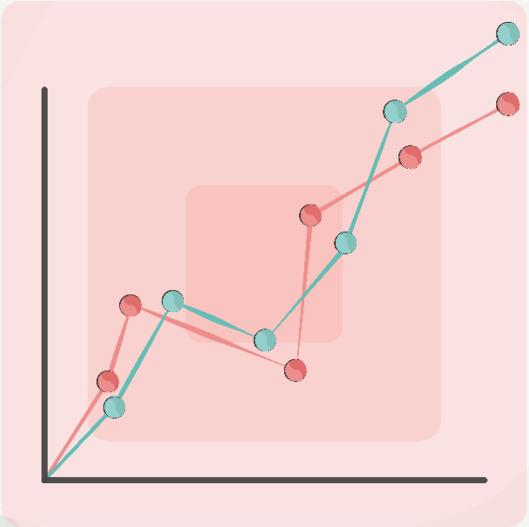
Level 5 Data Engineer
Module 4 Topic 2

Cyber Security Essentials

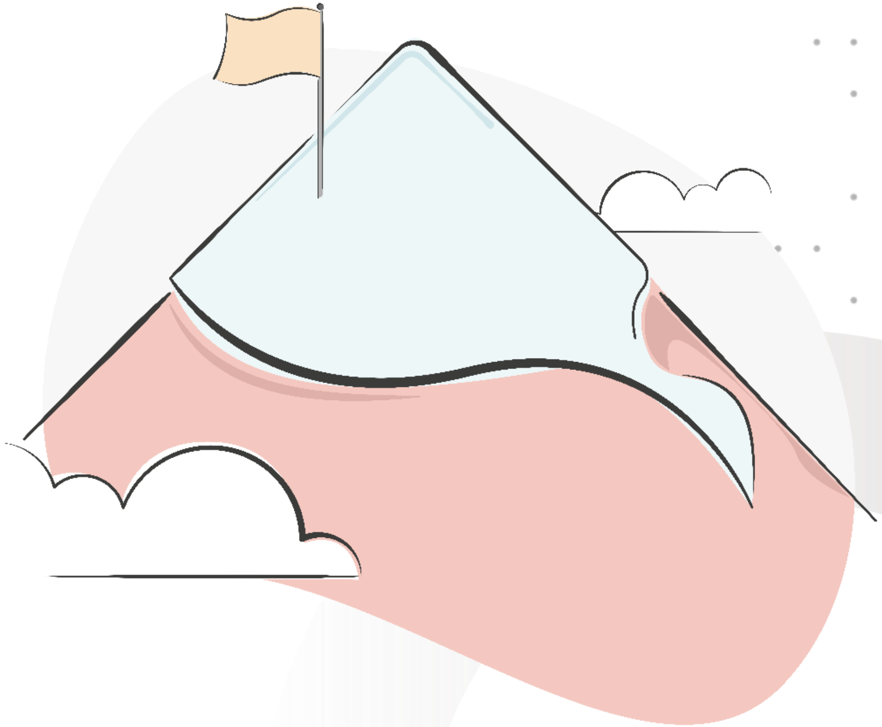
Welcome to today's webinar.



Session aim and objectives

This webinar supports the following learning outcomes:

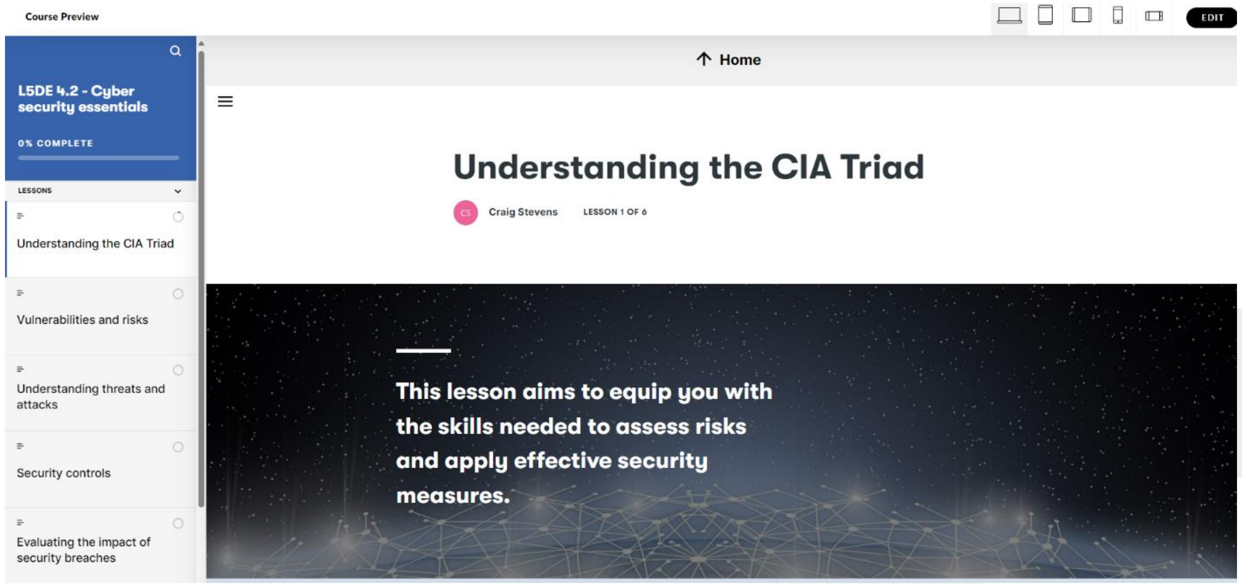
- Understand the fundamental principles of the CIA triad and its application in cyber security.
- Recognise risks, vulnerabilities, and threats to ensure robust security for data products.
- 3. Explain security controls and quantify and evaluate the impact of security breaches
- 4. Identify and mitigate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



Recap of e-learning

Are you happy with your learning?

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

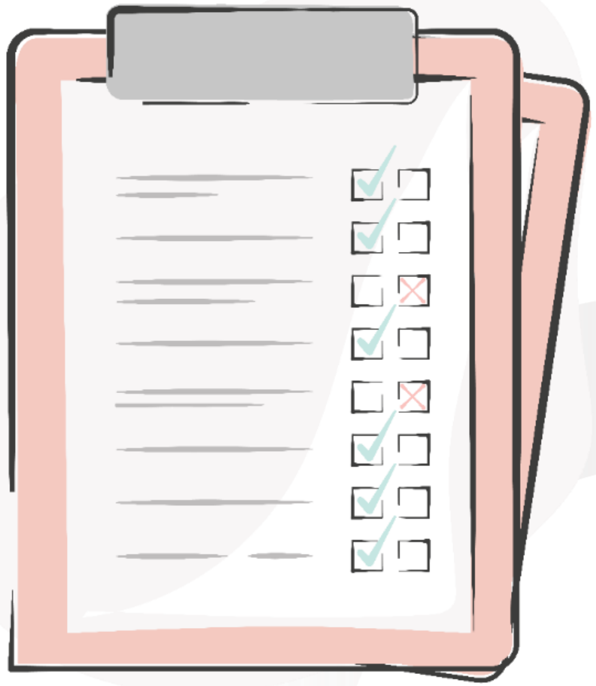


A screenshot of topic 2 e-learning

Webinar Agenda

What we will cover in the webinar:

1. Deep Dive into the CIA Triad
2. Cryptography basics
3. NIST Cybersecurity Framework
4. Monitoring Practices and Open-Source Frameworks
5. Binary Risk Assessment
6. Case Study: Financial Impact of a Security Breach



Introduction to the CIA Triad

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 unauthorised access, ensuring that only authorised 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 authorised users have reliable and timely access to information and resources when needed, minimising disruptions and downtime.

Confidentiality

What approaches you need to know about…

- **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 asymmetric encryption. They are cryptographic methods (cryptography is a branch of applied maths dealing with keeping secrets!)

BPP

Confidentiality

Types of encryption

- 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 are based on the premise that each communicating party knows the pre-shared key.
- Asymmetric algorithms use two different keys, public and private, to encrypt and decrypt data.

Symmetric Encryption

- Use the same key to encrypt and decrypt data.
- Key lengths are short (40 bits - 256 bits).
- Faster than asymmetric encryption.
- Commonly used for encrypting bulk data such as in VPN traffic.

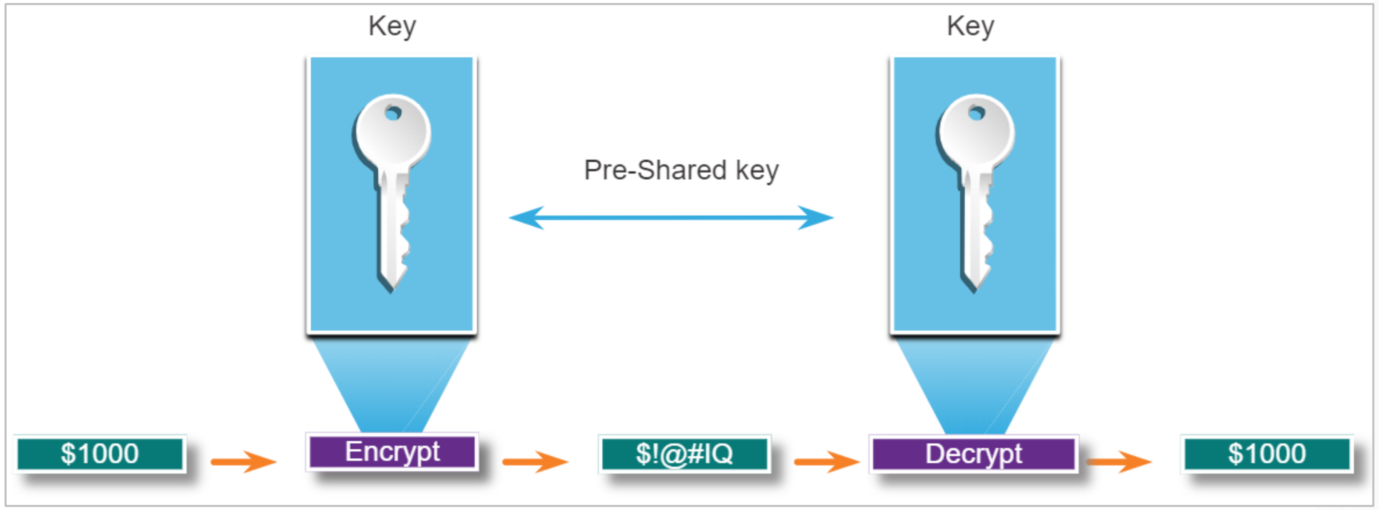
Asymmetric Encryption

- Uses different keys to encrypt and decrypt data.
- Key lengths are long (512 bits - 4096 bits).
- Computationally tasking therefore slower than symmetric encryption.
- Commonly used for quick data transactions such as HTTPS when accessing your bank data.

