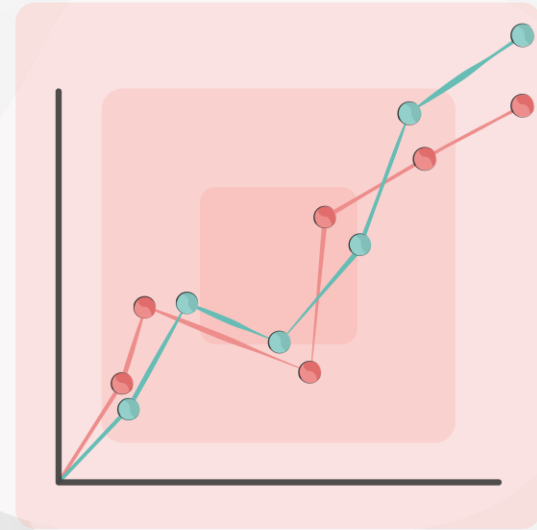




# **Level 5 Data Engineer Module 4 Topic 2**

## **Cyber security essentials**

**Welcome to today's  
webinar.**

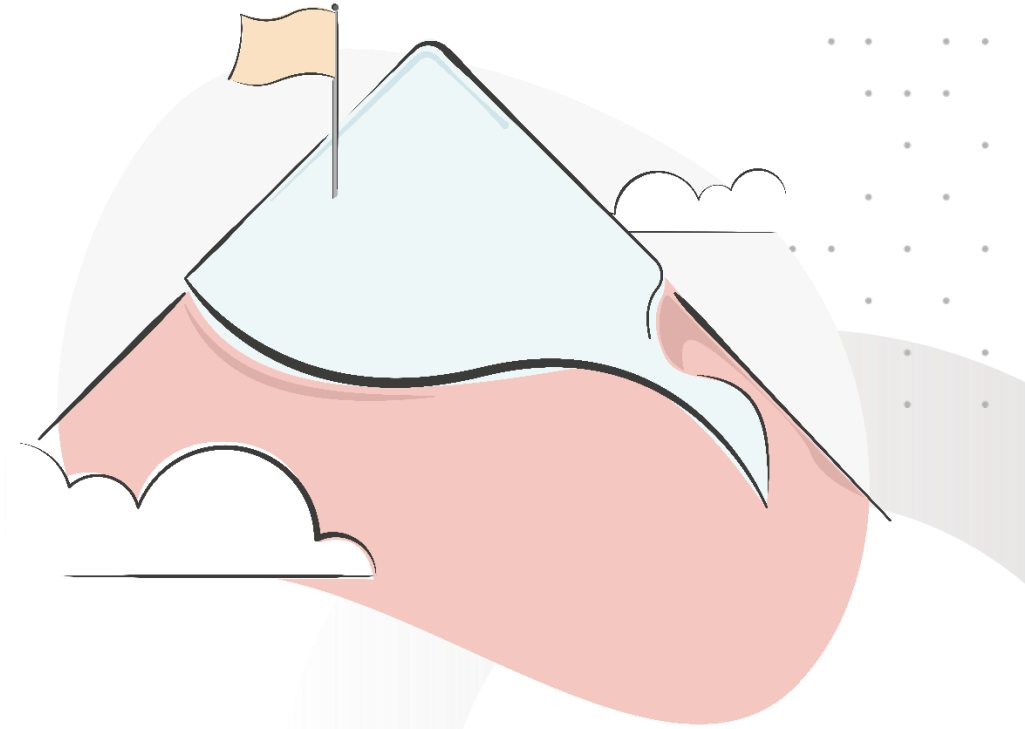
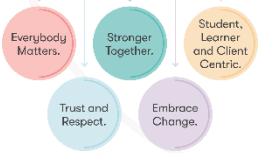


# Session aim and objectives

This webinar supports the following learning outcomes:

- Understand the fundamental principles of the CIA triad and its application in cyber security.
- Recognise risks, vulnerabilities, and threats to ensure robust security for data products.
- 3. Explain security controls and quantify and evaluate the impact of security breaches
- 4. Identify and mitigate common cyber threats

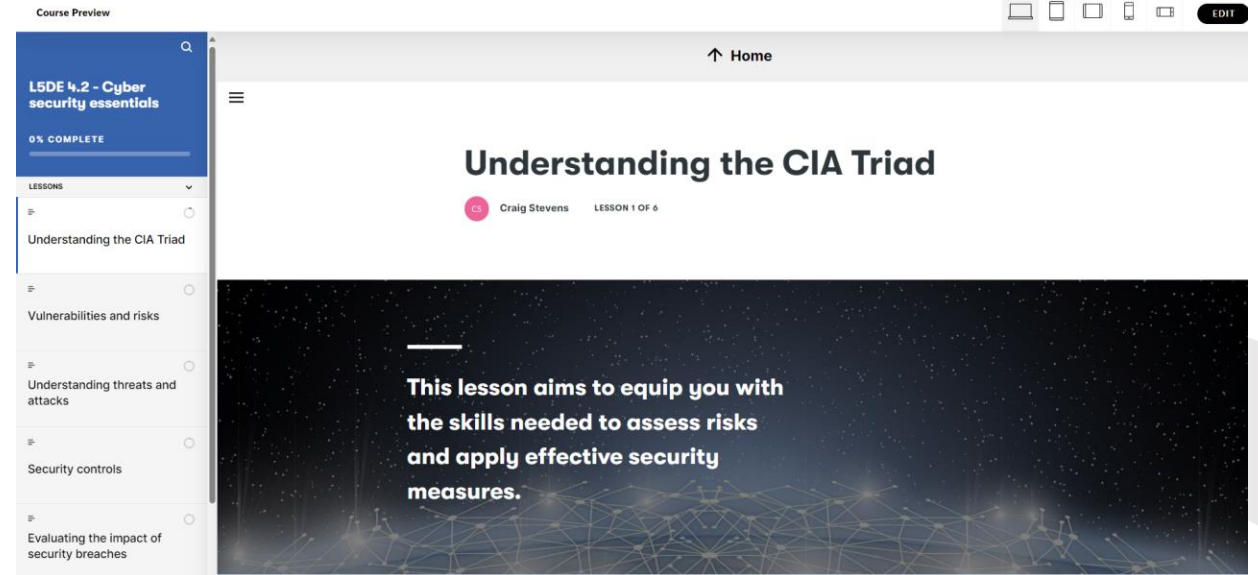
Building Careers  
Through Education



# Recap of e-learning

Are you happy with your learning?

- Risks, Vulnerabilities and Threats
- Attack types
- Security controls



*A screenshot of topic 2 e-learning*

# Webinar Agenda

## What we will cover in the webinar:

### 1. Deep Dive into the CIA Triad

- Explore the core principles of Confidentiality, Integrity, and Availability in cybersecurity.

### 2. Cryptography basics

- How cryptography can aid confidentiality

### 3. NIST Cybersecurity Framework

- Introduce the NIST framework and its core functions for comprehensive security management.

## What we will cover in the webinar:

### • Monitoring Practices and Open-Source Frameworks

Discuss the importance of continuous monitoring and explore open-source security tools to help integrity and availability

### • Binary Risk Assessment

Explain the concept of binary risk assessment and demonstrate its application.

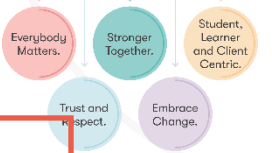
### • Case Study: Financial Impact of a Security Breach

Analyze the financial implications of a security breach and the importance of risk mitigation..



# Introduction to the CIA Triad

Building Careers  
Through Education



## Definition and Importance

The CIA triad is a fundamental concept in cybersecurity that outlines three essential principles for protecting information: Confidentiality, Integrity, and Availability.

## Confidentiality

Protecting sensitive information from unauthorized access, ensuring that only authorized individuals or entities can view and use the data.

## Integrity

Ensuring the accuracy and completeness of data, preventing unauthorised modification or tampering, and maintaining the trustworthiness of information.

## Availability

Ensuring that authorized users have reliable and timely access to information and resources when needed, minimizing disruptions and downtime.

# Confidentiality

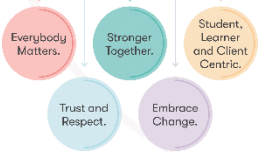
Confidentiality refers to the protection of sensitive data from unauthorised access.

This is a critical aspect of cybersecurity, ensuring that only authorised individuals or entities can view and handle the information.

**Impact: Reducing risk of data breaches**



Building Careers  
Through Education



# Confidentiality approaches

What you need to know...

- **Access Controls:** Restricting data access to authorised users
- **Authentication Protocols:** Verifying user identities
- **Encryption:** Scrambling data to protect it

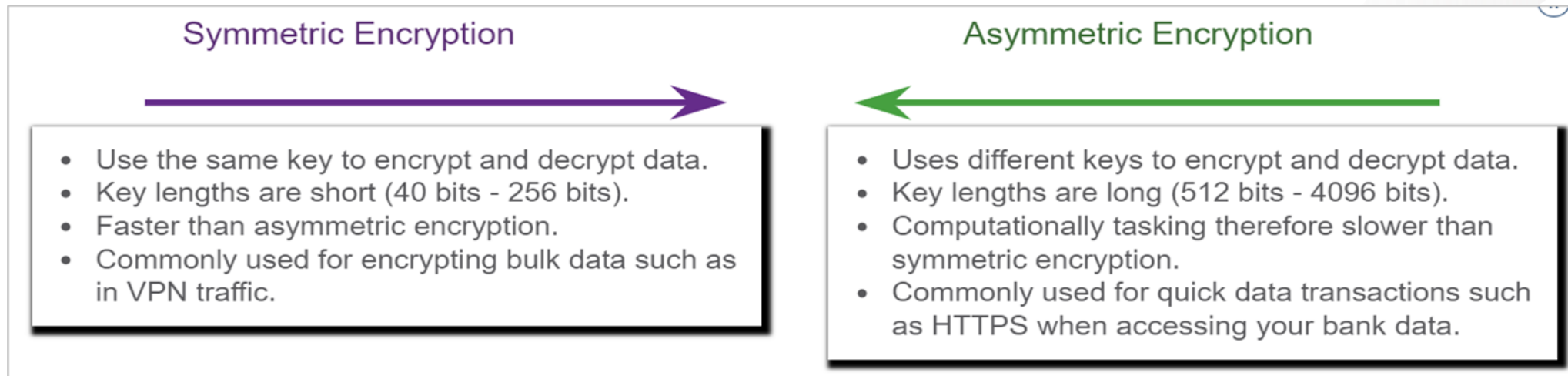
We will learn about symmetric and assymetric encryption. They are cryptographic methods (cryptography is a branch of applied maths dealing with keeping secrets!)



# Confidentiality

## Data confidentiality...

- There are two classes of encryption used to provide data confidentiality; asymmetric and symmetric. These two classes differ in how they use keys.
- Symmetric encryption algorithms such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key.
- Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).
- The figure highlights some differences between symmetric and asymmetric encryption.

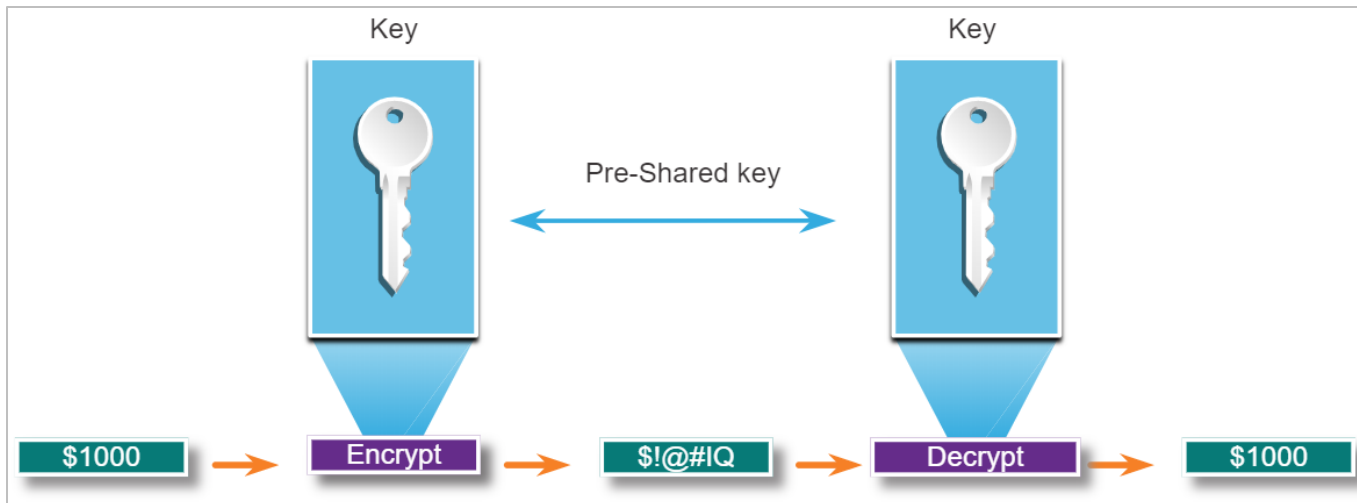




# Confidentiality

## Symmetric encryption...

- Symmetric algorithms use the same pre-shared key (secret key) to encrypt and decrypt data.
- Symmetric encryption algorithms are commonly used with VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
- When using these algorithms, the longer the key, the longer it will take for someone to discover the key.
- Most encryption keys are between 112 and 256 bits. Use a longer key for more secure communications.
- Symmetric encryption algorithms are sometimes classified as a block cipher or a stream cipher.



# Confidentiality

## Symmetric encryption (cont)...

Well-known symmetric encryption algorithms are described in the table.

