpler when the attacker is able to gather several pieces of ciphertext and thereby look for trends or statistical data that would help in the attack

Known Plaintext

- The attacker has access to the ciphertext and the plaintext versions of the same message
- The goal of this type of attack is to find the cryptographic key that was used to encrypt the message
- Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key

Chosen Plaintext

- The attacker knows the algorithm used for the encrypting or has access to the machine used to do the encryption and is trying to determine the key
- This may happen if a workstation used for encrypting messages is left unattended
- The attacker can run chosen pieces of plaintext through the algorithm

Chosen Ciphertext

- Similar to the chosen plaintext attack in that the attacker has access to the decryption device or software and is attempting to defeat the cryptographic protection by decrypting chosen pieces

  of ciphertext to discover the key
  - Sometimes called the lunchtime attack
- An adaptive chosen ciphertext would be the same, except that the attacker can modify the ciphertext prior to putting it through the algorithm
  - Sometimes called the midnight attack

Linear and Differential Cryptanalysis

- Linear cryptanalysis is a known plaintext attack that requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key
  - It focuses on statistical analysis against one round of decryption on large amounts of ciphertext
- Differential cryptanalysis is a chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts
  - It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm

Implementation Attacks

Some of the most common and popular attacks against cryptographic systems due to problems with their implementation ease and reliance on system elements outside of the algorithm such as random number generators.

Replay Attack

- Disrupts and damages processing by the attacker by resending repeated files to the host
- If there are no checks such as time-stamping, use of one-time tokens or sequence verification codes in the receiving software, the system might process duplicate files

Birthday Attack

The point of the birthday attack is that it is easier to find two messages that hash to the same message digest than to match a specific message and its specific message digest.

Factoring Attack

Because RSA uses the product of large prime numbers to generate the public and private keys, this attack attempts to find the keys through solving the factoring of these numbers.

Attacking the Random Number Generators

- This attack was successful against the SSL installed in Netscape several years ago
- Because the random number generator was too predictable, it gave the attackers the ability to guess the random numbers
- Short Initialization Vectors led to compromise of WEP since the IV was not random enough

Other Cryptographic Attacks

Algebraic	Timing	Power analysis
Frequency analysis	Statistical analysis	Social engineering
Brute force	Dictionary attacks	Rainbow tables

Accessing Temporary Files

- Most cryptosystems will use temporary files to perform their calculations
- If not deleted and overwritten, they may be compromised and lead an attacker to the message in plaintext

Social Engineering for Key Discovery

- Through coercion, bribery, or befriending people in positions of responsibility, spies gain access to systems without having any technical expertise
- This is the most common type of attack and usually the most successful

Module 7

Physical Security

Module Objectives

1. Apply security principles to site and facility design.
2. Implement and manage physical security controls.
3. Implement and manage physical controls in wiring closets and intermediate distribution facilities.
4. Implement and manage physical controls in server rooms and data centers.
5. Implement and manage physical controls in media storage facilities.
6. Implement and manage physical controls for evidence storage.
7. Implement and manage physical controls in restricted areas.

Module Objectives (continued)

8. Implement and manage physical controls in work areas.
9. Implement and manage environmental controls for utilities and power.
10. Implement and manage controls for heating, ventilation, and air conditioning (HVAC).
11. Implement and manage environmental controls.
12. Implement and manage environmental controls for fire prevention, detection, and suppression.

Physical Security

- Physical security plans and infrastructure are often designed, implemented, and operated by physical security specialists
- Physical security infrastructure is typically controlled outside of IT or IT security control
- The CISSP MUST understand physical security fundamentals in order to:
  - Assess the risk reduction value of physical security controls
  - Communicate physical security needs to physical security managers
  - Identify risks to Information Security due to physical security weaknesses

Apply Security Principles to Site and Facility Design

- Physical design should support confidentiality, integrity, and availability of information systems
- Physical design must consider human safety and external factors as well

Physical Design that Supports Confidentiality, Integrity, and Availability (CIA)

- Physical design protects information systems from unauthorized access
- Provides for auditing or observation of sensitive physical access
- Includes identification of subjects in sensitive areas
- Ensures robust services (e.g., power, cooling) to information systems