Confidentiality

Symmetric encryption

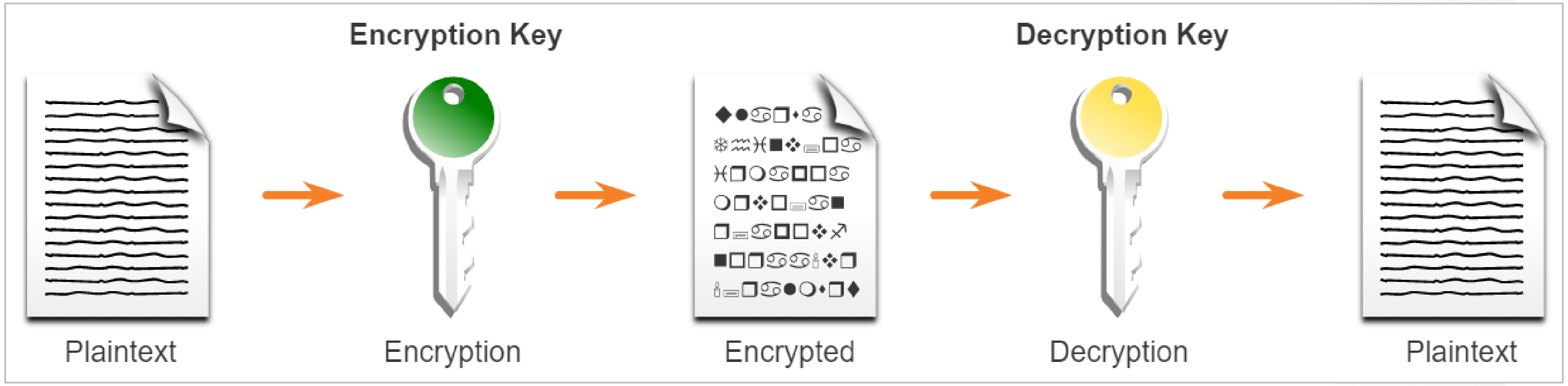
- Symmetric algorithms use the same pre-shared key (secret key) to encrypt and decrypt data.
- Symmetric encryption algorithms are commonly used with VPN traffic because they use less CPU resources than asymmetric encryption algorithms.
- When using these algorithms, the longer the key, the longer it will take for someone to discover the key.
- Most encryption keys are up to 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

Asymmetric encryption…

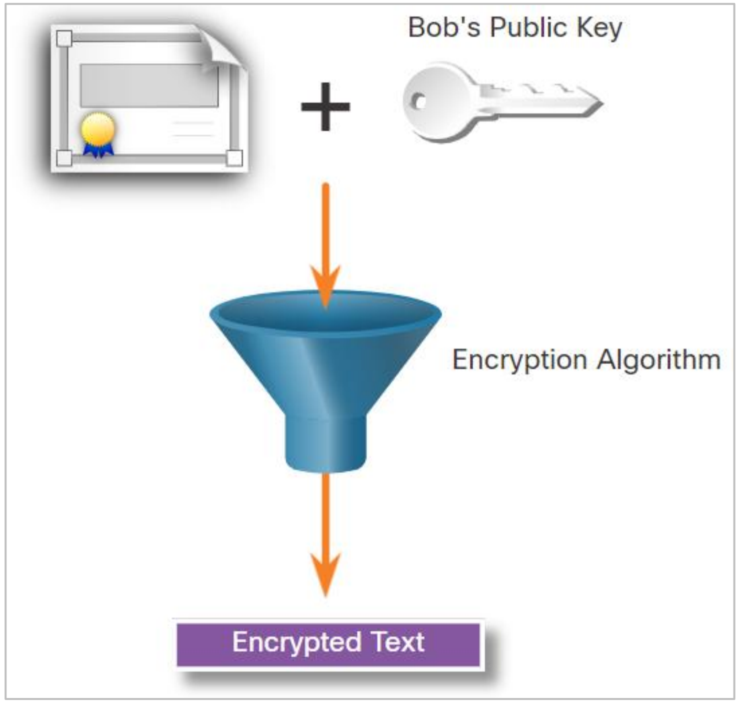
- Asymmetric algorithms, also called public-key algorithms, are designed in a way that the encryption and the decryption keys are different.
- Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for decryption.
- Asymmetric encryption can use key lengths up to 4,096 bits.
- Asymmetric algorithms are substantially slower than symmetric algorithms.



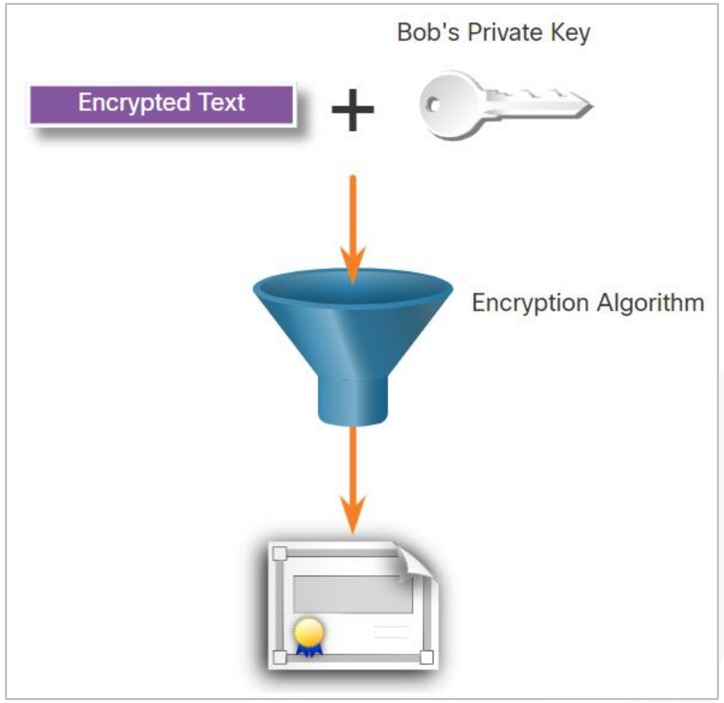
Confidentiality

Asymmetric encryption – confidentiality

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.

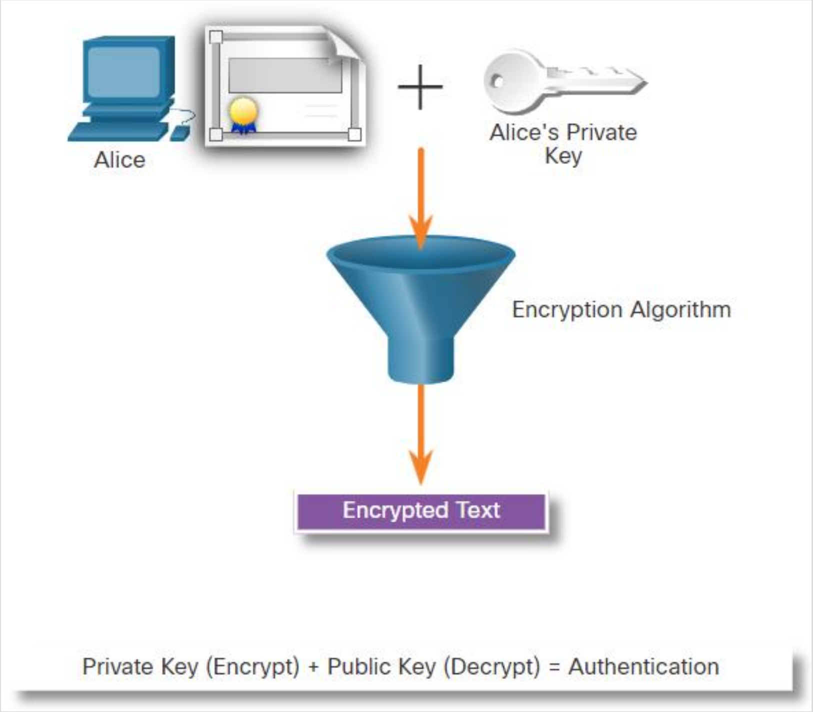


Bob decrypts the message with the private key and as he is the only one with the private key, confidentiality is achieved.