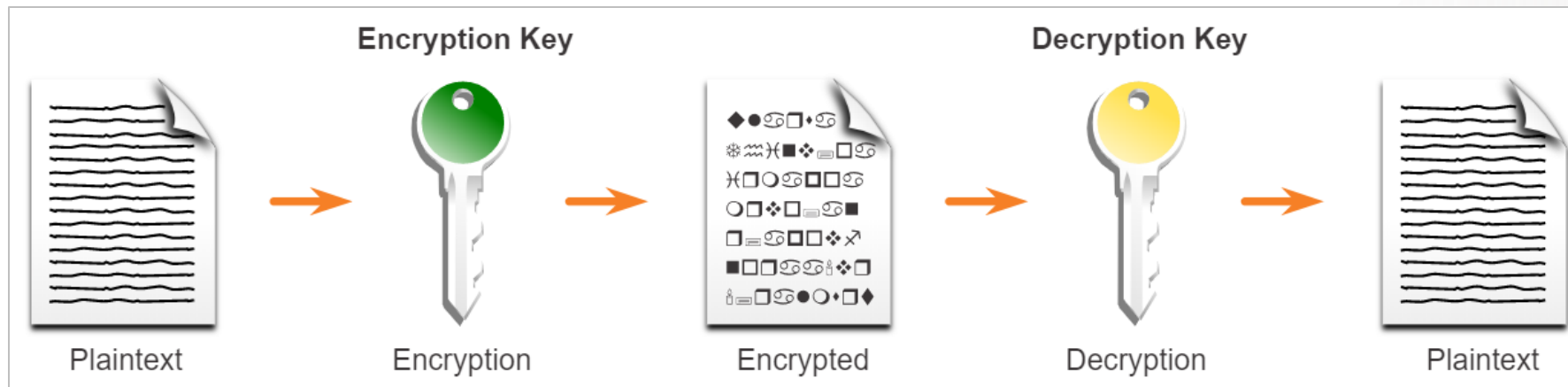
| Symmetric Encryption Algorithms                | Description   |
|--|---|
| Data Encryption Standard (DES)                 | This is a legacy algorithm. It uses a short key length that makes it insecure.  |
| 3DES (Triple DES)                              | This is the replacement for DES and repeats the DES algorithm three times. It should be avoided as it is scheduled to be retired in 2023. If implemented, use very short key lifetimes. |
| Advanced Encryption Standard (AES)             | It offers combinations of 128-, 192-, or 256-bit keys to encrypt 128, 192, or 256 bit-long data blocks.   |
| Software-Optimized Encryption Algorithm (SEAL) | It is a stream cipher that uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.   |
| Rivest ciphers (RC) series algorithms          | RC4 is a stream cipher that was used to secure web traffic. It has been found to have multiple vulnerabilities which have made it insecure. RC4 should not be used.                     |



# Confidentiality

## Asymmetric encryption...

- Asymmetric algorithms, also called public-key algorithms, are designed in a way that the encryption and the decryption keys are different.
- Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for decryption.
- The process is also reversible. Data that is encrypted with the public key requires the private key to decrypt.
- Asymmetric algorithms achieve confidentiality and authenticity by using this process.
- Asymmetric encryption can use key lengths between 512 to 4,096 bits.
- Asymmetric algorithms are substantially slower than symmetric algorithms.

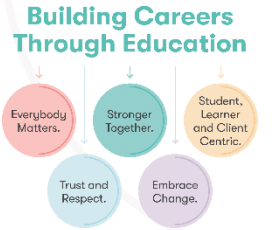


# Confidentiality

## Asymmetric encryption (cont)...

Common examples of asymmetric encryption algorithms are described in the table.

| Asymmetric Encryption Algorithms                                       | Key Length                  | Description  |
|--|-----------------------------|--|
| Diffie-Hellman (DH)  | 512, 1024, 2048, 3072, 4096 | This algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used, given the number and the outcome. |
| Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA) | 512 – 1024                  | It specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA, but is 10 to 40 times slower for verification.  |
| Elliptic curve techniques  | 224 or higher               | Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.   |

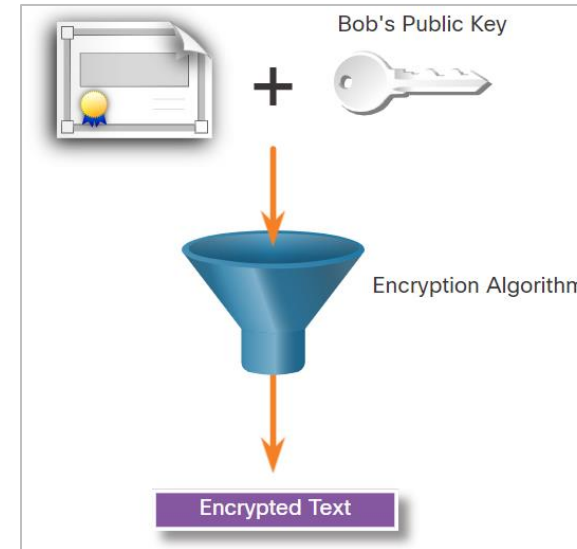


# Confidentiality

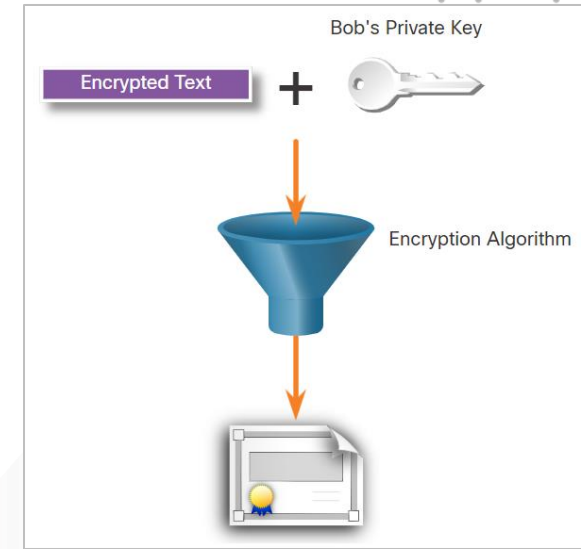
## Asymmetric encryption – confidentiality

- Asymmetric algorithms are used to provide confidentiality without pre-sharing a password.
- The confidentiality objective of asymmetric algorithms is initiated when the encryption process is started with the public key.
- The process can be summarized using the formula: **Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality**
- When the public key is used to encrypt data, the private key must be used to decrypt data.
- Only one host has the private key; therefore, confidentiality is achieved.

### Example: Data exchange between Bob and Alice



Alice acquires and uses Bob's public key to encrypt a message and then send it to Bob.



Bob decrypts the message with the private key and as he is the only one with the private key, confidentiality is achieved.

# Confidentiality

## Asymmetric encryption - authentication...

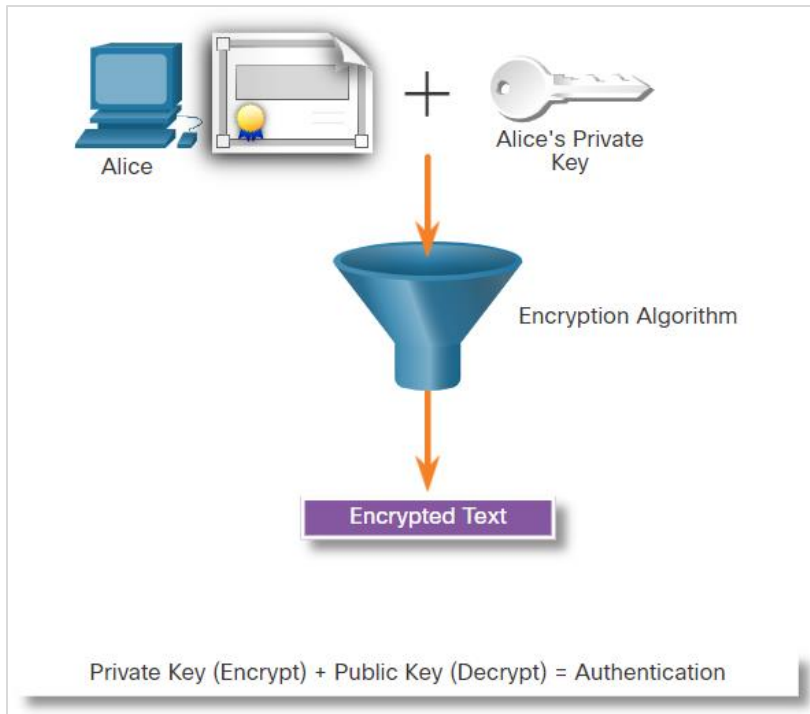
- The authentication objective of asymmetric algorithms is initiated with the private key encryption process.
- The process can be summarized using the formula: **Private Key (Encrypt) + Public Key (Decrypt) = Authentication**
- When the private key is used to encrypt the data, the corresponding public key must be used to decrypt the data.
- Because only one host has the private key, only that host could have encrypted the message, providing authentication of the sender.
- When a host successfully decrypts a message using a public key, it is trusted that the private key encrypted the message, which verifies who the sender is. This is a form of authentication.



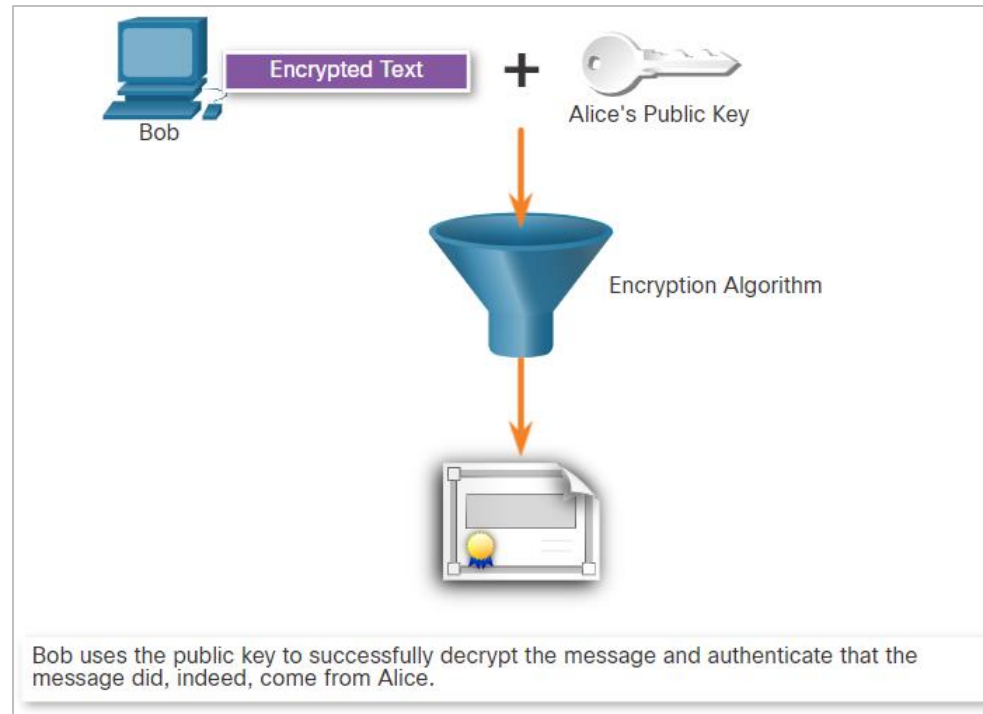
# Confidentiality

## Asymmetric encryption - authentication

- Let's see how the private and public keys can be used to provide authentication to the data exchange between Bob and Alice.



**Alice uses her private key**  
Alice encrypts a message using her private key and sends it to Bob.

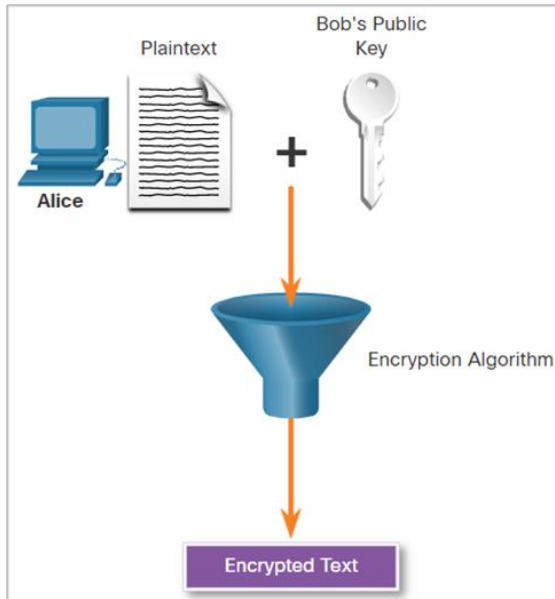


**Bob decrypts using the public key**  
After Bob obtains Alice's public key, he uses it to decrypt the message and to authenticate that the message has been received from Alice.

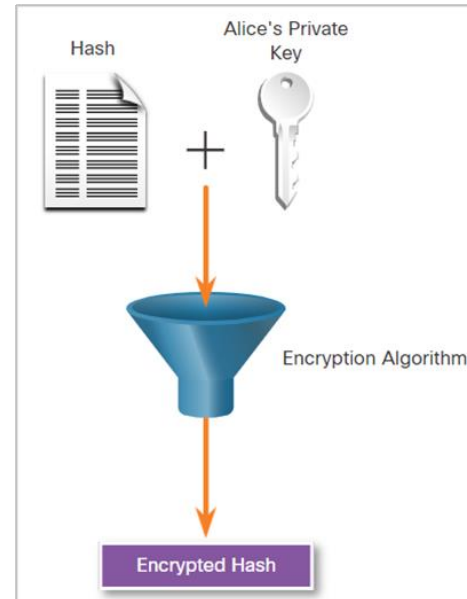
# Confidentiality

## Asymmetric encryption - Integrity

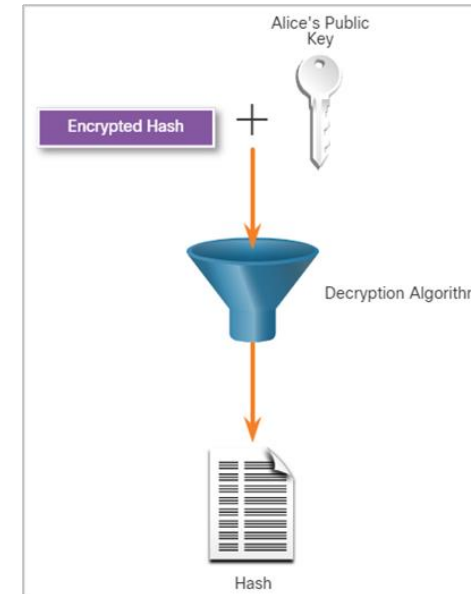
- Combining the two asymmetric encryption processes provides message confidentiality, authentication, and integrity. In this example, a message will be ciphered using Bob's public key and a ciphered hash will be encrypted using Alice's private key.