Physical Design that Supports Human Safety

- Emergency alarms (audible, visible)
- Egress routes
- Safety equipment
- Emergency power or equipment shutoffs
- Equipment lockouts

Site and Facility Design Considerations

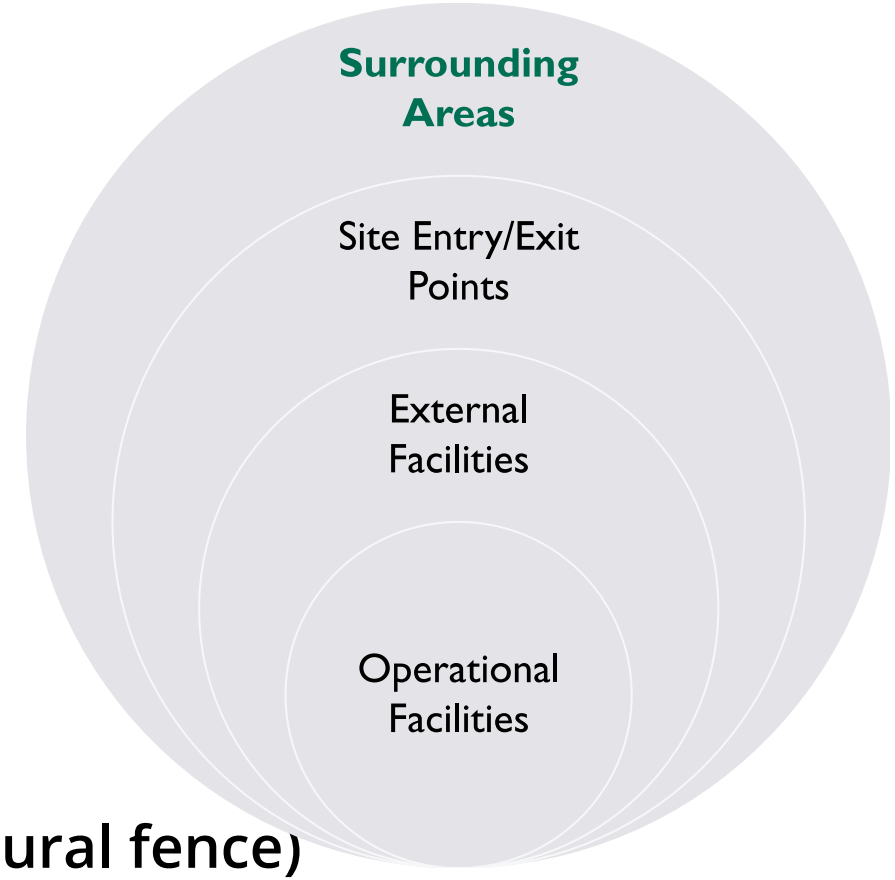
- Personnel policy and procedure
- Personnel screening
- Workplace violence prevention
- Response protocols and training
- Mail screening
- Shipping and receiving
- Property ID and tracking
- Parking and site security
- Site and building access control
- Video surveillance
- Internal access control
- Infrastructure protection
- Onsite redundancy
- Structural protections

Implement and Manage Physical Security

- Conduct a physical risk assessment (Domain 1)
  - Human action, natural disaster, industrial accident, equipment failure, etc.
- Develop layered physical protections commensurate with the risk assessment
  - E.g., Embassy level protections vs a small remote office
- Physical risk controls will impact information system design
  - E.g., weak physical controls may necessitate more complex information system protections to compensate
- Physical protections require monitoring and auditing