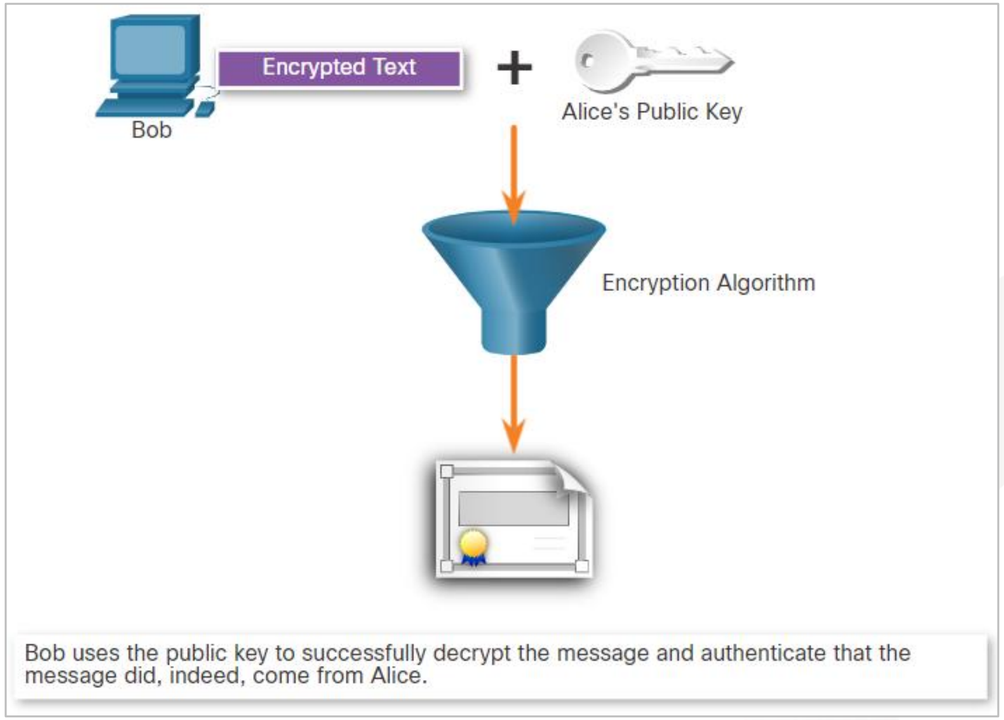
Confidentiality

Asymmetric encryption - authentication

- 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.



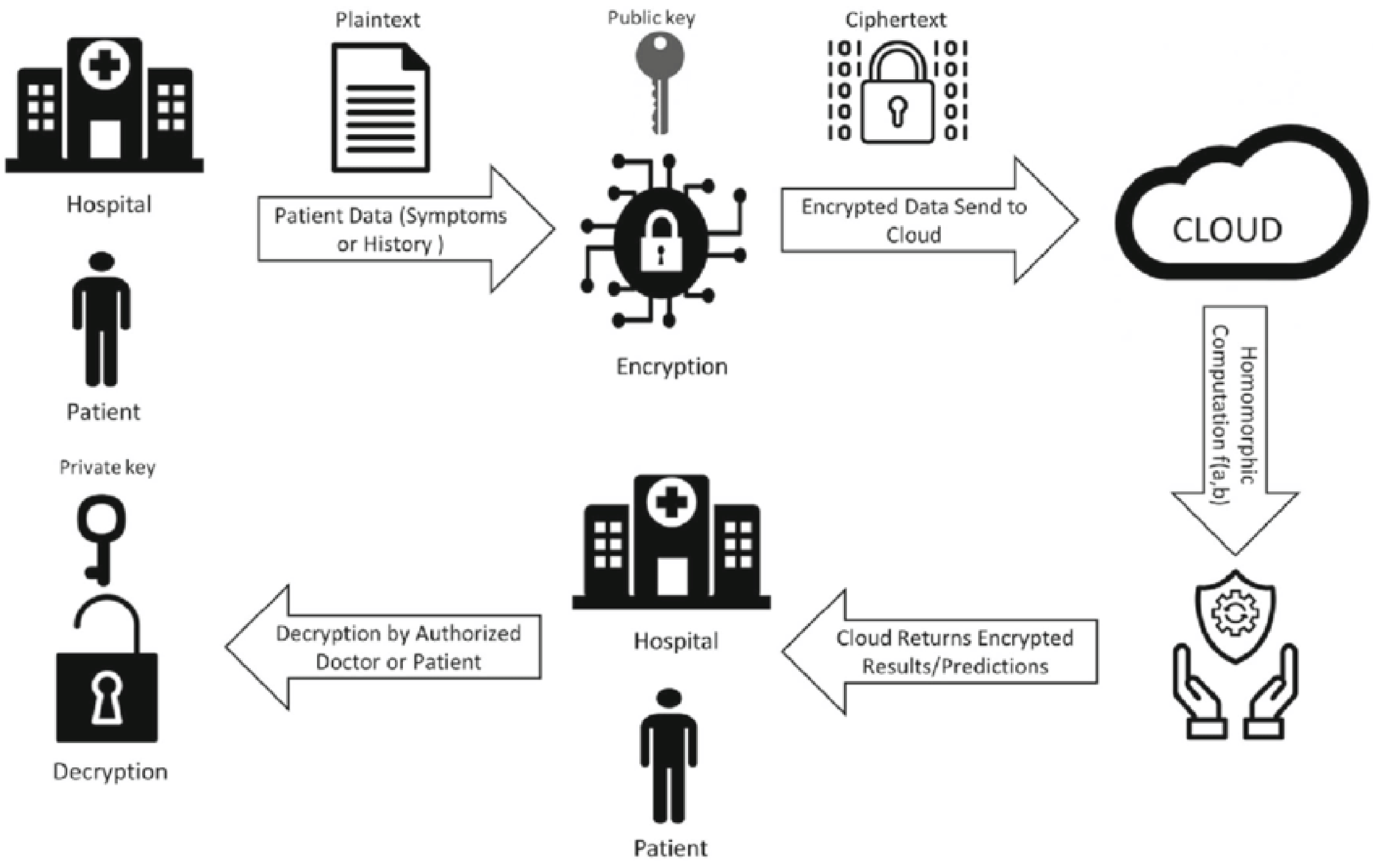
Bob decrypts using the public key
After Bob obtains Alice's public key, he uses it to decrypt the message and to authenticate that the message has been received from Alice.

Confidentiality case study discussion

Building Careers Through Education

Everybody Matters.
Stronger Together.
Student, Learner and Client Centric.
Trust and Respect.
Embrace Change.

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



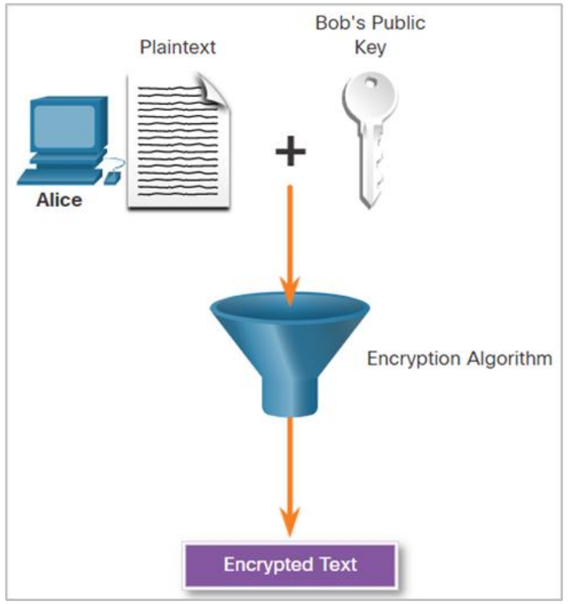
Submit your responses to the chat!

BPP

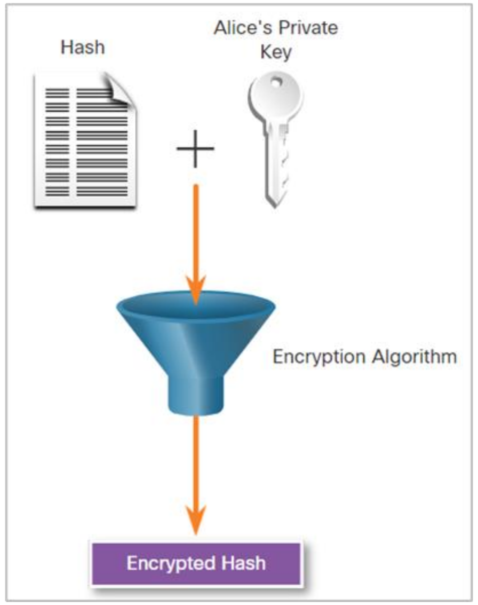
Confidentiality (+ Integrity)

Asymmetric encryption

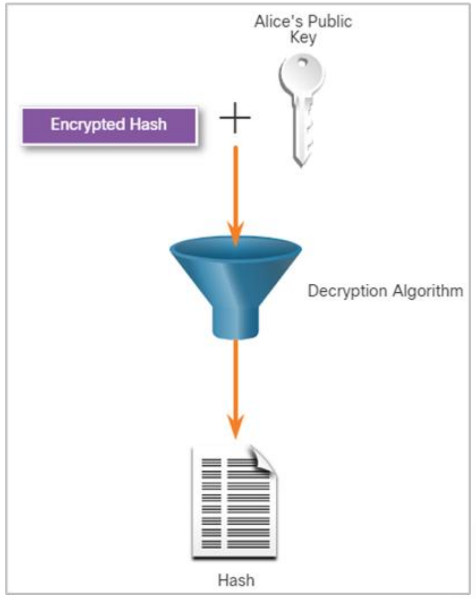
Combining the two asymmetric encryption processes provides message Confidentiality, Authentication, and now **<u>Integrity</u>**. In this example, a message will be ciphered using Bob's public key and a ciphered hash will be encrypted using Alice's private key.