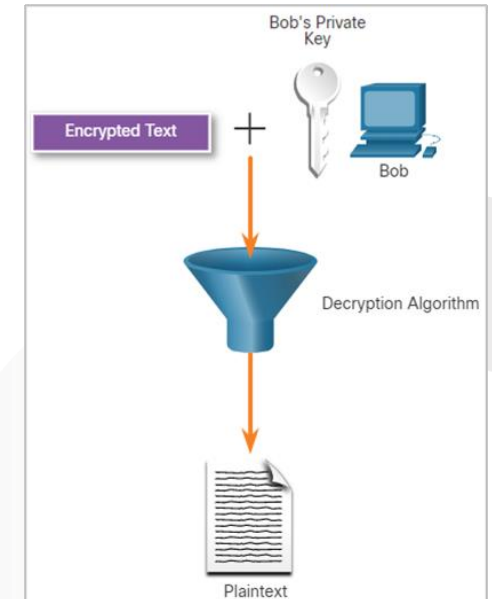
Alice uses Bob's Public Key



Alice encrypts a hash using her private key



Bob uses Alice's public key to decrypt the hash

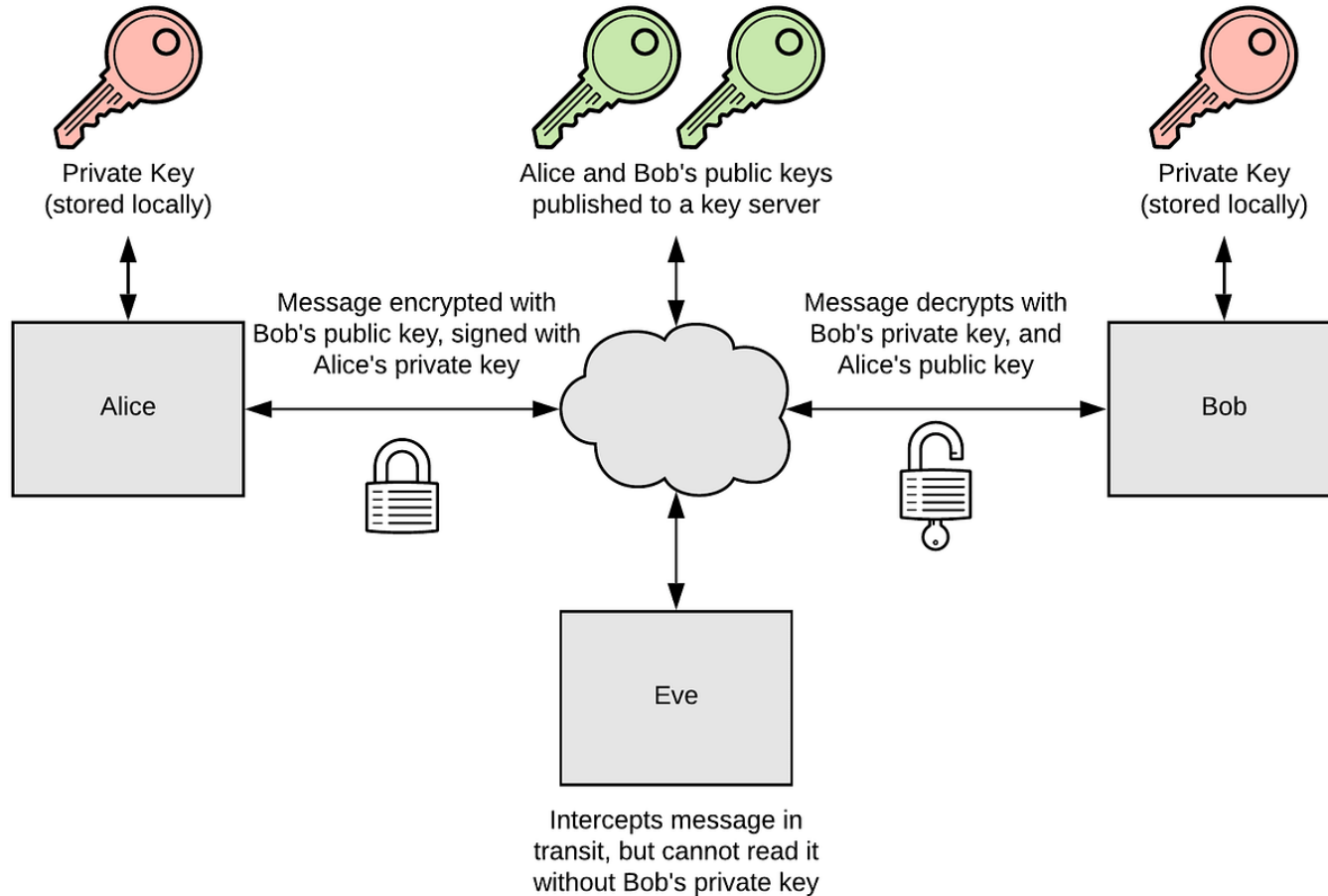


Bob uses his private key to decrypt the message

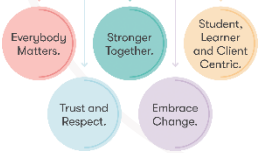


# Discussion

## Confidentiality - Encrypting and Decrypting Data Using asymmetric encryption



Building Careers  
Through Education



**Submit your responses to  
the chat!**



# Lab

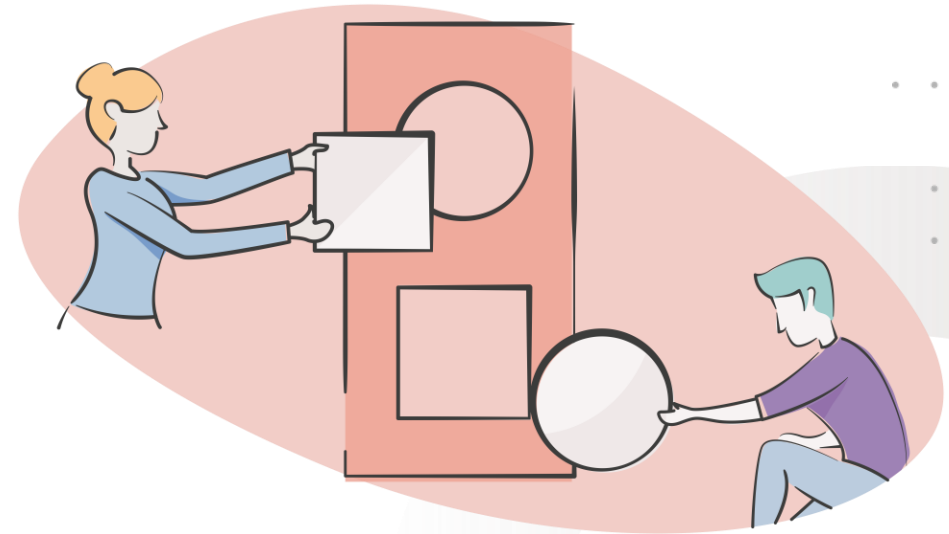
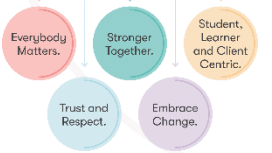
## Confidentiality - Encrypting and Decrypting Data Using asymmetric encryption

In this lab, you will complete the following objectives:

- Encrypting Messages with AES
- Decrypting Messages with AES

<https://encode-decode.com>

Building Careers  
Through Education



# Example

- Password - Pass
- Message - this is another example
- Encryption - DNkmsOBwZmjU0J4Q1idnTbZvWB6iMbdTrr1LfwbPQas=

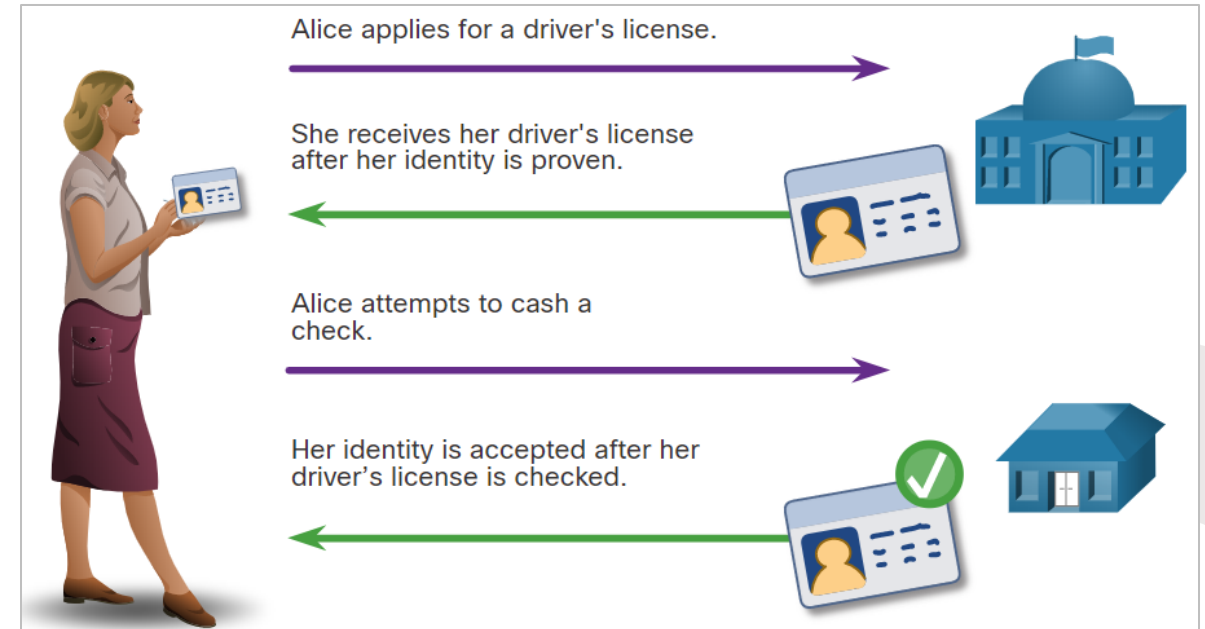
Building Careers  
Through Education



# Public key management

## Authorities and the PKI trust system

- When establishing an asymmetric connection between two hosts, the hosts will exchange their public key information
- Trusted third parties on the Internet validate the authenticity of these public keys using digital certificates. The third-party issues credentials that are difficult to forge.
- From that point forward, all individuals who trust the third party simply accept the credentials that the third-party issues.
- The Public Key Infrastructure (PKI) consists of specifications, systems, and tools that are used to create, manage, distribute, use, store, and revoke digital certificates.
- The Certificate Authority (CA) creates digital certificates by tying a public key to a confirmed identify, such as a website or individual.

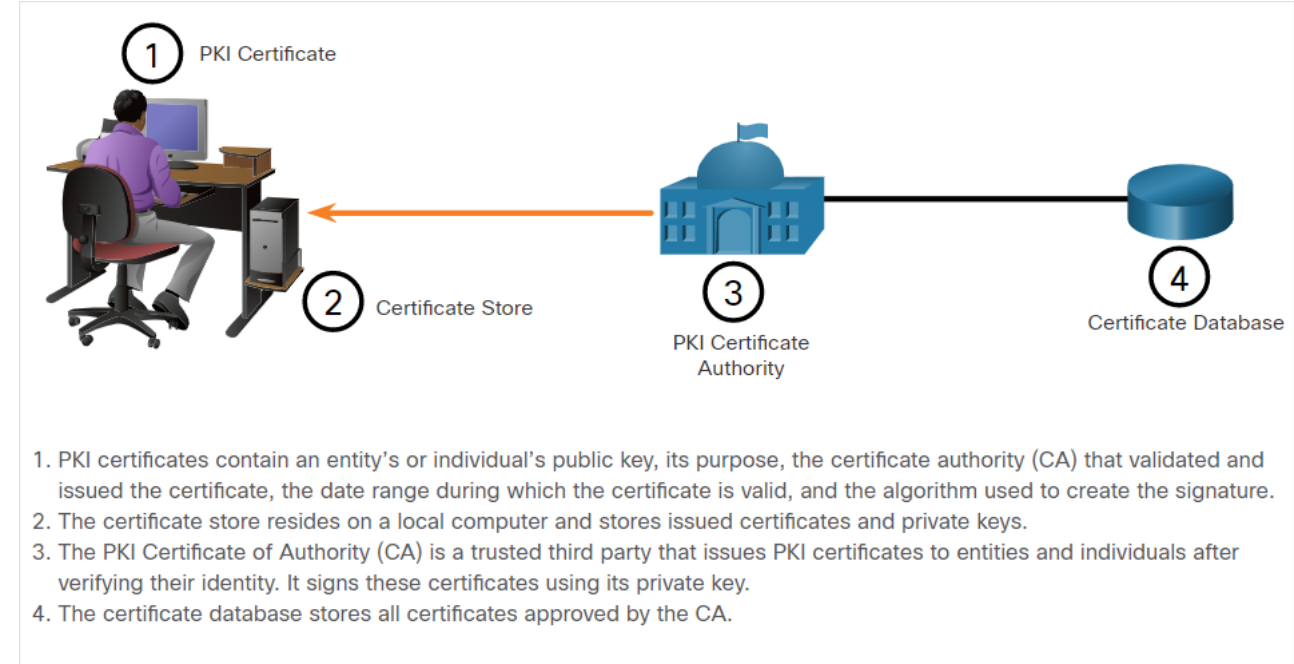


Illustrates how a driver's license is analogous to a digital certificate

# The public key infrastructure

## Authorities and the PKI trust system

- PKI is needed to support large-scale distribution and identification of public encryption keys.
- The PKI framework facilitates a highly scalable trust relationship.
- It consists of the hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
- The figure shows the main elements of the PKI.