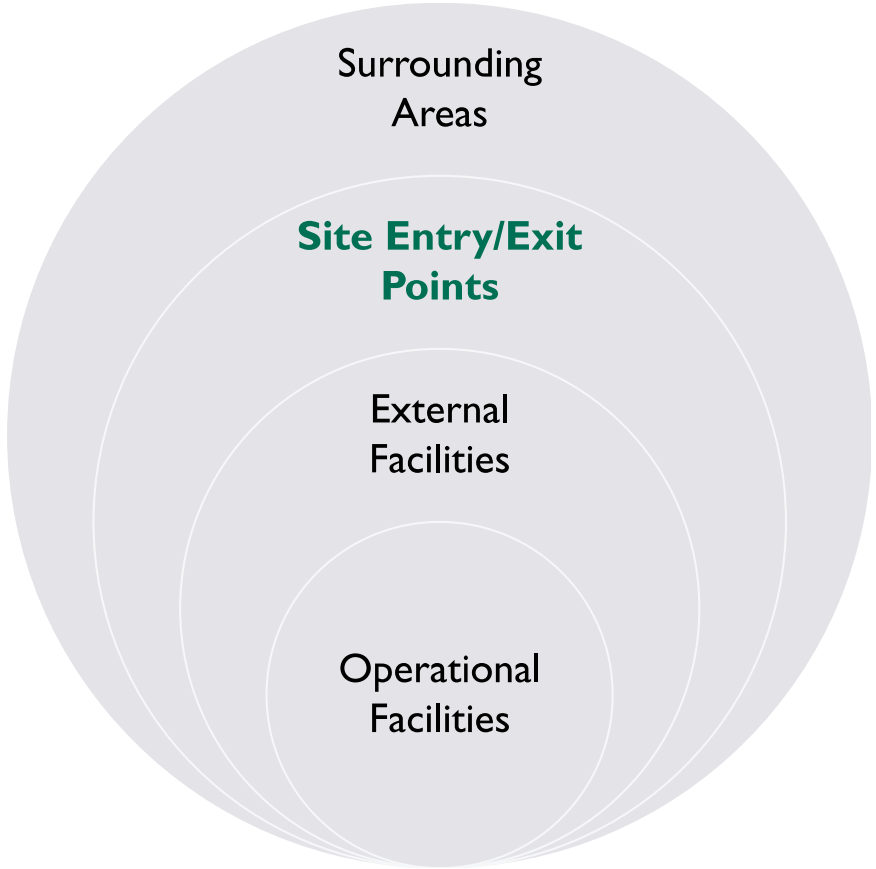
Perimeter Security Controls

- Surrounding Areas:
  - Roadways
  - Waterways
  - Geography
  - Lines of sight
- Consider:
  - Facility visibility from roads
  - Potential for vehicle borne threats
  - Vehicular and pedestrian access point locations
  - Fencing, perimeter landscaping (natural fence)



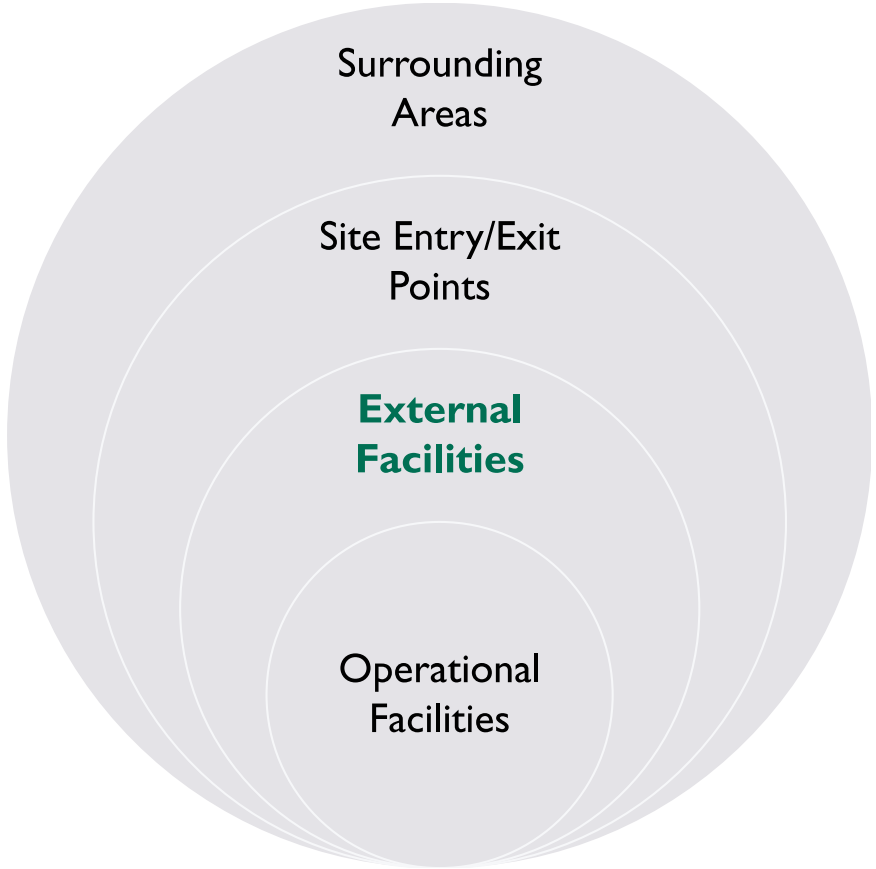
Perimeter Security Controls (continued)