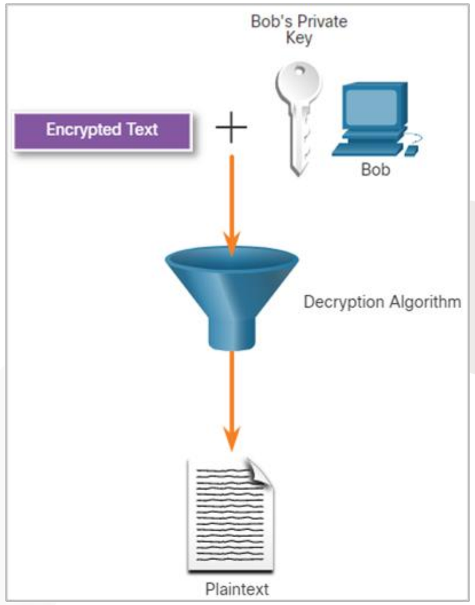
Alice uses Bob's Public Key



Alice encrypts a hash using her private key



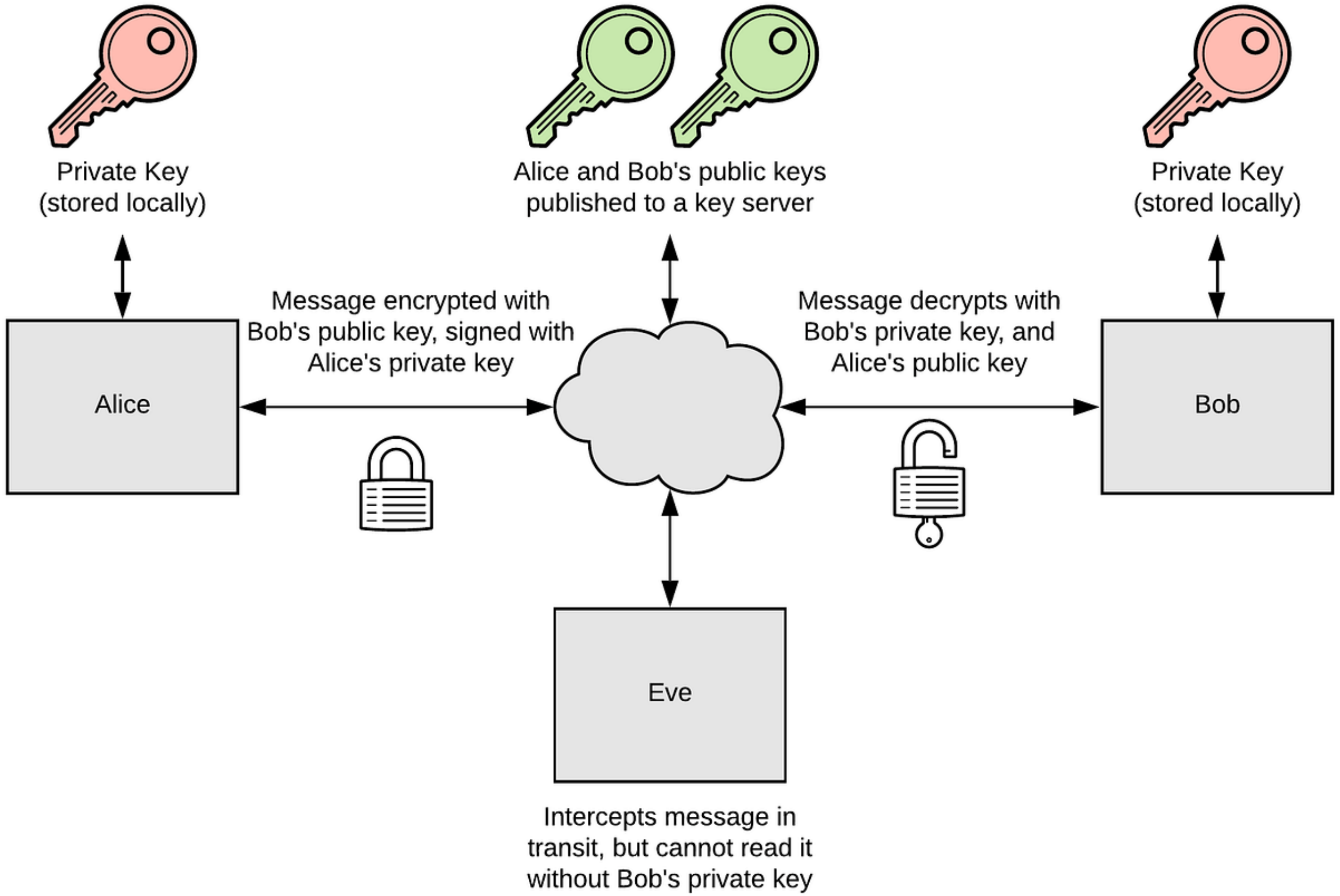
Bob uses Alice's public key to decrypt the hash



Bob uses his private key to decrypt the message

Discussion

How does asymmetric encryption ensure **Integrity** and **Confidentiality** with the following example?

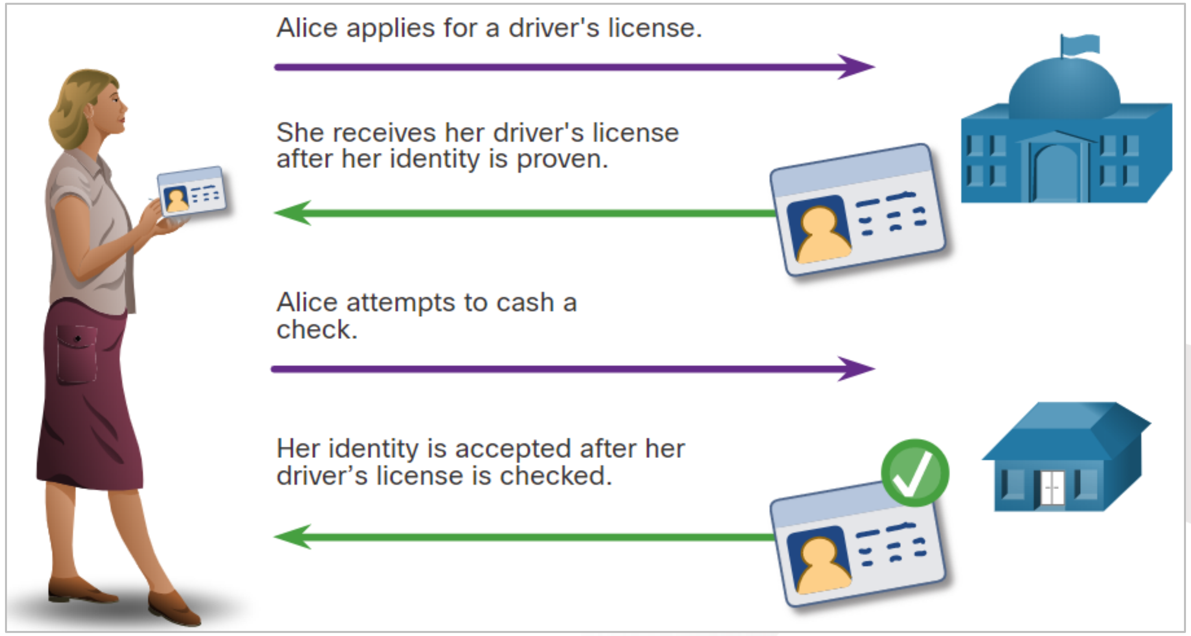


Submit your responses to the chat!

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.

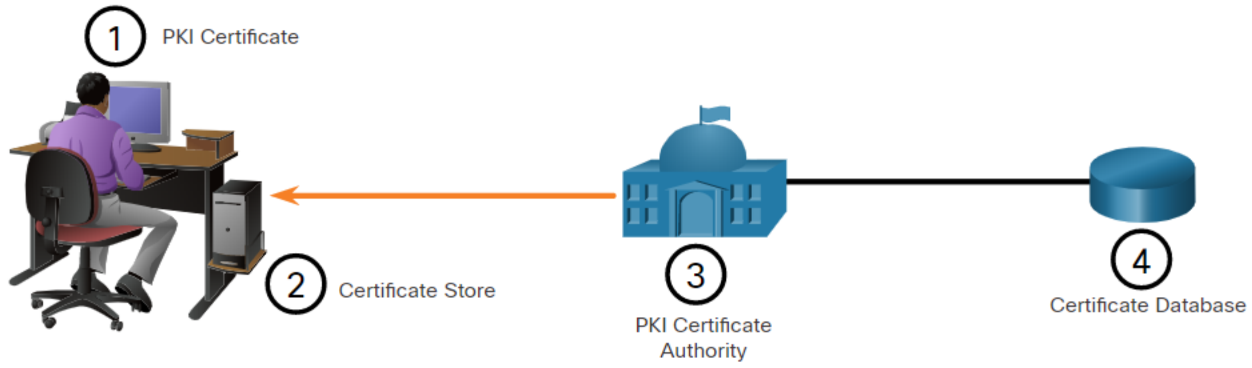


Illustrates how a driver's license is analogous to a digital certificate

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.