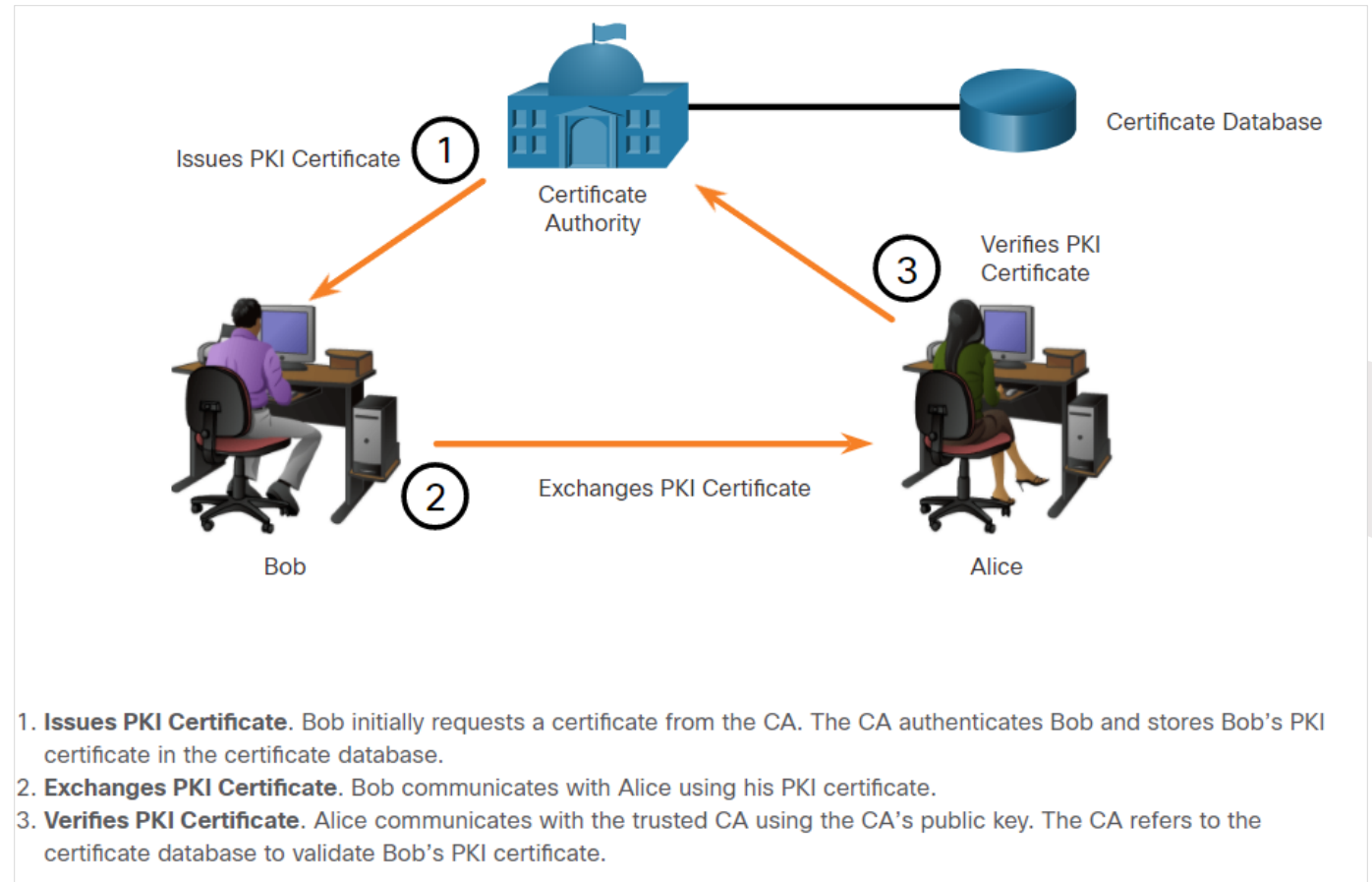


# The public key infrastructure

## Authorities and the PKI trust system

This figure shows how the elements of the PKI interoperate:

**Note:** Not all PKI certificates are directly received from a CA. A Registration Authority (RA) is a subordinate CA and is certified by a root CA to issue certificates for specific uses.



# The PKI authorities system

## Authorities and the PKI trust system

- Many vendors provide CA servers as a managed service or as an end-user product.
- Organizations may also implement private PKIs using Microsoft Server or Open SSL.
- CAs issue certificates based on classes which determine how trusted a certificate is.
- The class number is determined by how rigorous the procedure was that verified the identity of the holder when the certificate was issued.
- The higher the class number, the more trusted the certificate.
- Some CA public keys are preloaded, such as those listed in web browsers.

| Class | Description  |
|-------|--|
| 0     | Used for testing in situations in which no checks have been performed. |
| 1     | Used by individuals who require verification of email.                 |
| 2     | Used by organizations for which proof of identity is required.         |
| 3     | Used for servers and software signing.                                 |
| 4     | Used for online business transactions between companies.               |
| 5     | Used for private organisations or government security.                 |

**Note:** An enterprise can also implement PKI for internal use. PKI can be used to authenticate employees who are accessing the network. In this case, the enterprise is its own CA.

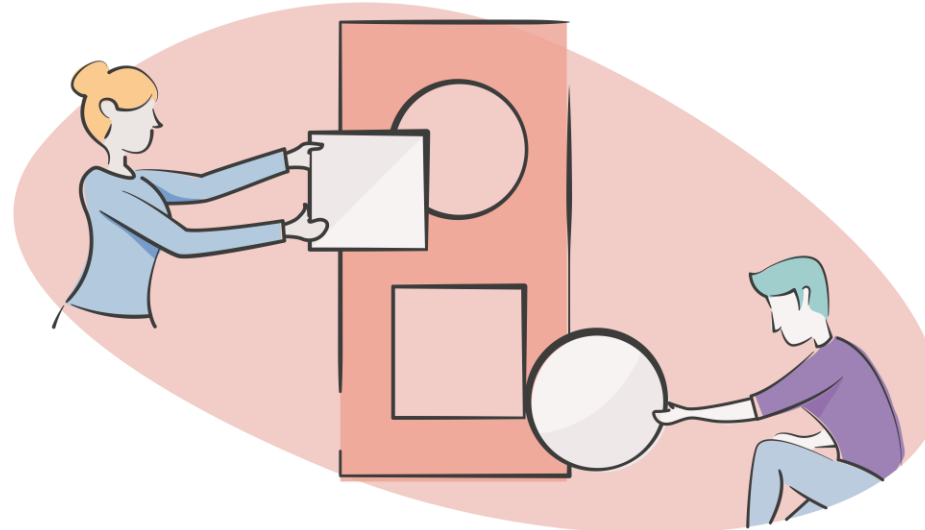


# Lab – Certificate authority stores

## Authorities and the PKI trust system

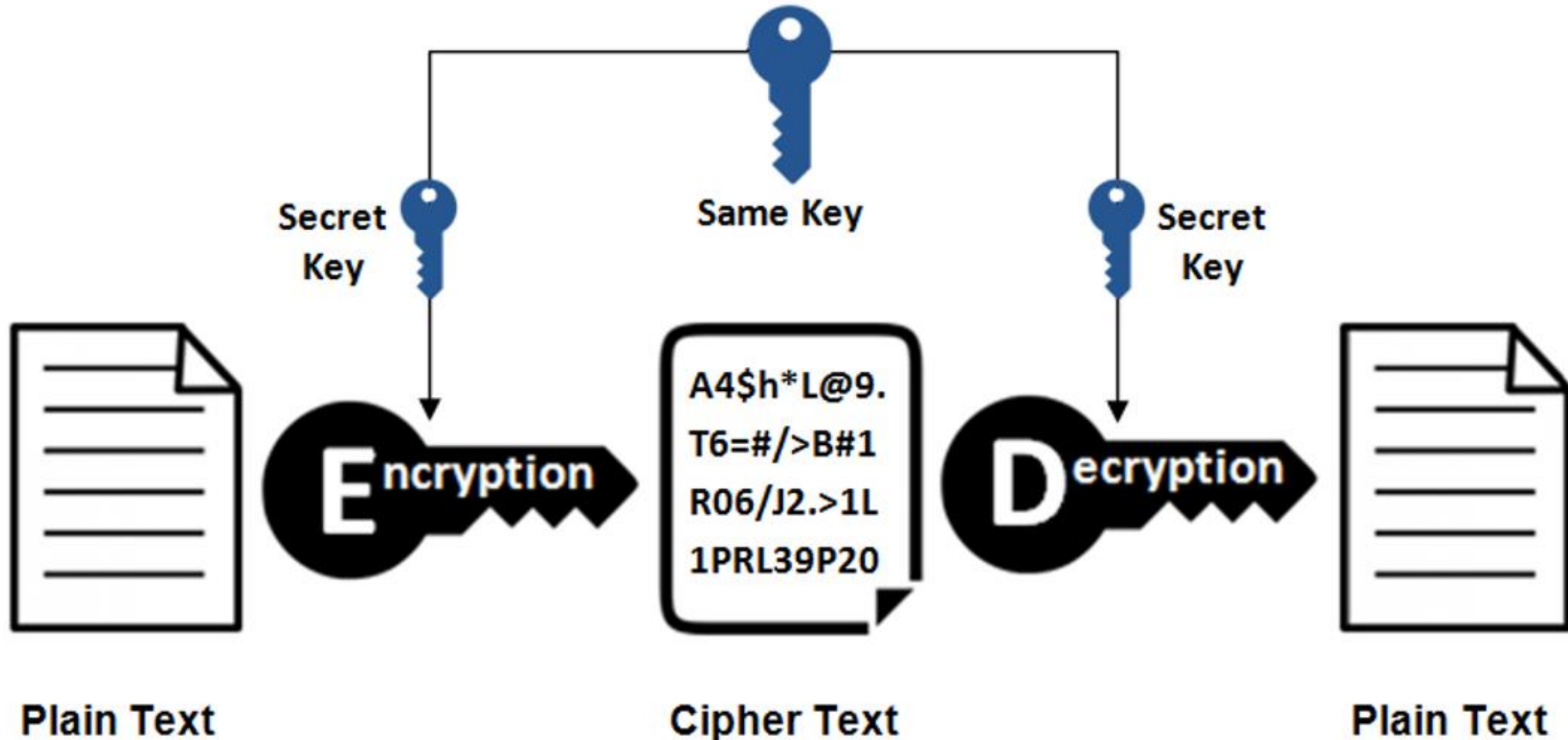
In this lab, you will complete the following objectives:

- Certificates Trusted by Your Browser
- Using chrome or any other browser View your certificates.