- Site Entry/Exit points:
  - Vehicular
    - Public/customer/visitor
    - Staff/employee
    - Delivery/truck
  - Pedestrian
- Consider:
  - Access controls
  - Surveillance
  - Lighting
  - Intrusion detection
  - Barriers/traffic control



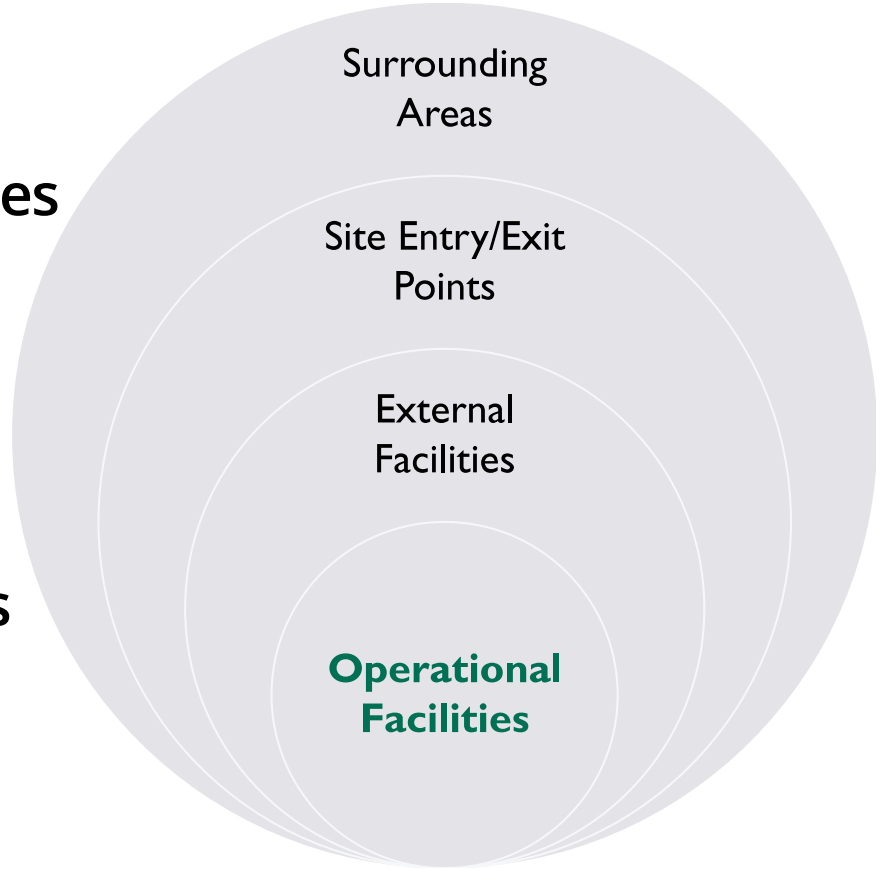
Perimeter Security Controls (continued)

- External Facilities:
  - Parking structures/lots
  - Utilities components
    - Electric transformers/lines
    - Telecommunications
  - Landscaping
- Consider:
  - Lighting
  - Surveillance
  - Intrusion detection
  - Lines of sight



Perimeter Security Controls (continued)

- Operational Facilities:
  - Where employees work
  - Where information technology operates
- Consider:
  - Exterior lighting and surveillance
  - Building materials
    - Doors, locks, windows, walls
  - Entry/exit points and access controls
    - Staff/employee entrance
    - Public/customer entrance
    - Delivery entrance
    - Sensors/intrusion detection



Perimeter Security Controls—Typical Control

Types

- Lighting
  - Bright enough to cover target areas
  - Limits shadow areas
  - Sufficient for operation of cameras, must be coordinated with camera plan
- Surveillance/camera
  - Narrow focus for critical areas
  - Wide focus for large areas
  - IR/low light in unlit areas
  - Monitored and/or recorded
  - Dummy cameras