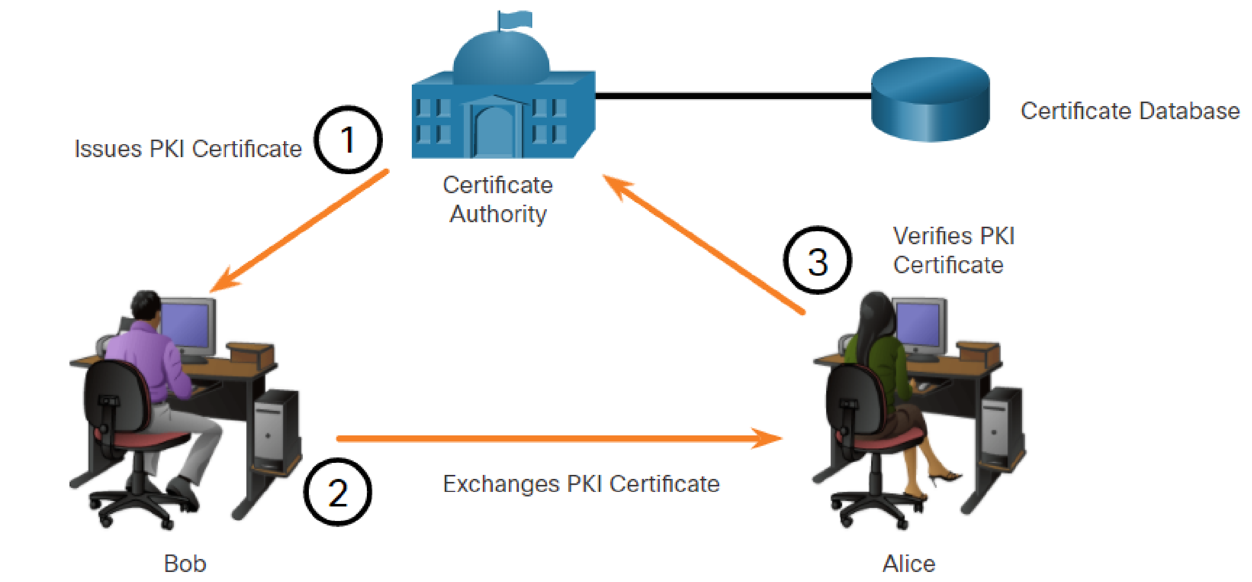
1. PKI certificates contain an entity's or individual's public key, its purpose, the certificate authority (CA) that validated and issued the certificate, the date range during which the certificate is valid, and the algorithm used to create the signature.
2. The certificate store resides on a local computer and stores issued certificates and private keys.
3. The PKI Certificate of Authority (CA) is a trusted third party that issues PKI certificates to entities and individuals after verifying their identity. It signs these certificates using its private key.
4. The certificate database stores all certificates approved by the CA.

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.



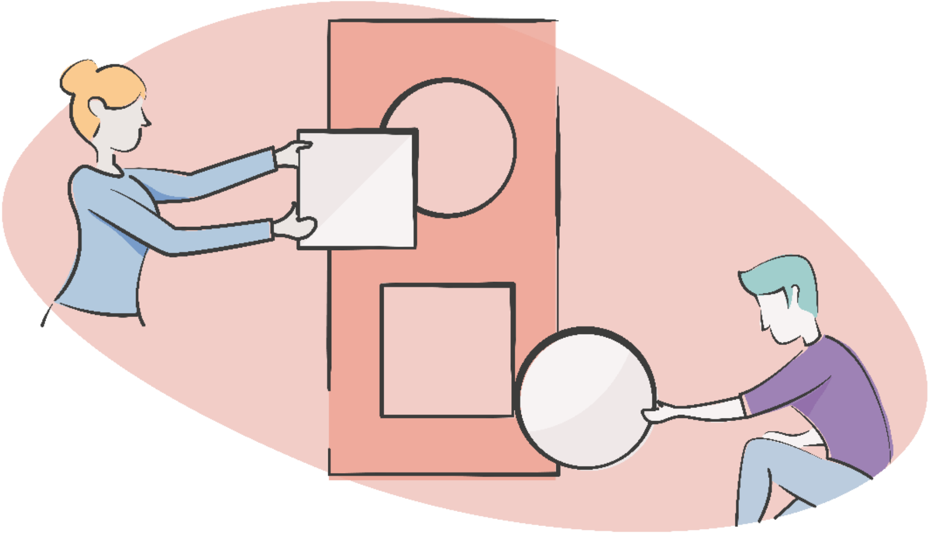
1. **Issues PKI Certificate**. Bob initially requests a certificate from the CA. The CA authenticates Bob and stores Bob's PKI certificate in the certificate database.
2. **Exchanges PKI Certificate**. Bob communicates with Alice using his PKI certificate.
3. **Verifies PKI Certificate**. Alice communicates with the trusted CA using the CA's public key. The CA refers to the certificate database to validate Bob's PKI certificate.

Activity – 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.



Integrity

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

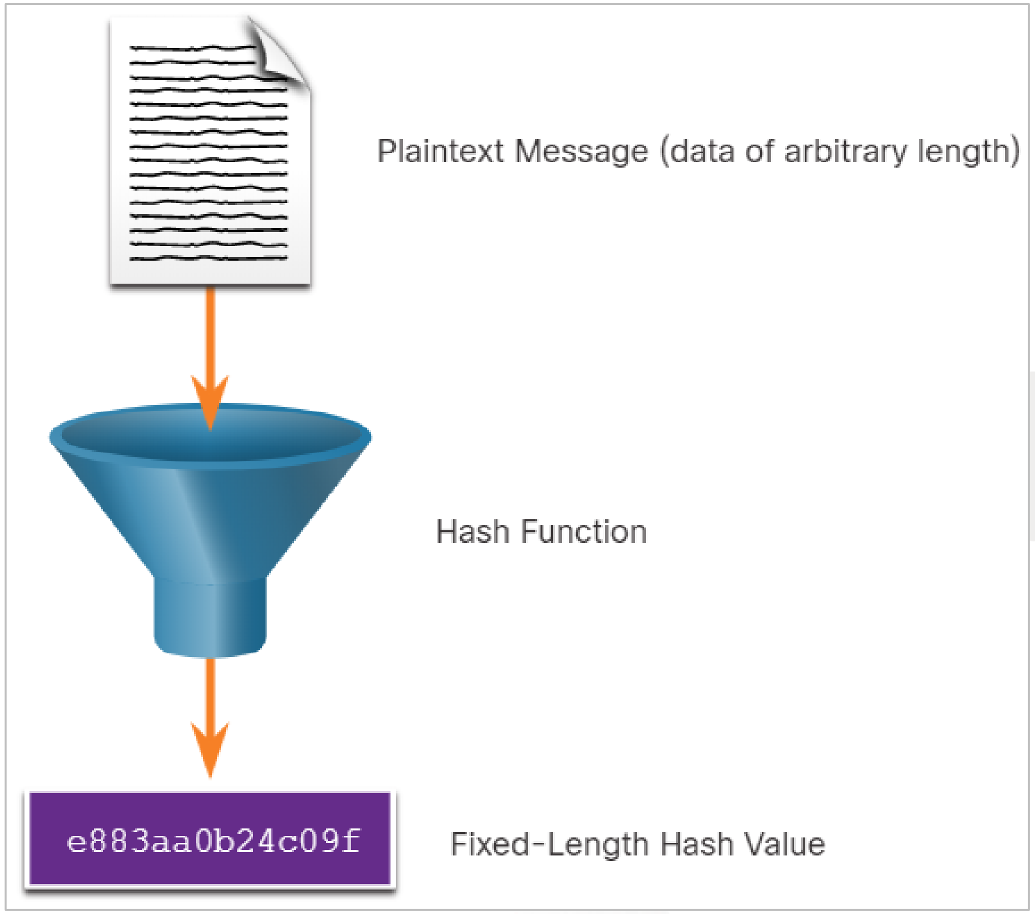
Some key techniques used to preserve data integrity include checksums, hash functions, and digital signatures.