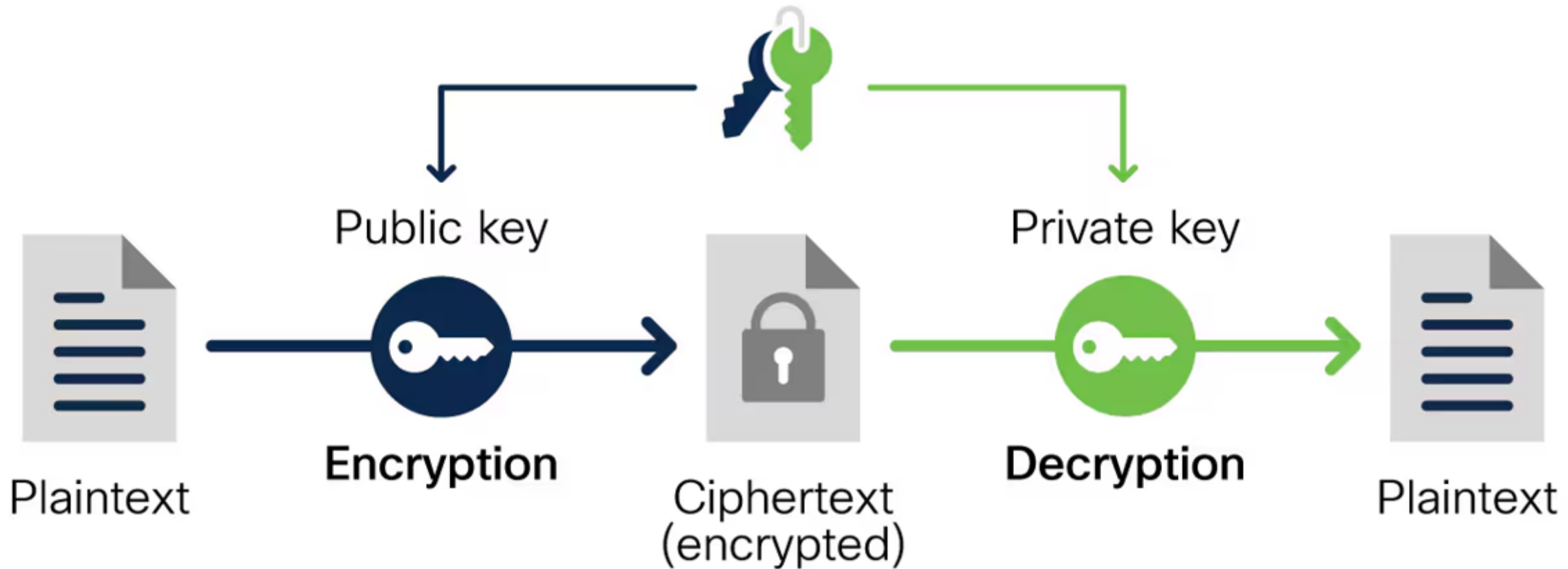




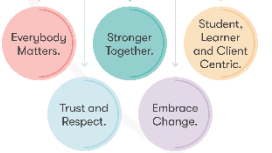
# Summary: symmetric encryption



# Summary: asymmetric encryption

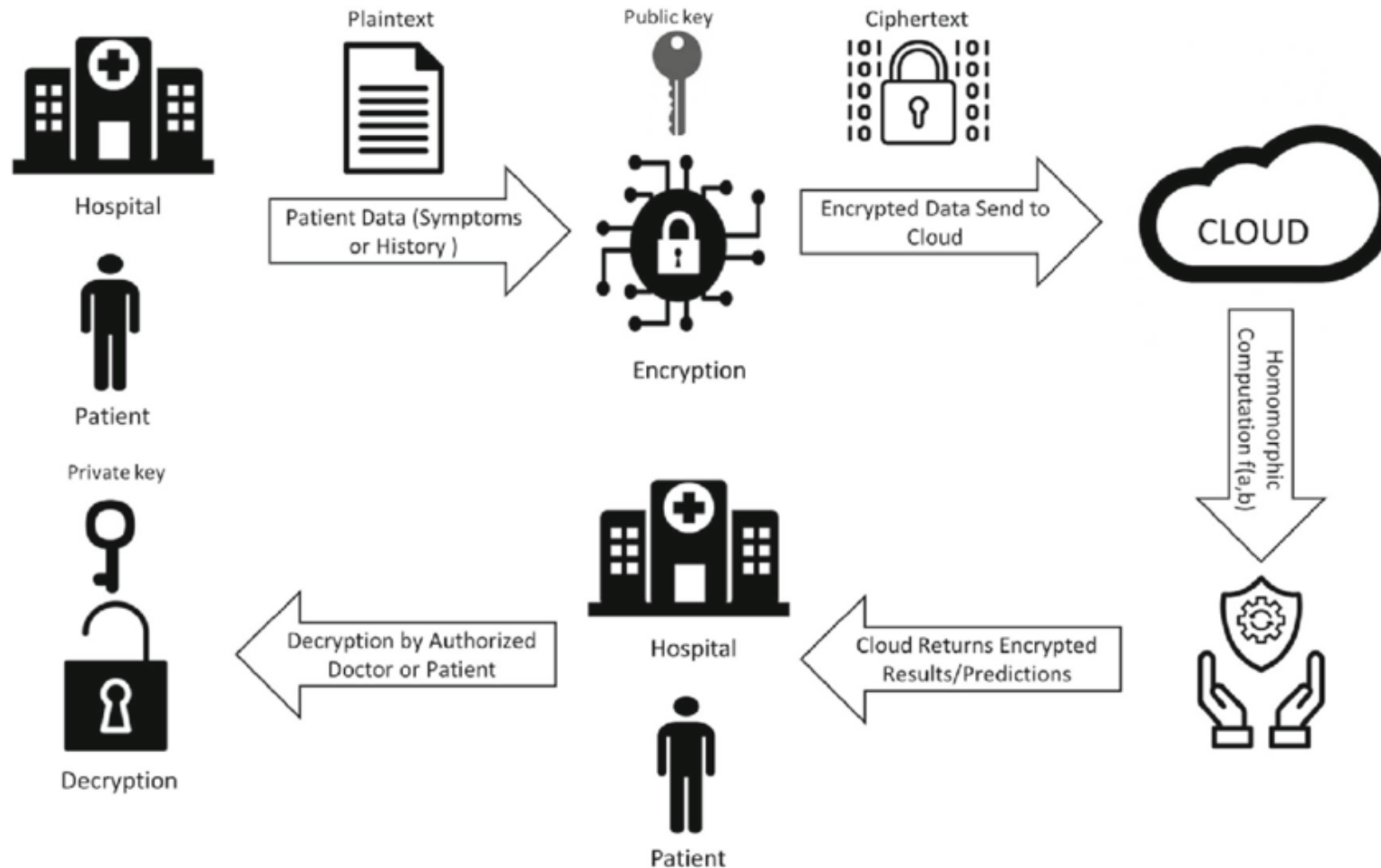


Building Careers  
Through Education

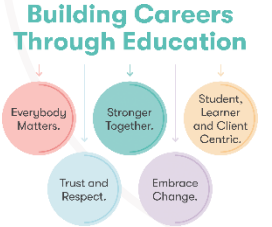


# Confidentiality case study discussion

Healthcare provider shares patient records. Discuss how confidentiality can be implemented.



Submit your responses to the chat!



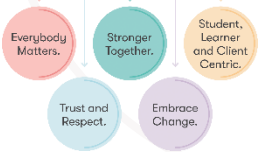
# Access Control Mechanism

**NIST** defines **Access Control Mechanism** as a logical component that serves to receive the access request for an **Object** from a **Subject** and decide & enforce the access decision.



# Authentication

- Authentication
  - Who are you?
  - “I am user **student** and my password **validateme** proves it.”
- Authorization
  - What can you do? What can you access?
  - “User **student** can access host **serverXYZ** using Telnet.”
- Accounting
  - What did you do? How long did you do it?  
How often did you do it?
  - “User **student** accessed host **serverXYZ** using Telnet for **15 minutes.**”



# Integrity

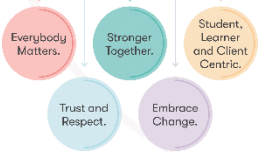
Integrity refers to the ability to maintain data accuracy and reliability. This is crucial for ensuring the trustworthiness and dependability of information.

Some key techniques used to preserve data integrity include checksums, hash functions, and digital signatures.

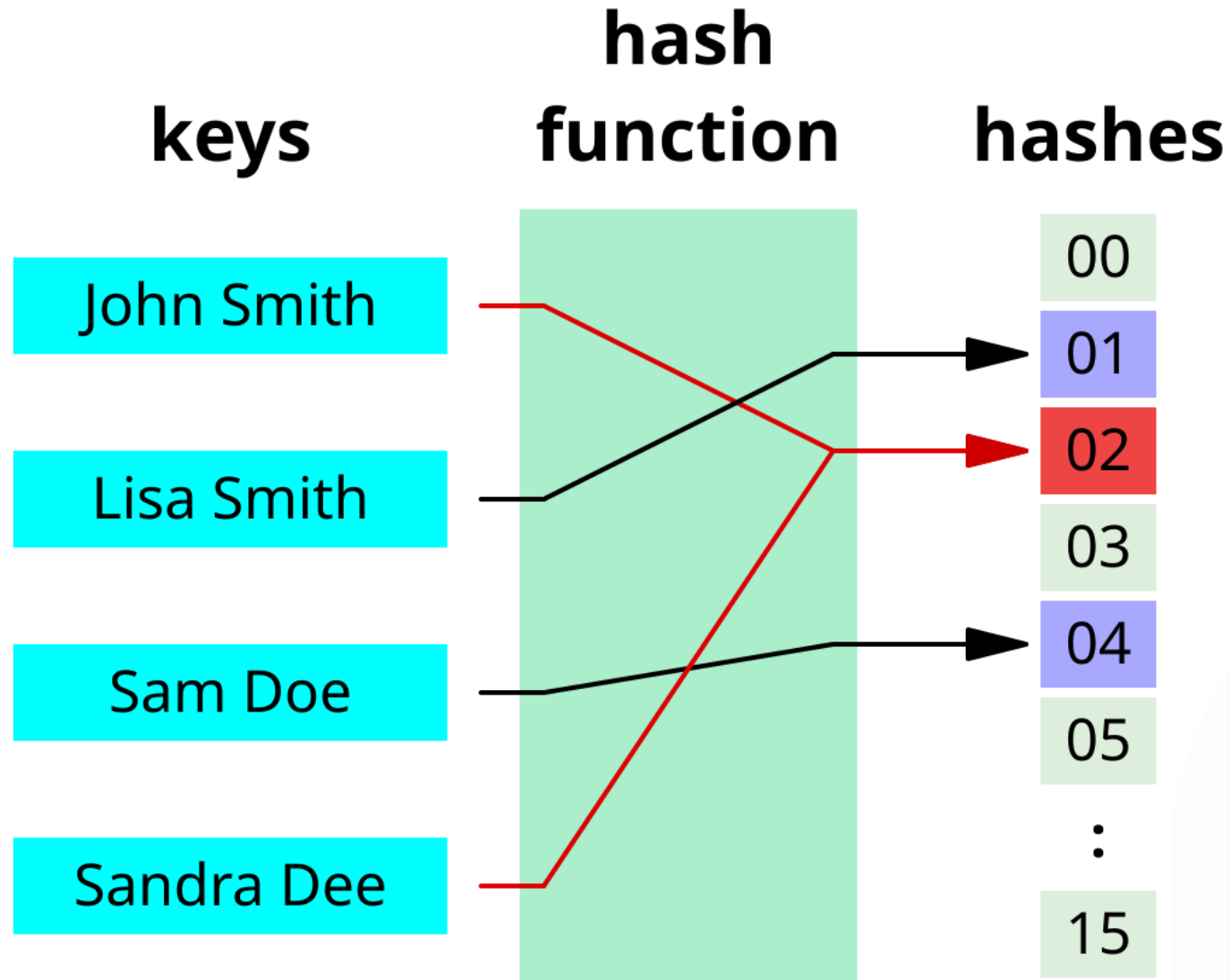
**Impact: Preventing data tampering**



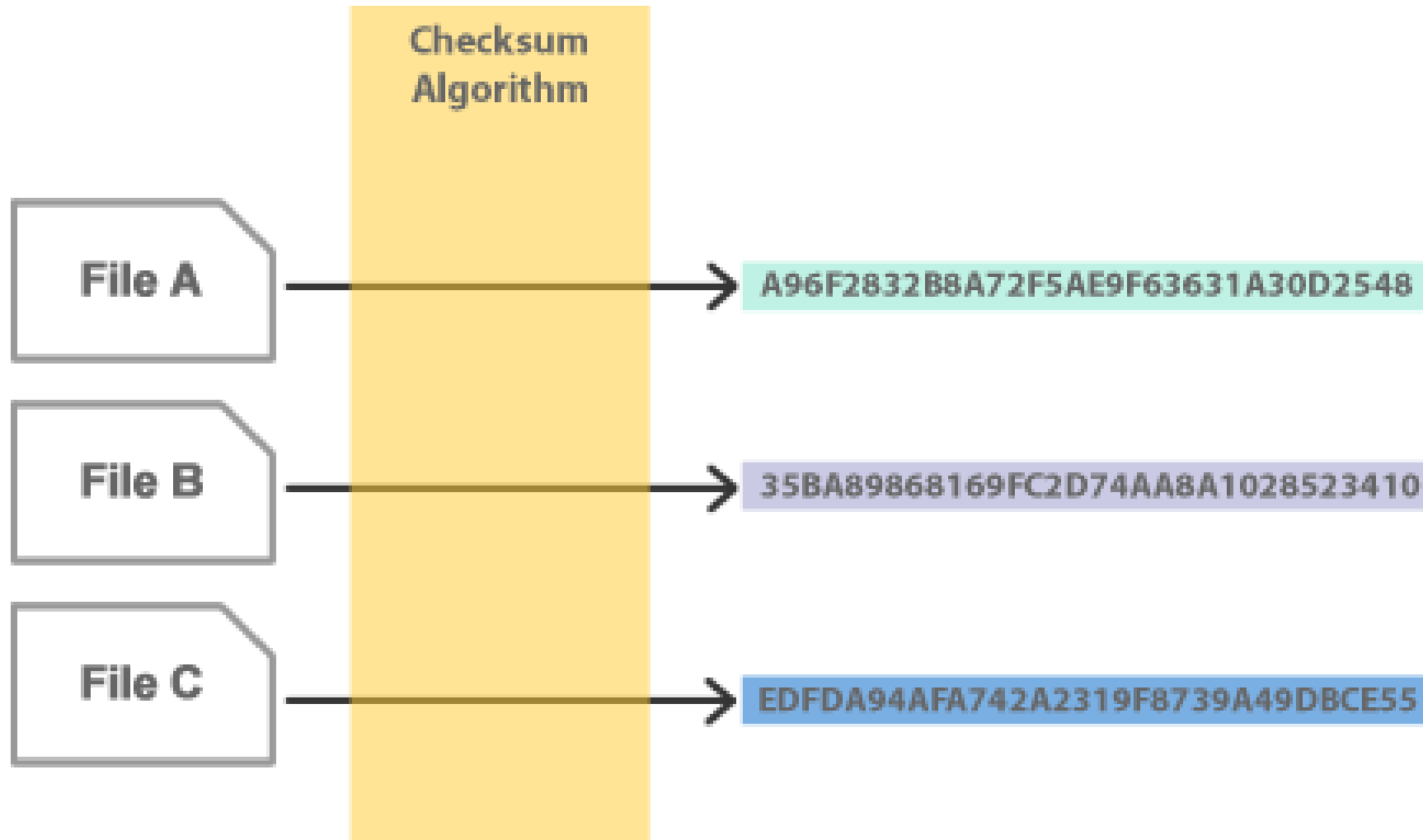
Building Careers  
Through Education



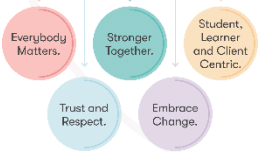
# Keys and hash functions



# Check sum algorithms



Building Careers  
Through Education





# Integrity

Integrity refers to the ability to maintain data accuracy and reliability. This is crucial for ensuring the trustworthiness and dependability of information.

Some key techniques used to preserve data integrity include checksums, hash functions, and digital signatures.

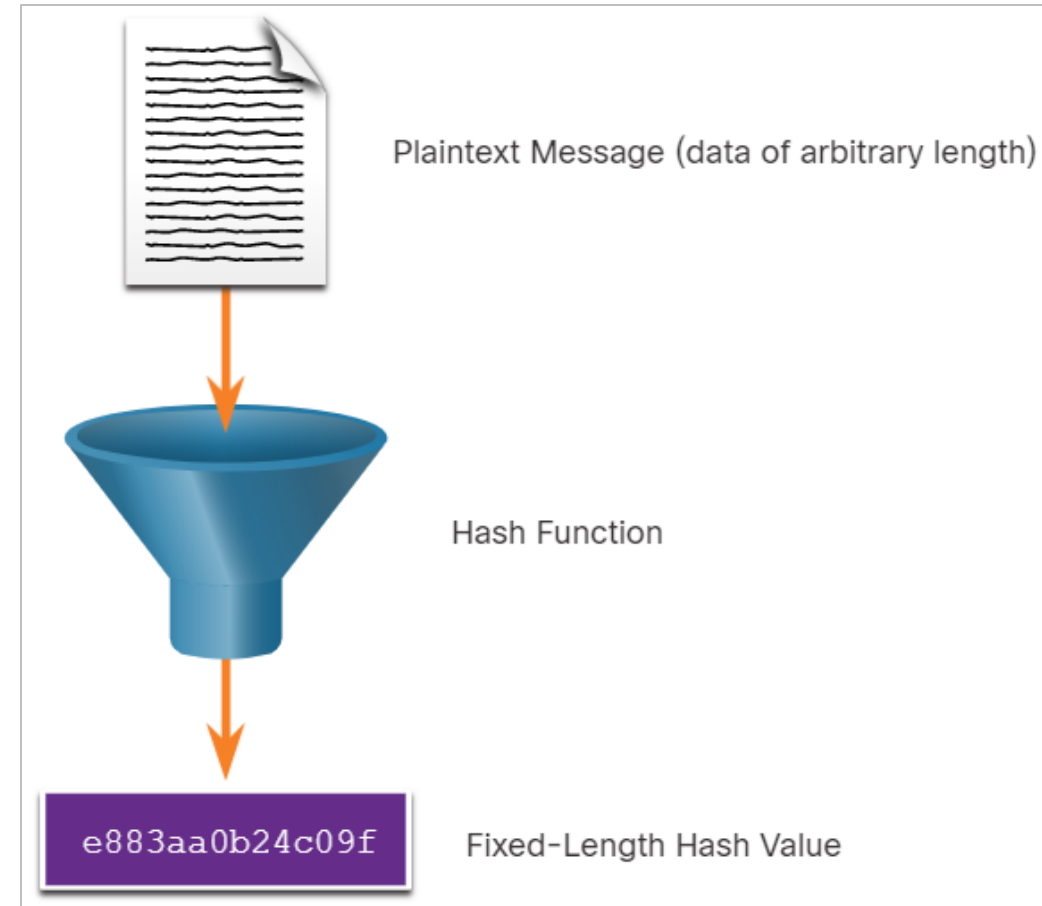
**Impact: Preventing data tampering**



# Cryptography

## Cryptographic hash functions

- Hashes are used to verify and ensure data integrity.
- Hashing is based on a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse.
- A hash function takes a variable block of binary data, called the message, and produces a fixed-length, condensed representation, called the hash.
- The resulting hash is also sometimes called the message digest, digest, or digital fingerprint.
- With hash functions, it is computationally infeasible for two different sets of data to come up with the same hash output.
- Every time the data is changed or altered, the hash value also changes.