Perimeter Security Controls—Typical Control

Types (continued)

- Intrusion detection
  - Cut/break sensors
  - Sound/audio sensors
  - Motion sensors
- Barriers
  - Fixed barriers to prevent ramming
  - Fixed barriers to slow speeds
  - Deployable barriers to block access ways
- Fencing/security landscaping
  - Slows and deters
  - Should not impede monitoring

Perimeter Security Controls—Typical Control

Types (continued)

- Building material security examples:
  - High-security glass
  - Steel/composite doors
  - Steel telecommunications conduit
  - Secure walls
  - True floor to ceiling walls (wall continues above drop ceiling)
  - Anchored framing material
  - Solid walls/in-wall barriers
- Lock security examples:
  - Available in varying grades
  - Physical key locks
  - Mechanical combination locks
  - Electronic combination locks
  - Biometric locks
  - Magnetic locks
  - Magnetic strip card locks
  - Proximity card locks
  - Multifactor locks (e.g., card + pin)

Internal Security Controls

- Controls for human safety
  - Visible and audible alarms, fire suppression, response plans/training, emergency shutoffs
- Controls to manage access
  - Door locks (e.g., magnetic, card key, mechanical key, combination lock)
  - Access point security (e.g., mantraps, limited ingress, alarmed emergency egress)
  - Multifactor access (e.g., key card + pin for room entry)
- Internal monitoring
  - Physical access control system/monitor (e.g., records key card use)
  - Video surveillance/cameras
  - RF monitoring

Implement Site and Facility Security Controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted area security
- Utilities
- Heating, ventilation, and air conditioning (HVAC)
- Fire prevention, detection, and suppression
- Environmental issues

Wiring Closets/Intermediate Distribution Facilities

—Components

- Entrance facility
  - External communications enter facility
  - Phone, network, special connections
  - May house ISP/provider equipment
- Equipment room
  - Primary communication hub for facility
  - Houses wiring/switch components
  - May be combined with entrance facility
- Backbone distribution
  - Connects entrance facility, equipment room, and telecommunication room(s)

Wiring Closets/Intermediate Distribution Facilities

—Components (continued)

- Telecommunications room (wiring closet)
  - Serves a particular area of a facility
    - Floor, section, wing, etc.
  - Terminates local wiring into patch panels
  - Backbone distribution is broken out to individual connections (e.g., switch)
- Horizontal distribution system
  - Cables, patch panels, jumpers, cable

Wiring Closets/Intermediate Distribution Facilities

—Protections

Security Protections

- Rooms must be secured against unauthorized access
- Access to rooms should be monitored/recorded
- Secondary locks on equipment/racks
  - Rooms may share space with non-IT equipment and require access by non-IT staff
- Conduit or tamper protections for wiring

Environmental Protections

- Protection from lightning/surge
- Backup power/UPS
- Heating/cooling/air flow
  - Critical in enclosed spaces
- Appropriate fire detection/suppression
- Emergency shutoffs for high-power connections
  - May not be necessary in all closets

Server Rooms/Data Centers

- Similar security and environmental protections to wiring closets
- Access point security and access monitoring is a critical concern
  - Rack or equipment level locking for shared spaces
  - Especially in shared spaces
- Power/surge/uninterruptible power supply (UPS) equipment is tailored to the operating equipment
  - Human safety becomes an issue with power levels in most server rooms
  - Emergency shutoffs and non-conductive hooks/gloves are important for human safety
- Appropriate fire detection/suppression must be considered (e.g., sprinkler is inappropriate for electrical fires)
- Typically maintained at a higher level of physical security than the rest of the facility

Media Storage Facilities

- Media may be stored onsite and offsite from the main facility
- Offsite storage should duplicate critical media
- Access control is strictly limited and monitored (often limited to archivists)
- Temperature/humidity should be consistent with media storage requirements
  - As media types evolve, this must be continually reassessed
- Fire protection at both room and container levels

Evidence Storage

- Access strictly limited and monitored
- Individual lockers/secure containers for investigations/investigators
- Tamper evident seals available for evidence bags/containers
- Maintaining chain of custody is critical to prove evidence has not been modified or tampering has not occurred
- Evidence protected against damage/theft
- Environmental protections should be commensurate with evidence types stored (e.g., paper, digital, media)