Impact: Preventing data tampering

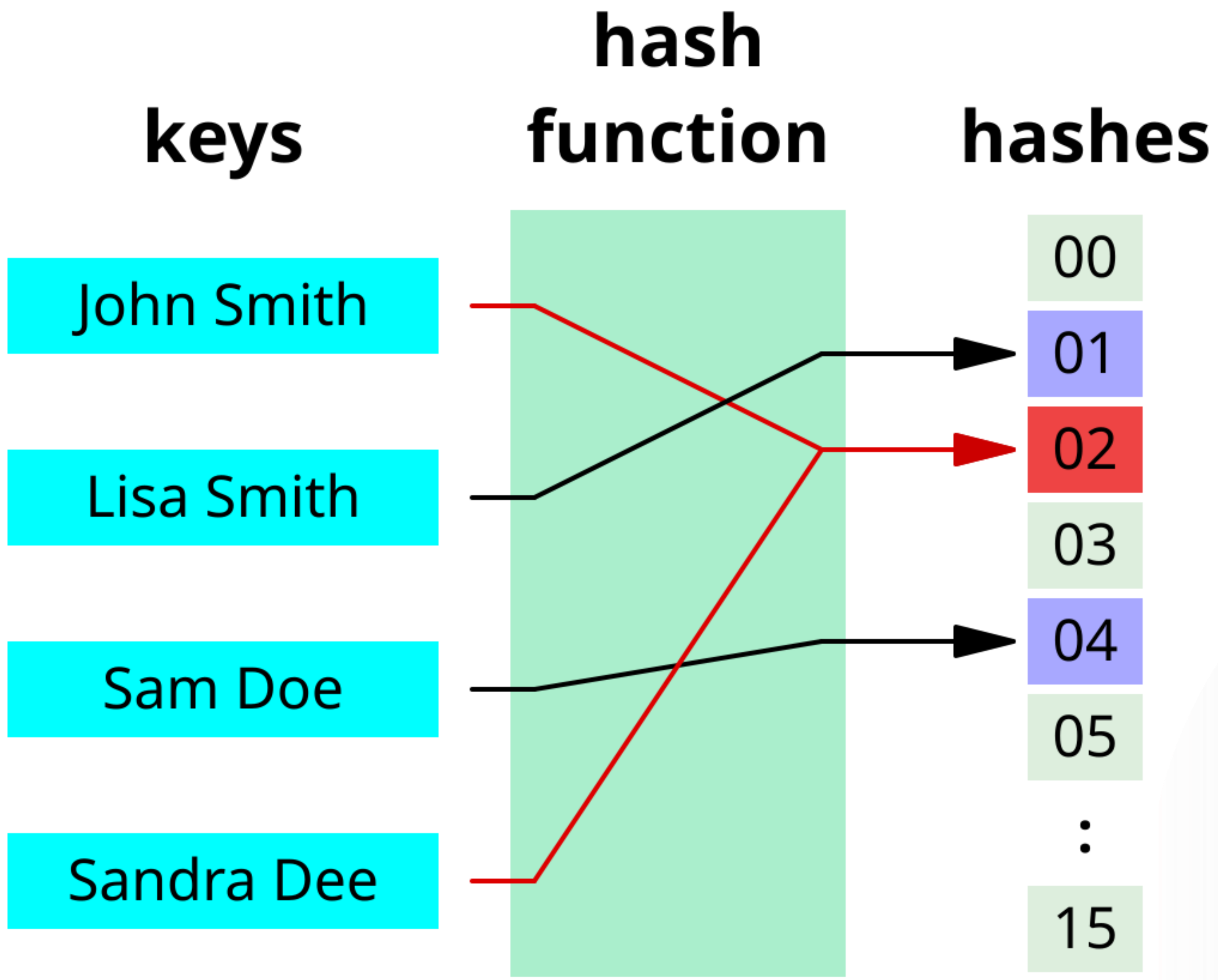
Cryptography

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.



Keys and hash functions

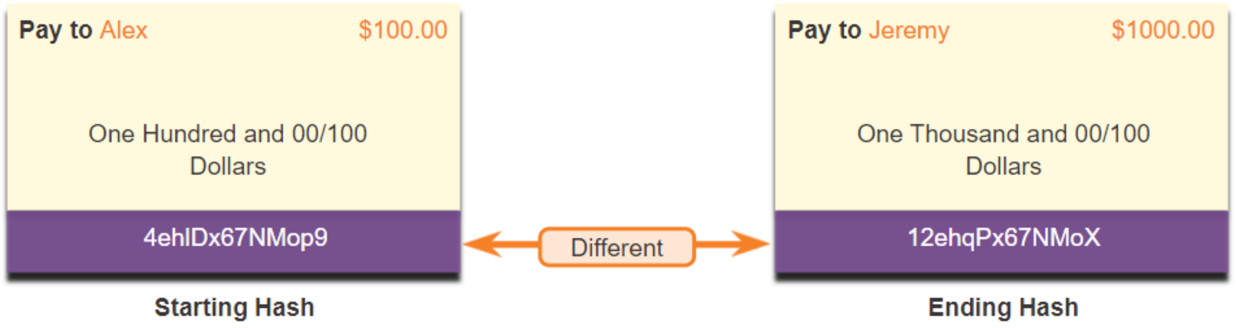


Cryptography

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.



The sender wants to ensure that the message is not altered on its way to the receiver.

1. The sending device inputs the message into a hashing algorithm and computes its fixed-length hash of 4ehiDx67NMop9.
2. This hash is then attached to the message and sent to the receiver. Both the message and the hash are in plaintext.
3. The receiving device removes the hash from the message and inputs the message into the same hashing algorithm. If the computed hash is equal to the one that is attached to the message, the message has not been altered during transit. If the hashes are not equal, as shown in the figure, then the integrity of the message can no longer be trusted.

Activity

Confidentiality - Encrypting and Decrypting Data Using asymmetric encryption

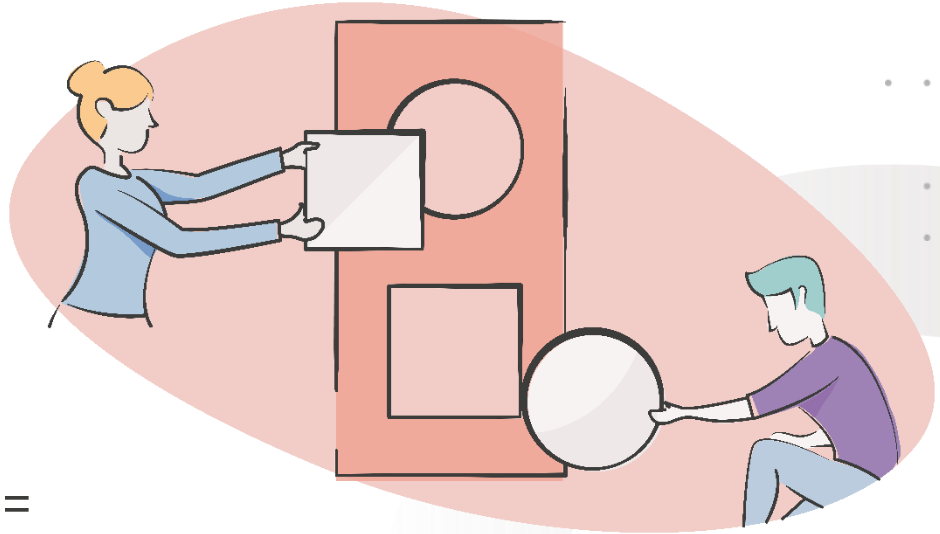
In this lab, you will complete the following objectives:

- Encrypting Messages with AES
- Decrypting Messages with AES

https://encode-decode.com

Try decoding this using AES 128 CBC:

1o/agaKaI7gF5jRwabN0u430Al7z5w0iCZT5reP1qU4=



Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

BPP

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

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

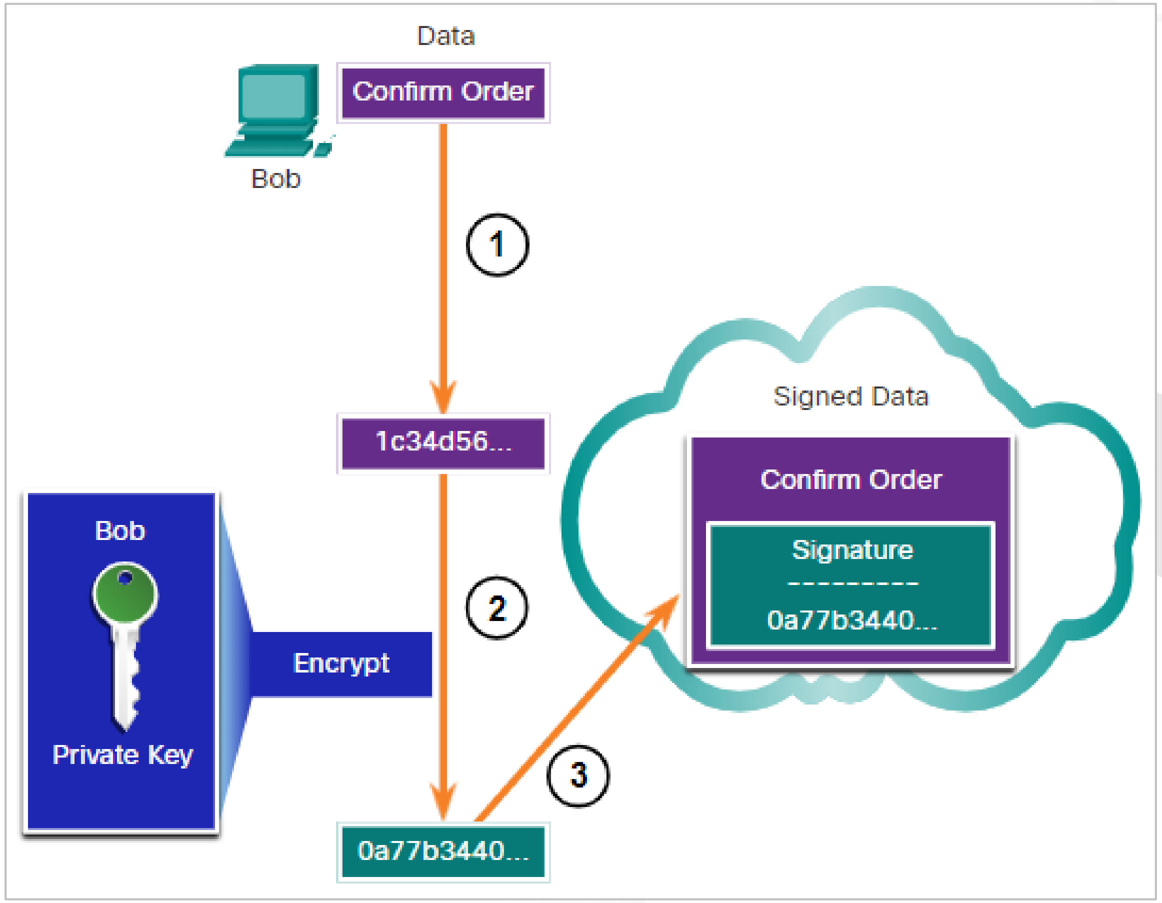
BPP

Public Key Cryptography

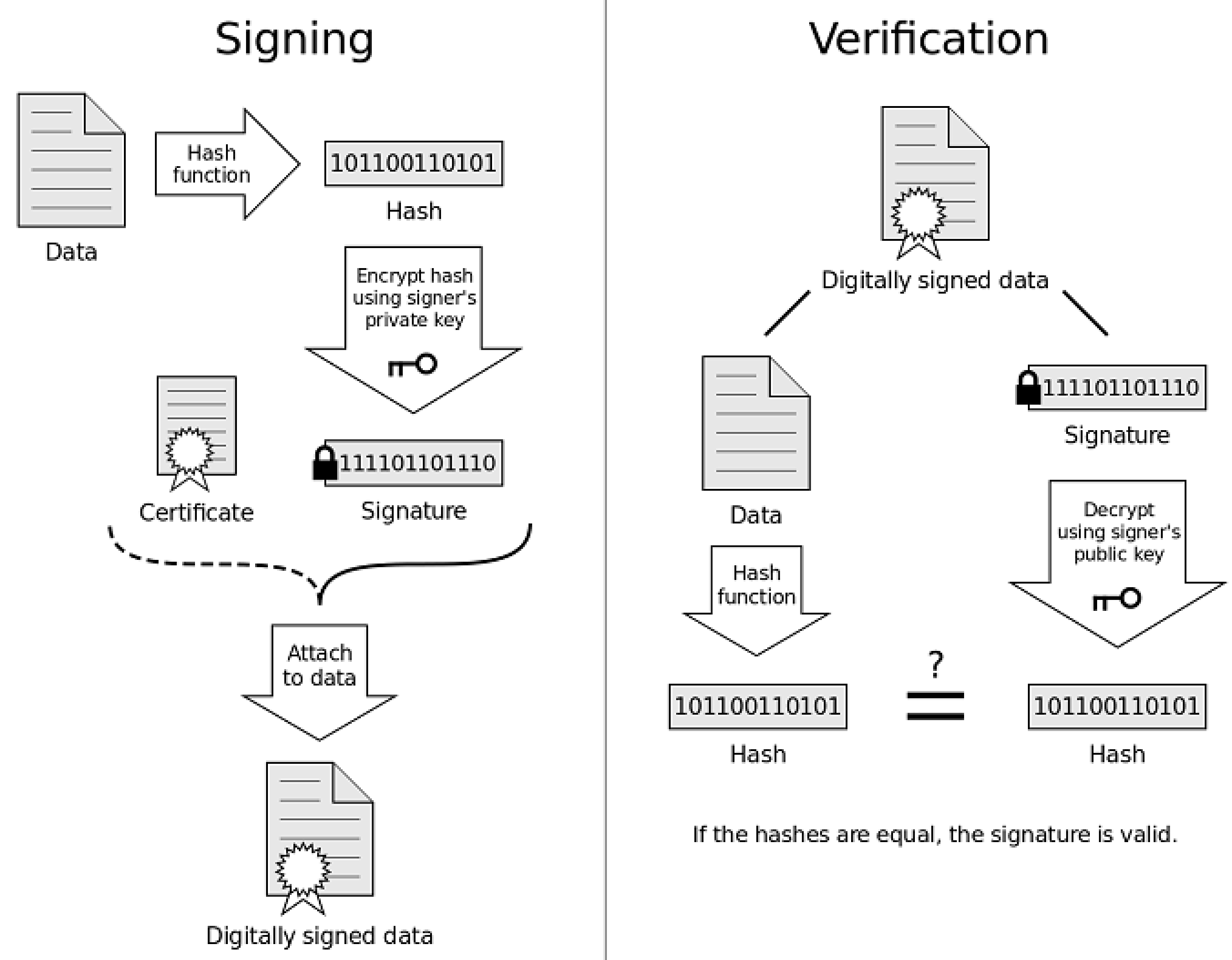
Digital signatures for digital

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

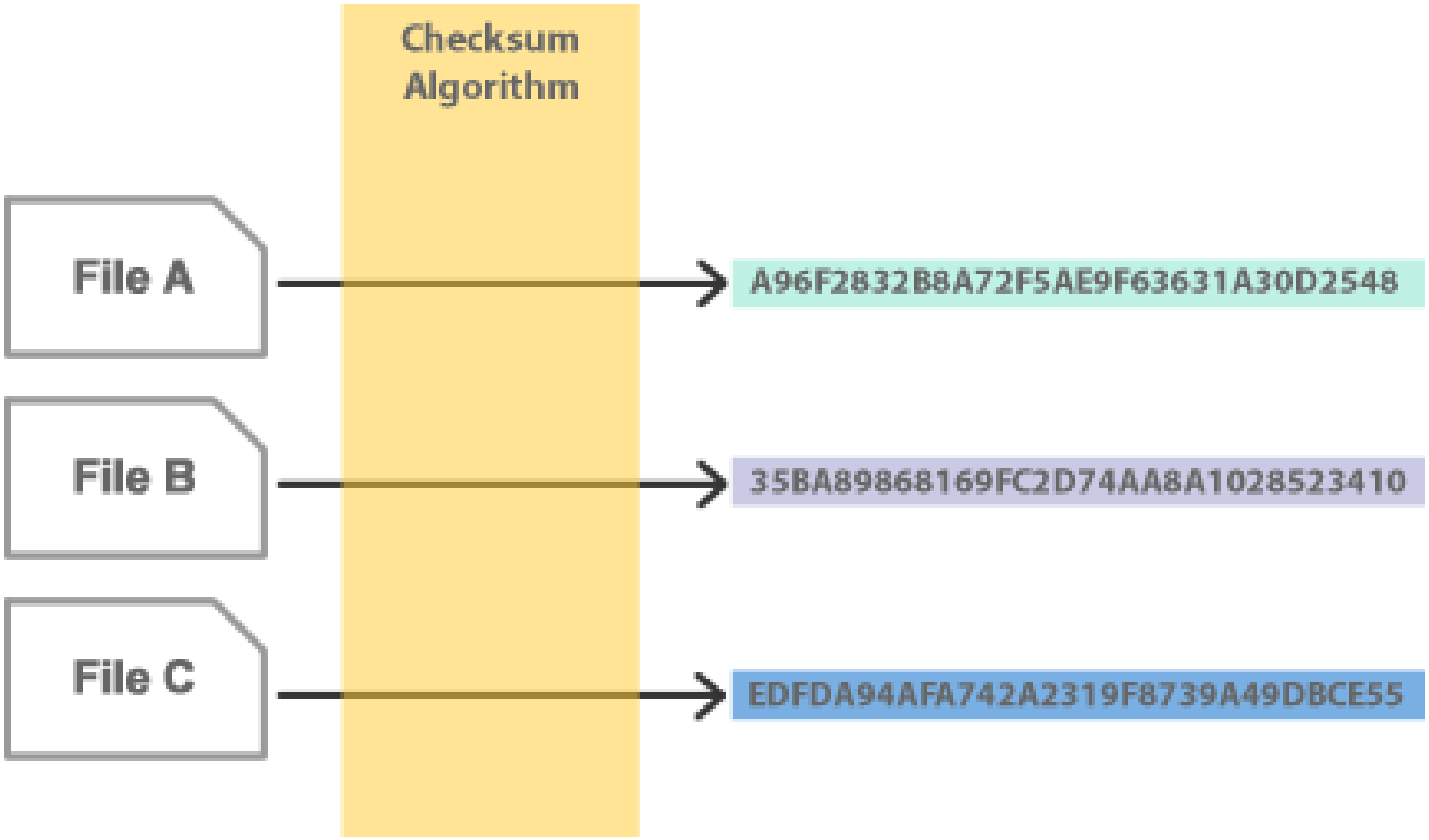
- Bob is confirming an order with Alice, which she is ordering from Bob’s website.
- Bob confirms the order and his computer creates a hash of the confirmation.
- The computer encrypts the hash with Bob's private key.
- The encrypted hash, which is the digital signature, is added to the document.
- The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



Signing and verification



Checksum algorithms



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.

Subject: user, NPE

Access Control Mechanism

Object: file, data, resource

Authentication, Authorisation, and Accounting

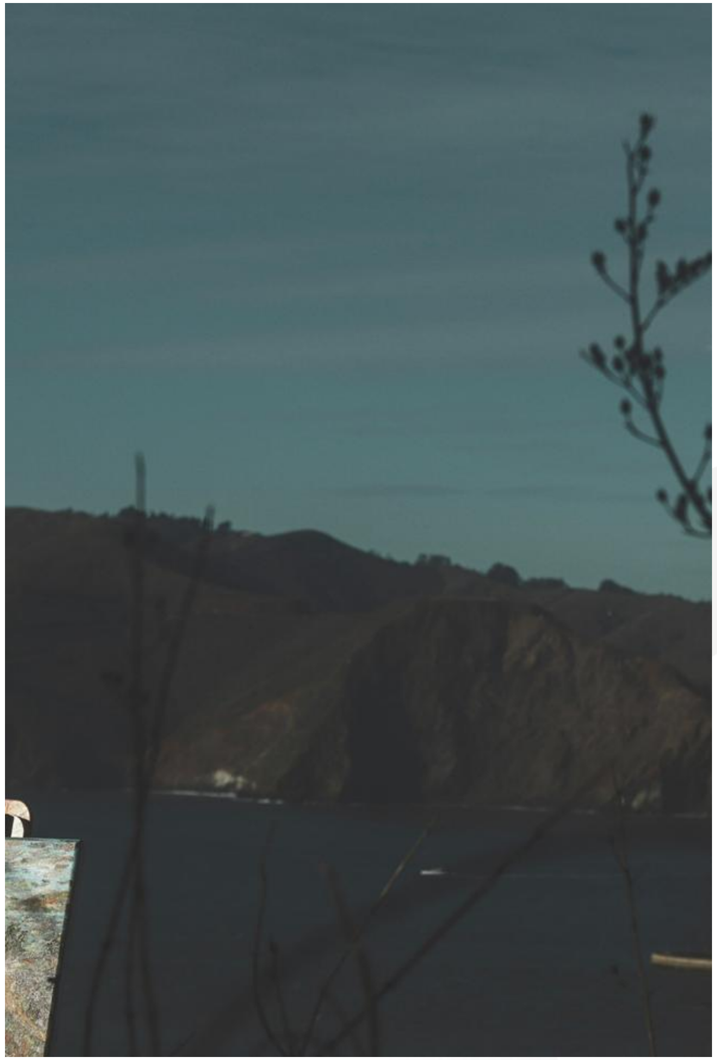
- Authentication
  - Who are you?
  - “I am user student and my password validateme proves it.”
- Authorization
  - What can you do? What can you access?
  - “User student can access host serverXYZ using Telnet.”
- Accounting
  - What did you do? How long did you do it? How often did you do it?
  - “User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