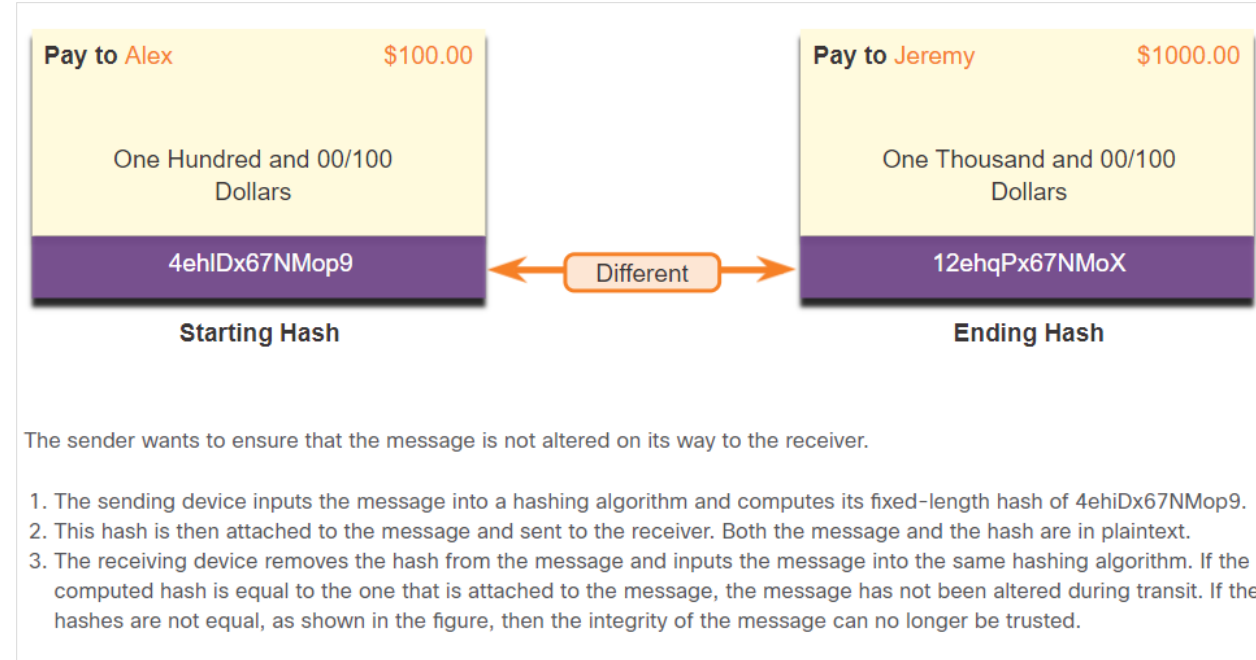
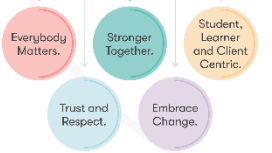
# Cryptography

## MD5 and SHA

There are four well-known hash functions:

- **MD5 with 128-bit digest** - A one-way function that produces a 128-bit hashed message. MD5 is a legacy algorithm.
- **SHA-1** - Very similar to the MD5 hash functions. SHA-1 creates a 160-bit hashed message and is slightly slower than MD5.
- **SHA-2** - If you are using SHA-2, then SHA-256, SHA-384, and SHA-512 algorithms should be used.
- **SHA-3** - Next-generation algorithms and should be used whenever possible.

Building Careers  
Through Education

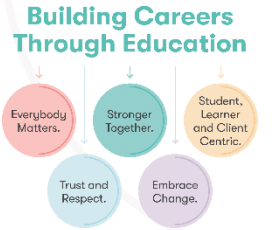


# Cryptography

## Origin authentication

- To add origin authentication and integrity assurance, use a keyed-hash message authentication code (HMAC).
- HMAC uses an additional secret key as input to the hash function.

**Note:** *Other Message Authentication Code (MAC) methods are also used. However, HMAC is used in many systems including SSL, IPsec, and SSH.*



# Lab

## Integrity - Hashing Data Using

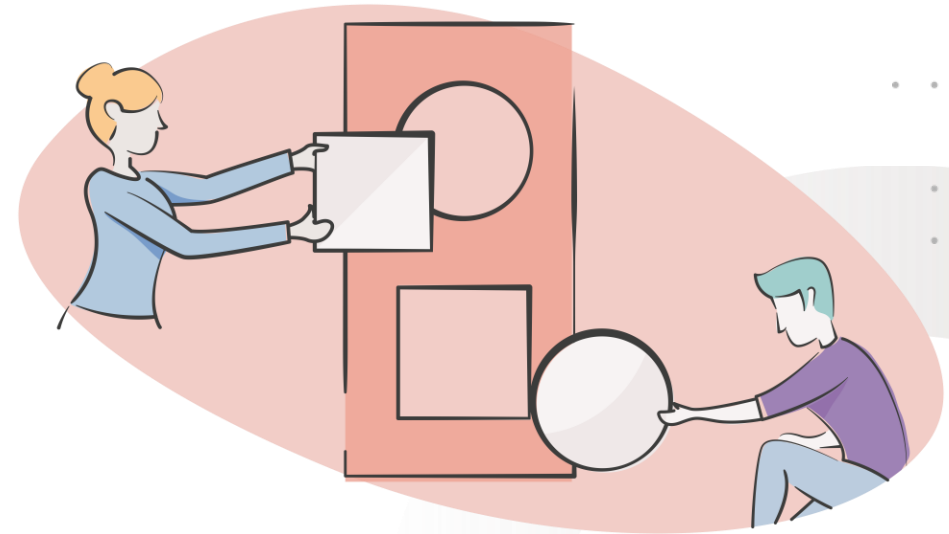
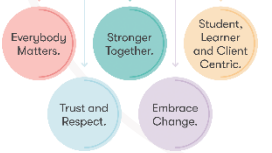
In this lab, you will complete the following objectives:

- Encrypting Messages with SHA

In sha 512 encode “this is an example”

<https://encode-decode.com/>

Building Careers  
Through Education



# Public Key Cryptography

## Using digital signatures

Digital signatures are a mathematical technique used to provide authenticity, integrity, and nonrepudiation.

- Digital signatures use asymmetric cryptography.
- Digital signatures are commonly used in the following two situations:
  - **Code signing** - Code signing is used to verify the integrity of executable files downloaded from a vendor website. It also uses signed digital certificates to authenticate and verify the identity of the site that is the source of the files.
  - **Digital certificates** - These are used to authenticate the identity of a system with a vendor website and establish an encrypted connection to exchange confidential data

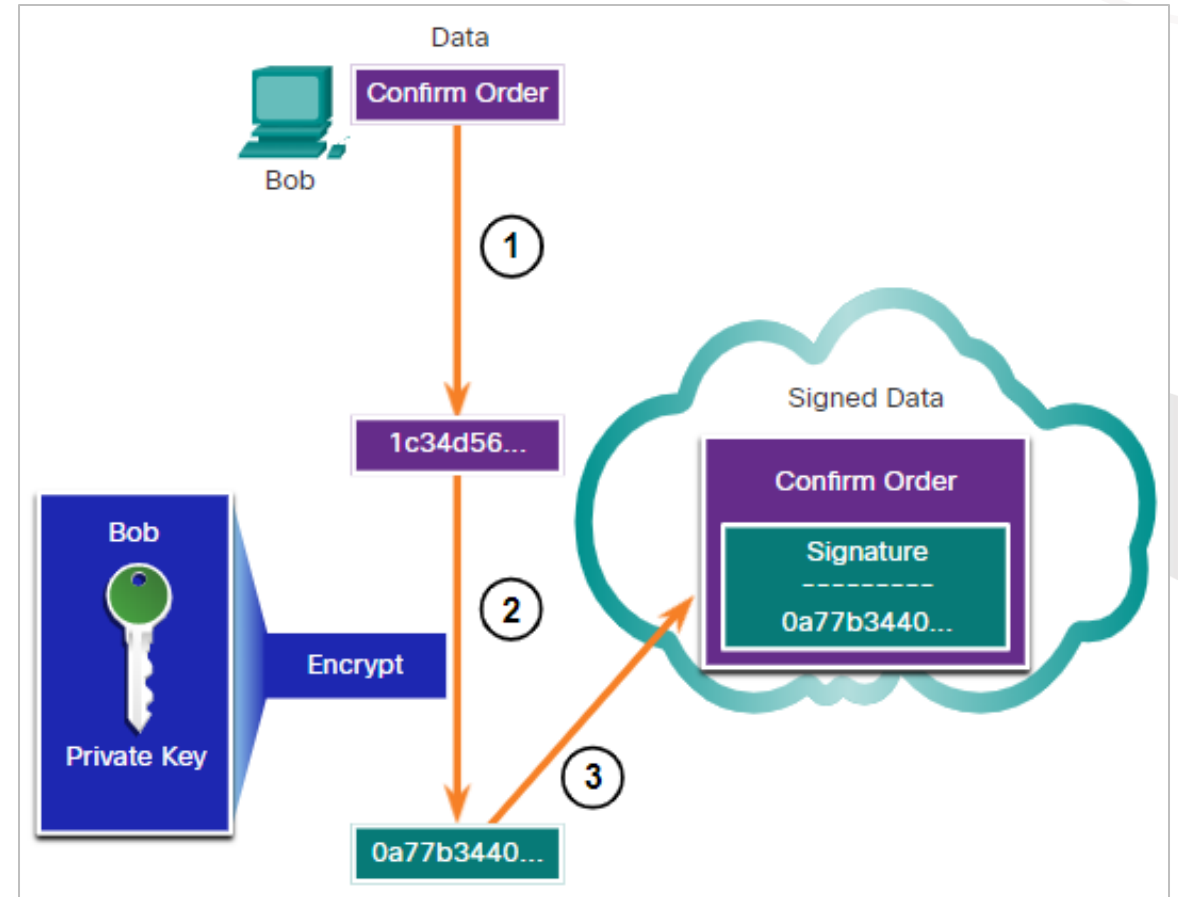


# Public Key Cryptography

## Digital signatures for digital

This scenario will help you understand how a digital signature is used.

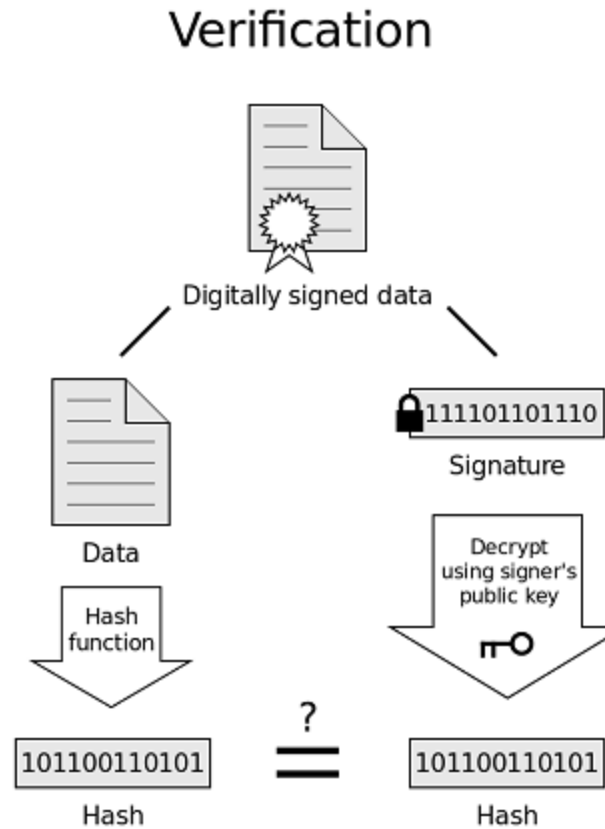
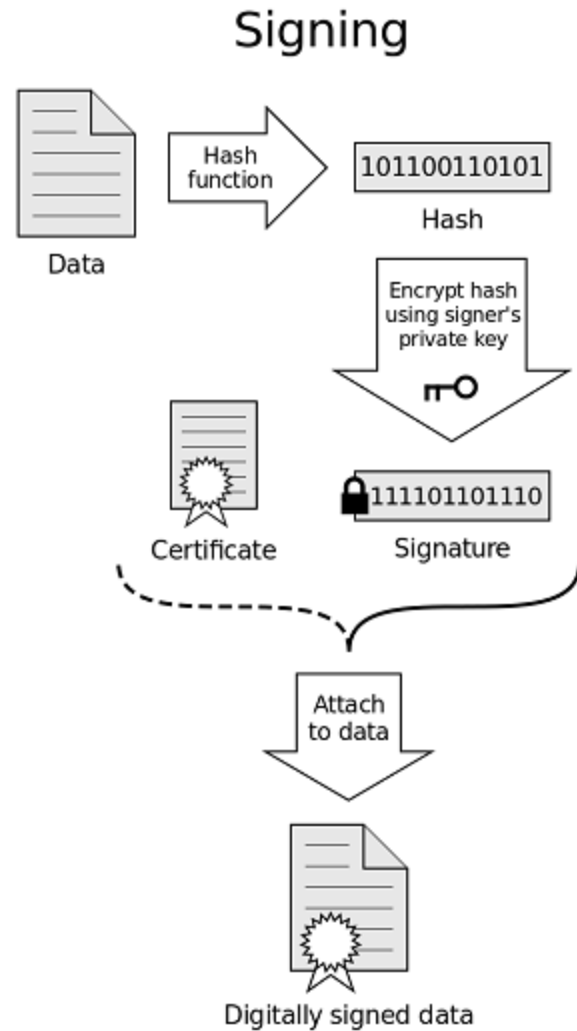
- Bob is confirming an order with Alice, which she is ordering from Bob's website.
- Bob confirms the order and his computer creates a hash of the confirmation.
- The computer encrypts the hash with Bob's private key.
- The encrypted hash, which is the digital signature, is added to the document.
- The order confirmation is then sent to Alice over the internet.