Restricted Area Security

- Includes secure facilities and classified workspaces
- Extremely high access control protections and logging of access
- May include audio protections against eavesdropping
- May include enhanced visual screening from exterior spaces
- May include protection against the detection of electromagnetic emissions from equipment

Utilities

- Power
  - Redundant power input from utilities
  - Redundant transformers/power delivery
  - Backup generators
  - Battery backups
  - Dual power infrastructure within data centers
  - Backup sources must be tested/exercised
  - Backup sources must be sized appropriately and upgraded when load increases
- Telecommunications
  - Multiple service provider inputs
  - Redundant communication channels/mechanisms
  - Redundancy on key equipment (eliminate single points of failure)
- Water/Sewer
  - Cooling/human habitation
  - Risk of leaks/damage to equipment
  - Supports most building-wide fire suppression plans

Utilities-Safety

- Generators, battery backups, and data center power feeds may carry very high electrical loads that are inherently dangerous
- Emergency power shutoffs in high-load areas:
  - Safeguard human life in case of electrocution (big red button)
  - Safeguard equipment in case of overload (automated shutoff)
  - Safeguard humans and equipment in emergencies
    - Flooding/sprinkler activation
- High load areas should provide access to nonconductive gloves/equipment and push/pull rods in case of emergency

Heating, Ventilation, and Air Conditioning (HVAC)

- High-density equipment requires adequate cooling and airflow
- Cooling must be designed match the equipment/space to be cooled
- High-capacity rooms (e.g., operations center) must have sufficient airflow for the number of human occupants (CO2 danger)
- Air should be filtered for contaminants (natural or intentionally introduced)

Fire Prevention and Detection

- Human training and awareness is critical to prevention
- Sensors (IR, temperature, smoke) can detect conditions leading up to a fire as well as fire initiation.
  - Smoke detectors include optical (photoelectric) and physical process (ionization)
  - Fire detectors include infrared and ultraviolet detectors

Fire Suppression

- Buildings should be equipped with one or more types of fire suppression systems than include installed and handheld
- Handheld extinguishers are typically chemical agent based with either wet or dry chemicals
- Two main types of installed suppression systems: water-based and gas-based

Fire Suppression (continued)

Water-based

- Effective for common material fires (e.g., wood, paper, building materials)
- Safe for human spaces
- Damages equipment
- Ineffective for electrical or petroleum fires
- Typically cheaper than gas-based

Gas-based

- Effective for any fire type
- Typically safe for equipment
- May be dangerous to humans in enclosed spaces (depending on

Fire Suppression (continued)

Water-based system types:

- Wet pipe
  - Most common, water in pipes, heat activated sprinkler heads
- Dry pipe
  - Pressurized gas in pipes, water released when activated, slight delay, less danger of pipe leaks/freezing
- Pre-action
  - Combines wet and dry pipe actions
- Deluge
  - Pre-action but with open sprinkler heads

Fire Suppression (continued)

Gas system examples:

- Hydrofluorocarbon
  - Halon (older type—mostly gone)
  - FM-200
- Inert gas (e.g., Argon/Nitrogen)
  - Argonite
  - Inergen
- Aerosol
  - Aero-K

Environmental Issues

Hurricane	Forest/wildfire	Flooding
Tornado	Earthquake	Mudslide

Module 9

Domain Review

Domain Summary

- Application of security engineering and architecture principles is a key element to any system lifecycle.
- Security models are used as templates for system security behavior and design.
- Security control frameworks are employed to ensure consistent and complete application of security functions across an environment.
- Various types of systems have inherent security strengths and weaknesses that must be understood to ensure they are properly employed.

Domain Summary (continued)

- The history of cryptography is very long, but over the last 50 years or so, cryptography has become an integral and necessary part of security implementations.
- Cryptography can be very effective in providing some key security services such as confidentiality, integrity, authenticity (proof of origin), non-repudiation, and access control.
- There are basic fundamental ways to do cryptography, stream and block ciphers.
- Symmetric key cryptography is very fast, but has problems related to key distribution and scalability.