Building Careers  
Through Education



# Signing and verification



If the hashes are equal, the signature is valid.

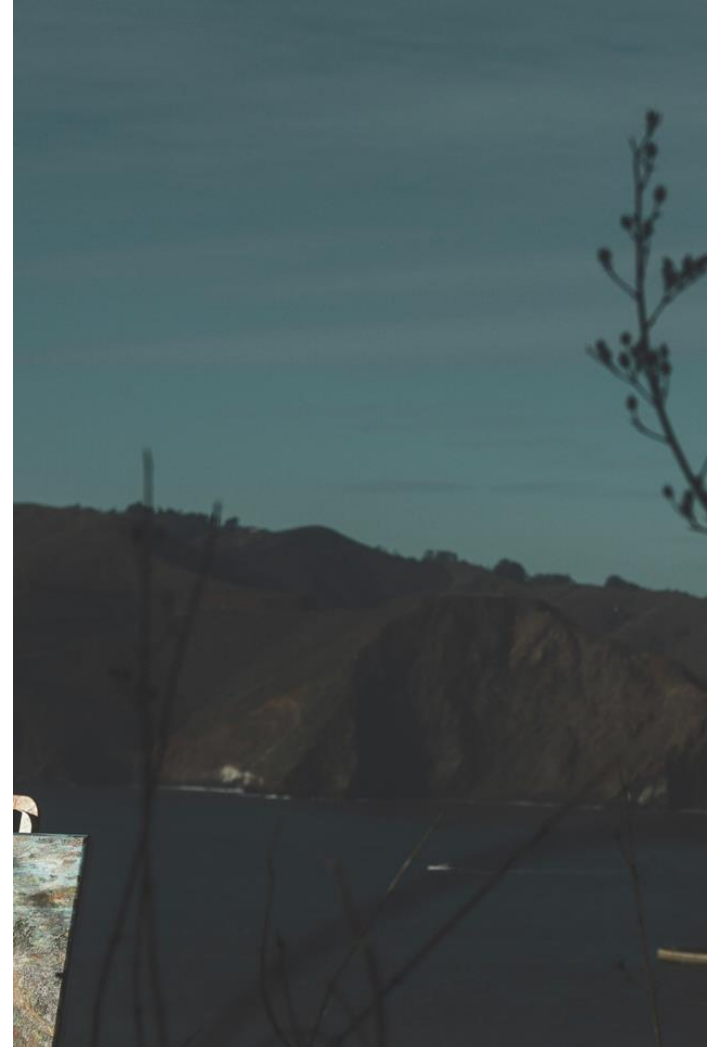


# Availability

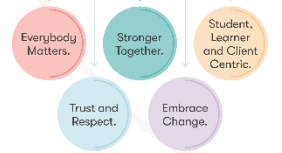
Ensuring authorized users have timely access to data is a critical aspect of cybersecurity.

Redundancy, failover mechanisms, and regular backups are key to maintaining data availability and minimizing downtime.

For example, an online retailer may implement redundant systems and automatic failover to standby servers to ensure their e-commerce platform remains accessible to customers, even in the event of a system failure.



## Building Careers Through Education



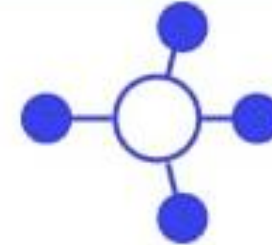
# Best practices for high availability



**Data backups  
and replication**



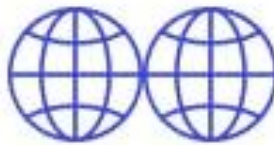
**Fail over  
solutions**



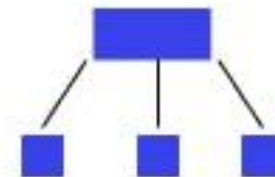
**Clustering**



**Plan for failure**

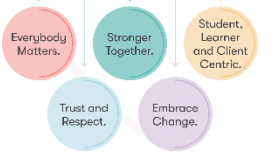


**Geographic  
redundancy**



**Network load  
balancing**

Building Careers  
Through Education



# Activity: CIA Triad Analysis

## Integrity - Hashing Data Using



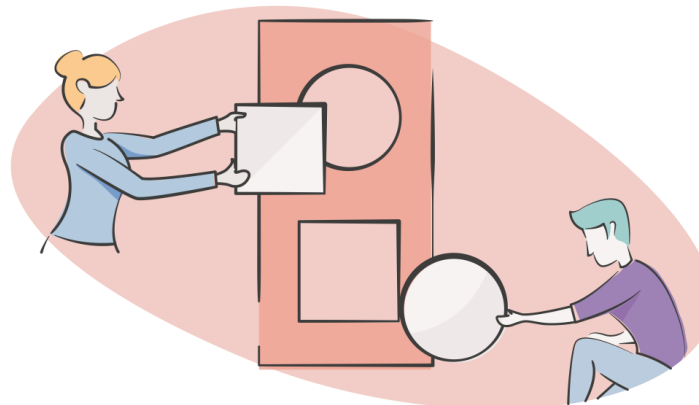
A GP practice faces multiple cybersecurity incidents.

Identify which aspect of the CIA Triad (Confidentiality, Integrity, or Availability) is affected in each of the given cybersecurity incidents:

**Phishing Attack**  
**Accidental Data Overwrite**  
**DDoS Attack**

Discuss potential measures to address each of the identified cybersecurity issues.

Groups will reconvene and share their findings on the affected CIA Triad aspects and the proposed mitigation measures.



# NSIT Cybersecurity

## The headlines...

The NIST Cybersecurity Framework is a comprehensive set of guidelines and best practices for organisations to manage and mitigate cybersecurity risks.

### Framework Benefits

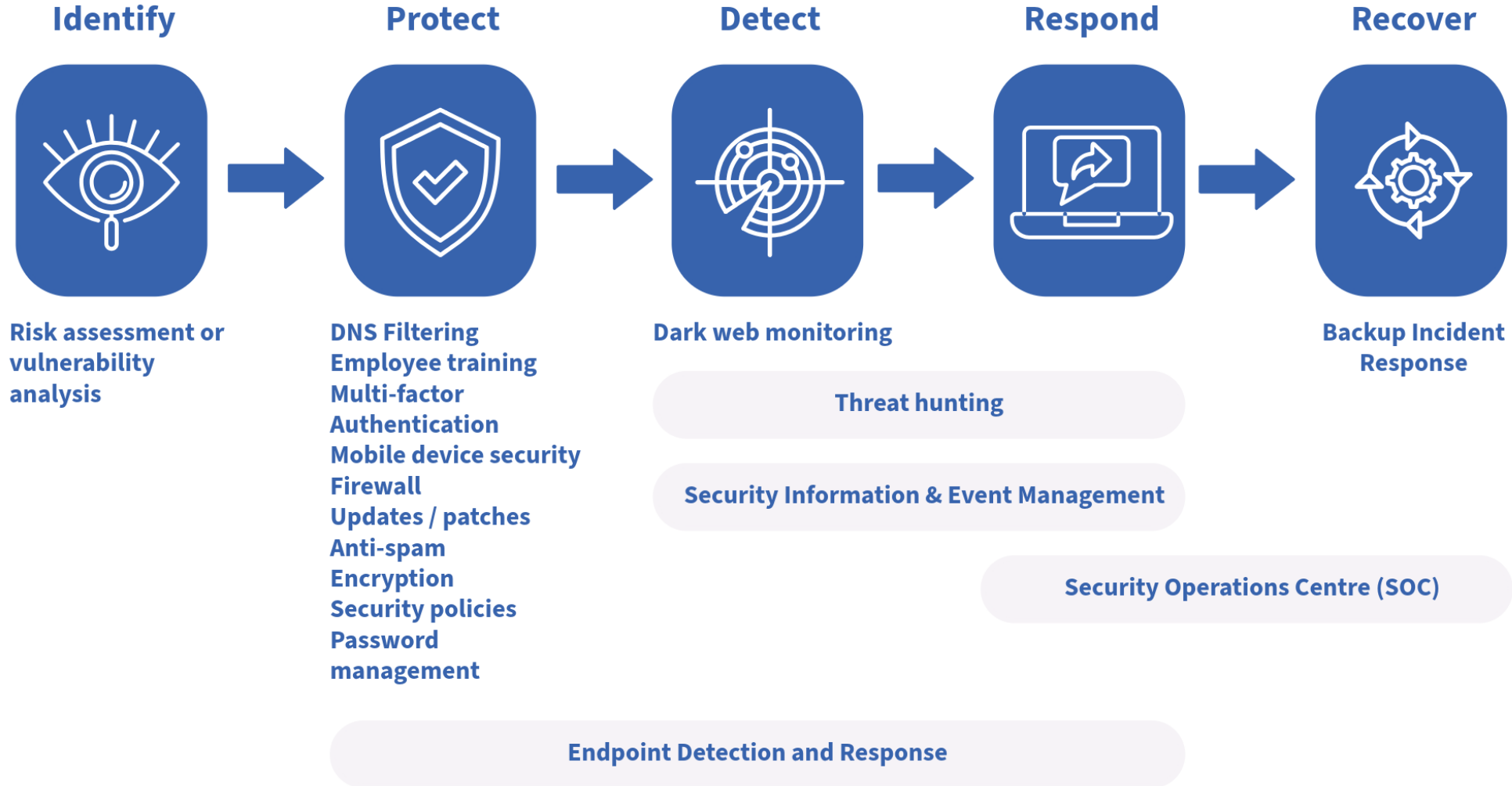
The NIST Cybersecurity Framework provides organisations with comprehensive security guidelines, enabling them to develop a holistic and adaptable cybersecurity strategy tailored to their specific needs and risk profile.

‘The NIST Cybersecurity Framework has become a widely adopted standard, helping organisations of all sizes and industries to strengthen their security posture and comply with industry regulations.’

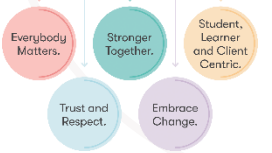


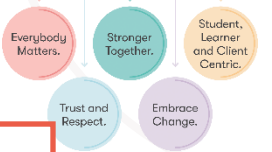
# NSIT Cybersecurity

## The framework...



Building Careers  
Through Education





## Core Functions

The framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover, which provide a structured approach to cybersecurity management.

### Identify

The Identify function helps organisations understand their critical assets, systems, and vulnerabilities, enabling them to prioritize risks and develop appropriate security measures.

### Protect, Detect, Respond, Recover

The remaining core functions - Protect, Detect, Respond, and Recover - outline the necessary controls, processes, and capabilities to safeguard against, identify, and effectively manage security incidents and ensure business continuity.

# NSIT Cybersecurity Framework



## Conduct a Risk Assessment

Identify and evaluate potential threats, vulnerabilities, and risks to the organisation's critical assets, systems, and processes.

## Develop a Cybersecurity Policy

Establish a comprehensive set of guidelines, standards, and procedures to manage and mitigate the identified risks, ensuring alignment with the organisation's goals and regulatory requirements.

## Implement Protective Measures

Deploy a range of security controls, such as access management, encryption, network security, and employee awareness training, to safeguard the organisation's resources and data.

## Monitor Systems Continuously

Implement continuous monitoring and logging mechanisms to detect and respond to suspicious activities, security incidents, and potential breaches in a timely manner.

## Plan and Practise Incident Response



# Importance of Monitoring in Cybersecurity

Building Careers  
Through Education



## Continuous Monitoring

Continuously tracking system activities and behaviors to quickly identify and address any suspicious or anomalous patterns, enabling a proactive defense against cyber threats.



## Detecting Anomalies

Identifying unusual or unexpected activities in the system, which could be indicators of a security breach or attempted attack, allowing for prompt investigation and mitigation.



## Real-Time Alerts

Providing immediate notification of security incidents or policy violations, enabling a rapid response and minimising the potential impact of a successful attack.



## Compliance Requirements

Implementing continuous monitoring practices to ensure compliance with industry regulations and standards, such as GDPR, which often mandate specific security monitoring and reporting capabilities.

Effective cybersecurity monitoring is essential for proactively defending against threats, quickly detecting and responding to incidents, and maintaining regulatory compliance. Continuous monitoring, anomaly detection, real-time alerts, and compliance requirements are all critical components of a robust security strategy.





# Introduction to binary risk assessment

## Using digital signatures

- **Definition and Concept**
- **Simplified Risk Evaluation:** Yes/No assessment
- **Use Cases:** Quick initial assessments
- **Benefits:** Efficient and easy to understand
- **Limitations:** Not suitable for complex risks

Building Careers  
Through Education



# Conducting a binary risk assessment



- **(1) Identify Assets**

Determine the critical data, systems, and resources that are essential for the organization's operations and need to be protected.

- **(2) Identify Threats**

Assess the potential risks and threats that could compromise the identified assets, such as cyber attacks, natural disasters, or human errors.

- **(3) Determine Risk (Yes/No)**

Evaluate the likelihood and impact of each threat, and make a binary decision on whether the risk is acceptable or requires further action.

- **(4) Implement Controls**

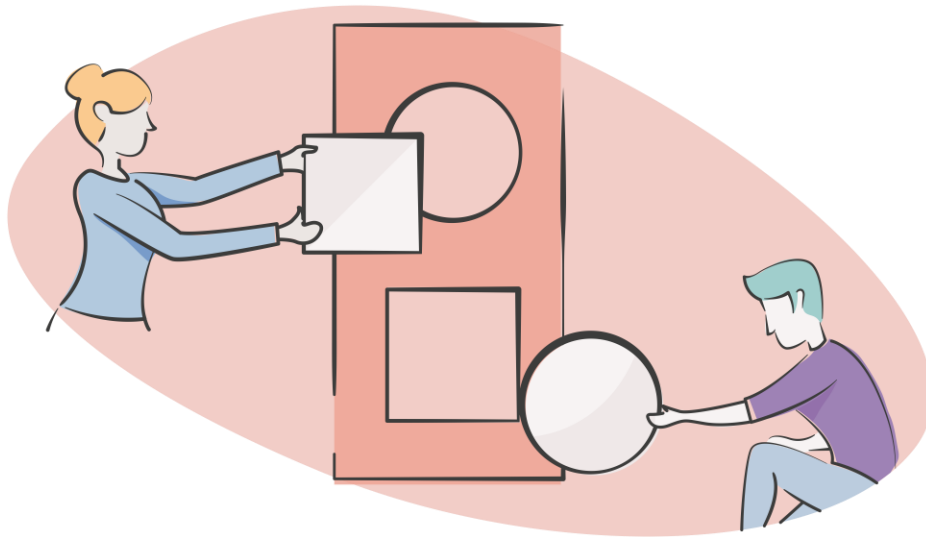
Implement appropriate security controls and measures to mitigate the identified risks, such as access controls, backup procedures, or incident response plans.