Domain Summary (continued)

- Asymmetric key cryptography is very slow but solves the problems related to key distribution and scalability.
- Hashing, which is defined as one-way encryption, can be very useful in addressing integrity of stored and transmitted information.
- Digital signatures can achieve non-repudiation of origin and non-repudiation of delivery.
- Key management, and key management techniques are the most important aspects of secure cryptography implementations.

Domain Summary (continued)

- There are many cryptanalysis attacks that try and break cryptography systems.
- Physical security is an important element to ensure information systems are protected.

Domain Review Questions

1. Requirements definition, design, implementation, and operation are examples of what type of System and Security Engineering processes?

A. Technology processes
B. Acquisition processes
C. Design processes
D. Technical processes

Answer

The correct answer is D.

A is incorrect terminology. B and C are specific processes, not types of processes.

Domain Review Questions

2. One security model includes a set of rules that can dynamically restrict access to information based upon information that a subject has already accessed in order to prevent any potential conflict of interest. This model is known as the:

A. Biba model
B. Brewer/Nash model
C. Graham–Denning model
D. Harrison, Ruzzo, Ullman model

Answer

The correct answer is B.

A, C, and D are models that describe an information system's rules for operation, but those rules are applied universally. The Brewer/Nash model is the only model that explicitly addressed conflicts of interest.

Domain Review Questions

3. Select the best answer. Inheritable or “common” security controls are characterized as:

A. Controls that are passed down from older systems to new systems through code sharing
B. Introduces unacceptable risk in most systems
C. Controls that are never assessed in an operational environment
D. Controls that are provided from one system to another in an operational environment

Answer

The correct answer is D.

D is the correct definition of the term. A, B, and C are not types of controls. All controls must be assessed whether inherited or not, and while inheritable controls may introduce risk if not operating properly, they do not generally introduce unacceptable risk, which makes D a better answer

Domain Review Questions

4. Three common types of industrial control systems include:

A. Supervisory control and data acquisition, distributed control systems, programmable logic controllers
B. Supervisory control and data anonymization, distributed control systems, programmable logic capability
C. Supervisory control and data anonymization, distributed chip systems, programmable logic controllers
D. Supervisory control and data acquisition, distributed chip systems, programmable logic capability

Answer

The correct answer is A.

Items B, C, and D include incorrect terminology.

Domain Review Questions

5. The four most common types of sprinkler systems are:

A. Soaking, wet pipe, dry pipe, and pre-action
B. Wet pipe, dry pipe, deluge, and pre-action
C. Wet pipe, dry pipe, soaking, and hybrid
D. Dry pipe, soaking, deluge, and hybrid

Answer

The correct answer is B.

Items A, C, and D each contain at least one incorrect element.

Domain Review Questions

6. The key used in a cryptographic operation is also called:

A. Cryptovariable
B. Cryptosequence
C. Cryptoform
D. Cryptolock

Answer

The correct answer is A.

The cryptovariable is the correct definition used by cryptologists to describe the key in a cryptography system.

Domain Review Questions

7. Most cryptographic algorithms operate either in block mode or:

A. Cipher mode
B. Logical mode
C. Stream mode
D. Decryption mode

Answer

The correct answer is C.

All ciphers either operate on stream mode, one bit at a time, or block mode, several bits at a time.

Domain Review Questions

8. Which of the following is NOT one of the primary objectives of cryptography?

A. Non-repudiation
B. Authenticity
C. Data integrity
D. Authorization

Answer

The correct answer is D.

The five services that cryptography can provide are confidentiality, integrity, authenticity, non-repudiation, and access control. Authorization, therefore, is not a service that cryptography can achieve.

Domain Review Questions

9. Another name for symmetric key cryptography is?

A. Shared
B. Public
C. Key clustering
D. Elliptic curve

Answer

The correct answer is A.

Symmetric, which means “the same,” implies that a shared key is required by the sender and the receiver in order to be able to encrypt and decrypt a message or data.

Domain Review Questions

10. How many keys would need to be managed for an asymmetric key system such as RSA with 500 users (N)?

A. Nx2
B. N (N-1)/2
C. 2 to the power of N
D. N to the power of 2

Answer

The correct answer is A.

Asymmetric key cryptography algorithms require users to have their private and public key pairs, two keys each. For 500 users, each having a key pair, the answer is 1,000, or Nx2.