# Lab

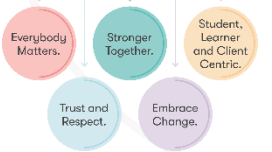
## Risk analysis

Your tutor will guide you through Binary Risk Analysis:

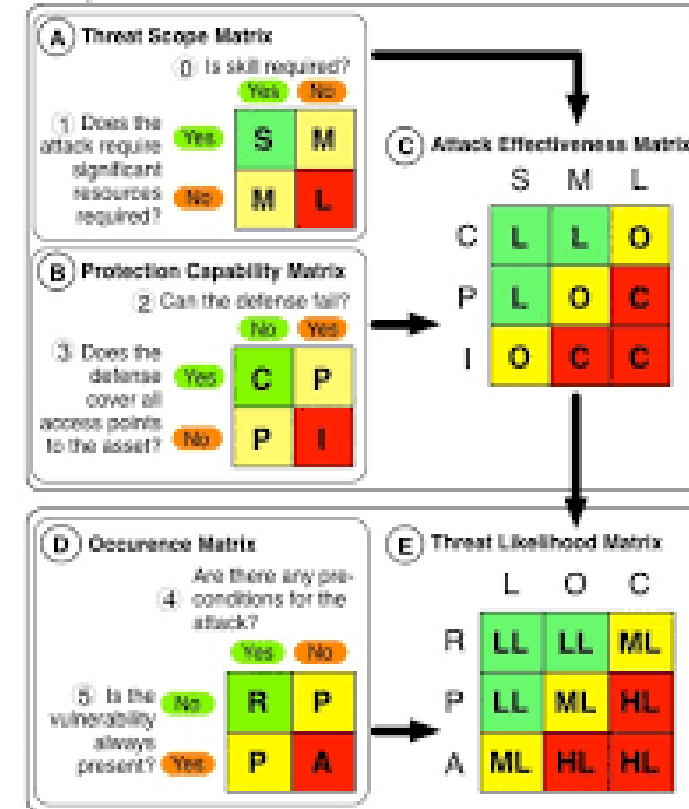
<https://binary.protect.io/>



Building Careers  
Through Education



### Step 1 - Determine Likelihood ⌚ 0:00:00



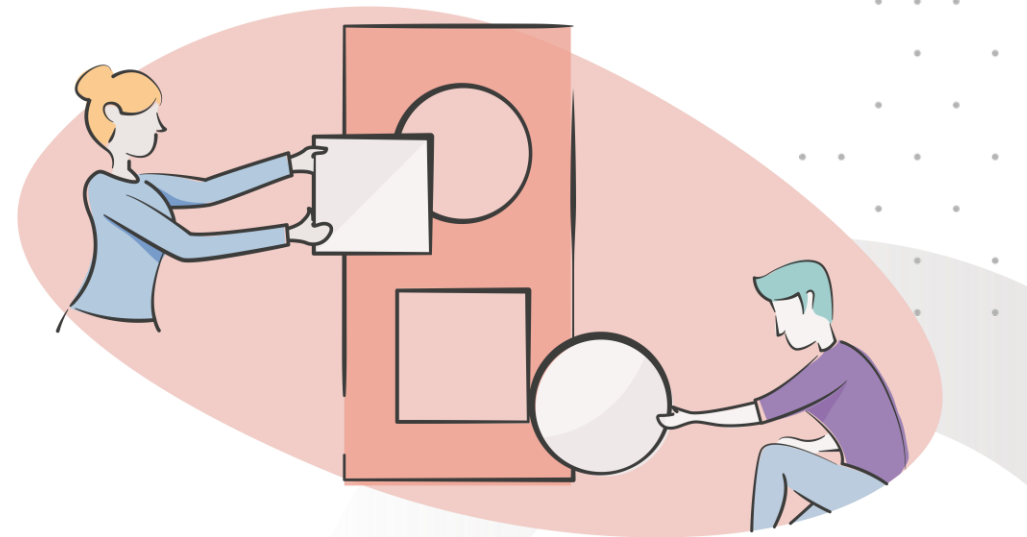
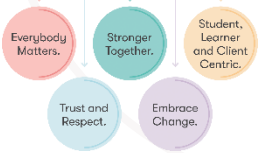
# Interactive activity

## Binary risk assessment

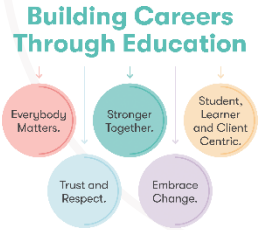
- **Scenario:** An organisation faces risks from outdated software and phishing attacks.
- **Step 1:** Conduct a binary risk assessment for each risk.
- **Step 2:** Discuss control measures and prioritise them.

Groups reconvene and share their assessments and control strategies.

Building Careers  
Through Education



# Understanding Financial Impact - Definitions



## Cost of Controls

The cost associated with implementing security measures and safeguards to mitigate identified risks.

## Annual Rate of Occurrence (ARO)

The expected frequency of a security incident or threat occurring within a year.

## Single Loss Expectancy (SLE)

The estimated financial loss from a single occurrence of a security incident or threat.

## Importance of Financial Impact Analysis

Analysing the financial impact of security incidents helps organizations make informed decisions on risk management and resource allocation.

# Calculating financial impact

## Formulas

**SLE:** Cost of a single incident

**ARO:** Expected frequency of an incident per year

**ALE (Annual Loss Expectancy) =  $SLE * ARO$**

- **Scenario:** A company faces potential ransomware attacks with an SLE of £50,000 and an ARO of 0.2.
- **Calculation:**  $ALE = £50,000 * 0.2 = £10,00$



# Risk reduction ROI

## Using digital signatures

- **Calculating ROI:**

- **Formula:**  $\text{ROI} = (\text{ALE before control} - \text{ALE after control}) / \text{Cost of control}$

- **Example:**

- **Scenario:** Implementing an anti-phishing solution costing £10,000 reduces ARO to 0.1.
- **Calculation:**
  - **New ALE for Ransomware:**  $\text{£}50,000 * 0.1 = \text{£}5,000$
  - **ROI for Anti-phishing Solution:**  $(\text{£}10,000 - \text{£}5,000) / \text{£}10,000 = 0.5 \text{ or } 50\%$

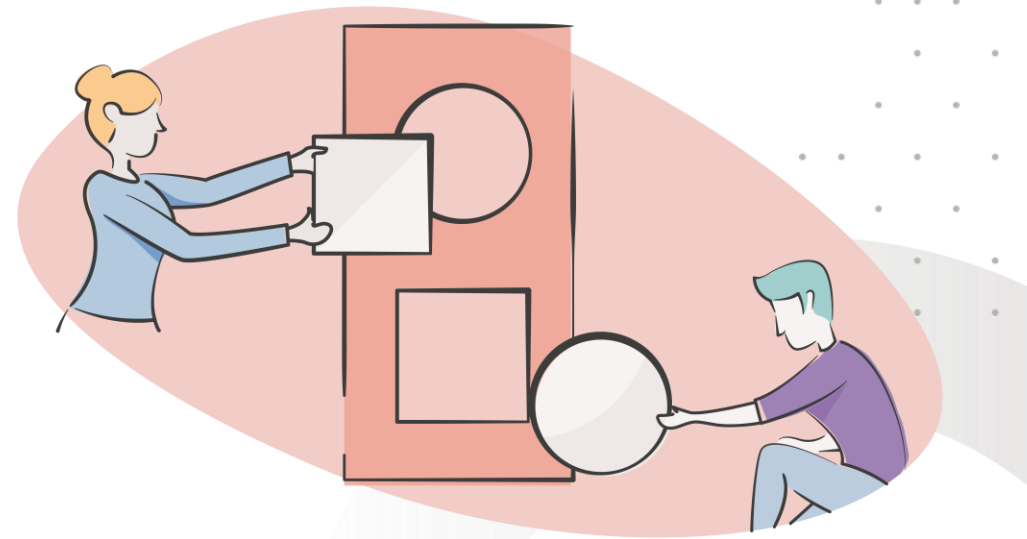
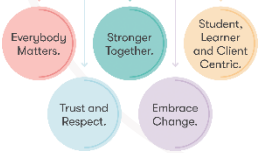


# Activity

## Financial impact calculation

- **Scenario:** A retail company faces potential threats with the following details:
  - **Breach:**  $SLE = £100,000$ ,  $ARO = 0.1$
  - **Step 1:** Calculate SLE, ARO, and ALE for each threat.
  - **Step 2:** Propose controls and calculate the ROI for each.
  - **Step 3:** Groups reconvene and share their calculations and control recommendations.

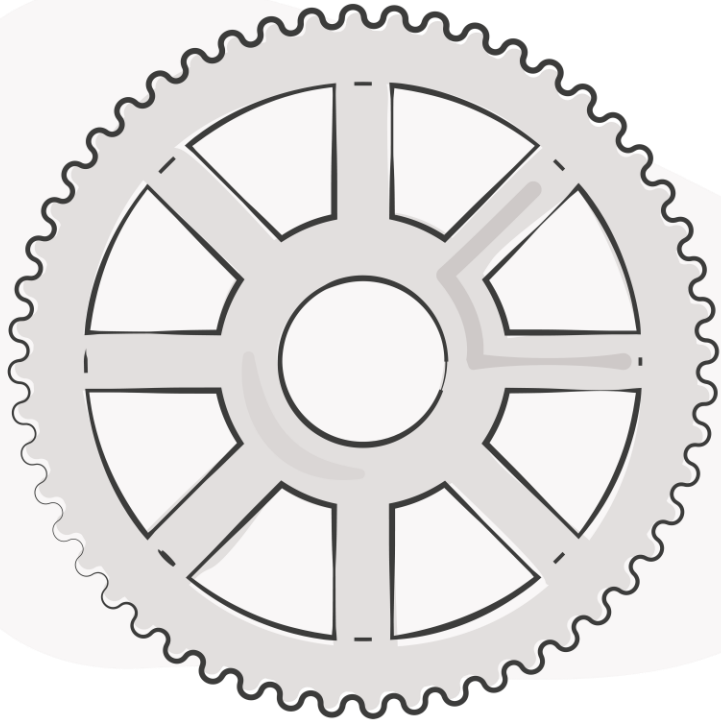
Building Careers  
Through Education



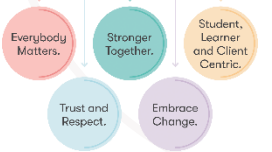


# Time for the practical lab!

Your tutor will provide guidance as required...



Building Careers  
Through Education



# Session wrap-up

## Post-Webinar Quiz Questions

- What does the CIA Triad stand for?
- What are the core functions of the NIST Cybersecurity Framework?
- How is ALE (Annual Loss Expectancy) calculated?

## Useful Tools for Cybersecurity

- SIEM Systems
- IDS/IPS Tools
- Encryption Software

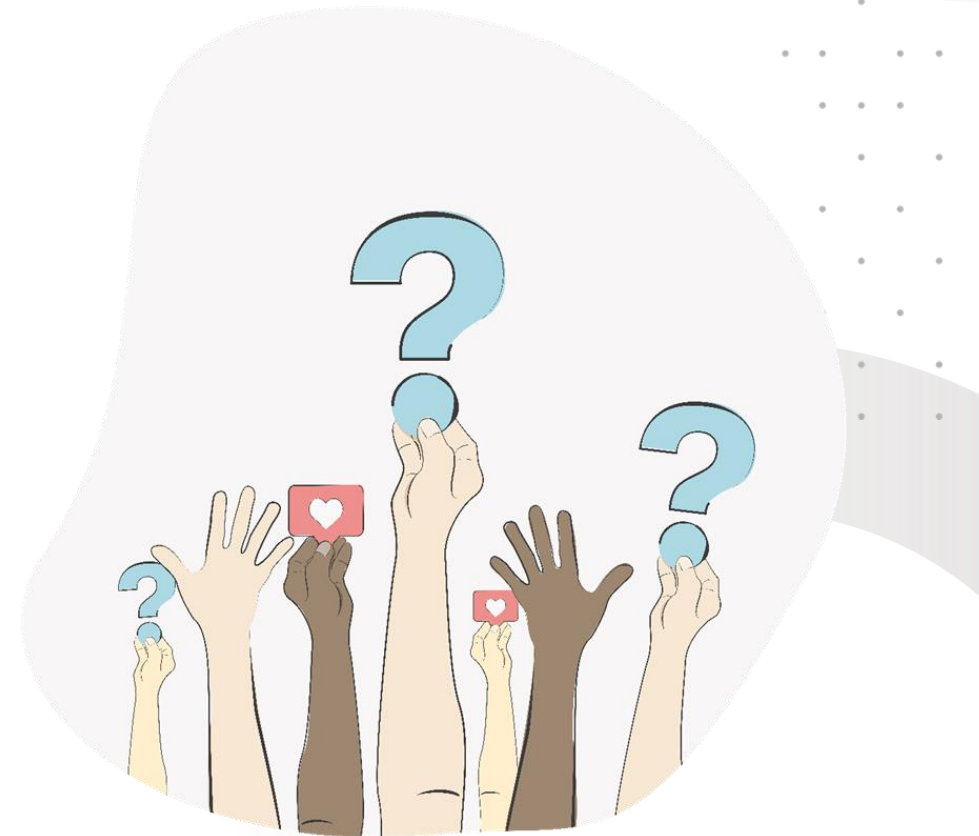
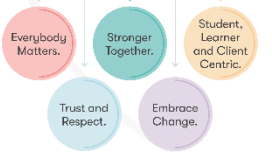
## Additional Resources for Further Reading

- NIST Cybersecurity Framework
- ISO 27001 Standards
- Books and Articles on Cybersecurity

## Courses and Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)

Building Careers  
Through Education



Any questions or  
feedback?