Availability

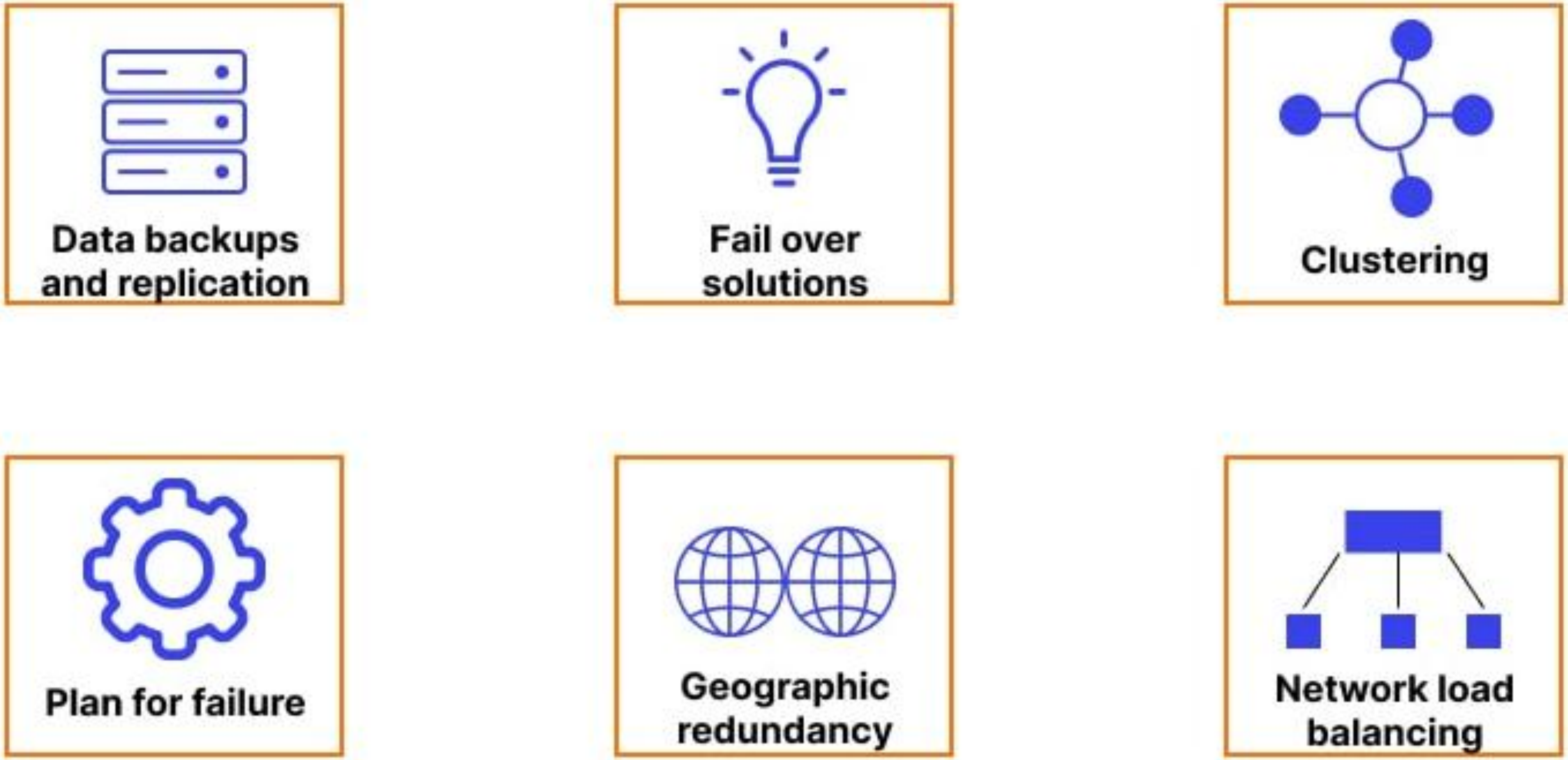
Ensuring authorised users have timely access to data is a critical aspect of cybersecurity.

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



Best practices for high availability



Activity: CIA Triad Analysis

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

Scenario	Step 1: Identify CIA Triad Aspects	Step 2: Discuss Mitigation Measures	Sharing findings	Example Solutions
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: 1. **Phishing Attack** 2. **DDoS Attack** 3. **Accidental Data Overwrite**	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.	

BPP

NIST 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.’

NIST Cybersecurity

The framework…

Identify	Protect	Detect	Respond	Recover
Risk assessment or vulnerability analysis	DNS Filtering Employee training Multi-factor Authentication Mobile device security Firewall Updates / patches Anti-spam Encryption Security policies Password management	Dark web monitoring		Backup Incident Response

Threat hunting

Security Information & Event Management

Security Operations Centre (SOC)

Endpoint Detection and Response

NIST Cybersecurity Framework

Building Careers Through Education

Everybody Matters.

Stronger Together.

Student, Learner and Client Centric.

Trust and Respect.

Embrace Change.

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

BPP

Importance of Monitoring in Cybersecurity

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

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.

BPP

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

Conducting a binary risk assessment

- **(1) Identify Assets**

  Determine the critical data, systems, and resources that are essential for the organisation'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**

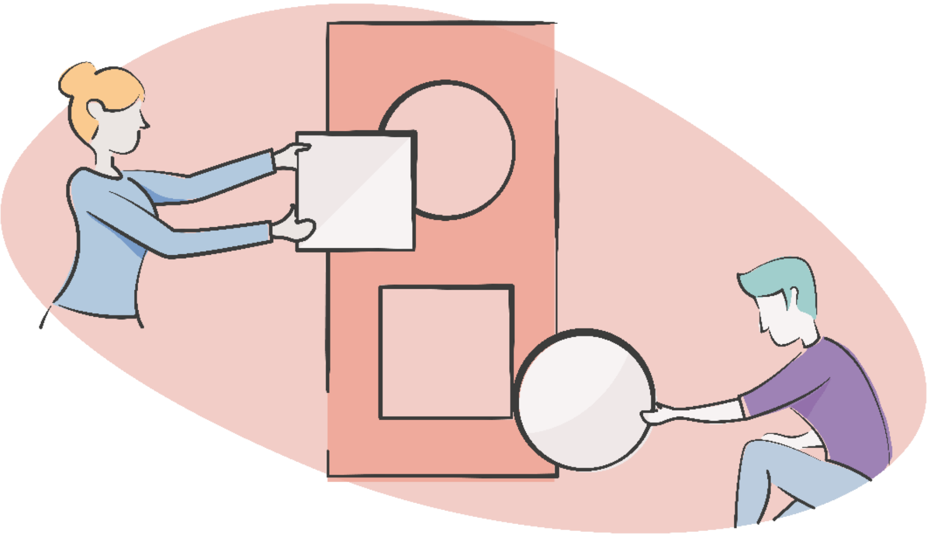
  Implement appropriate security controls and measures to mitigate the identified risks, such as access controls, backup procedures, or incident response plans.

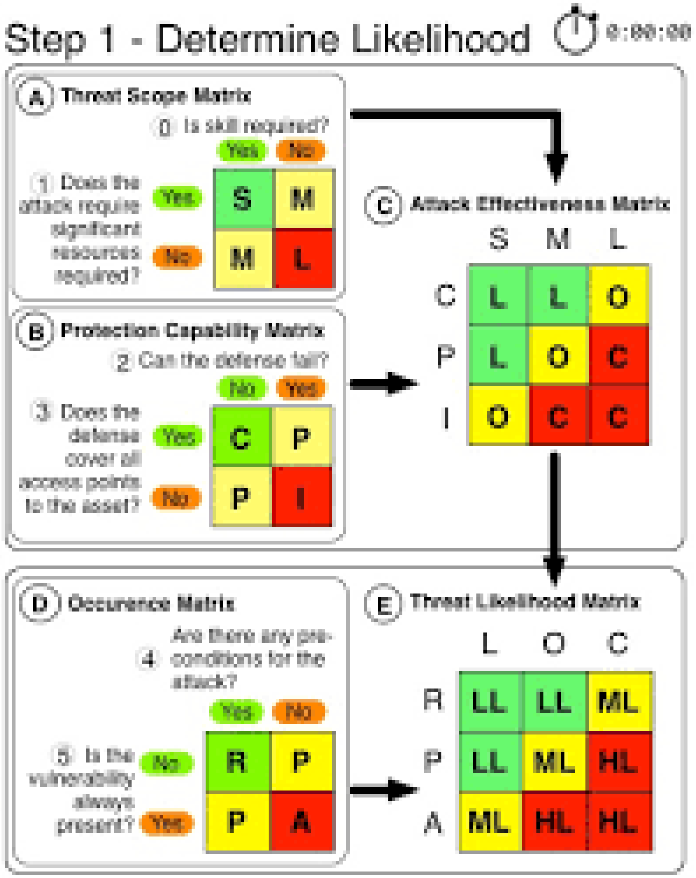
Lab

Risk analysis

Your tutor will guide you through Binary Risk Analysis:

https://binary.protect.io/





Interactive activity

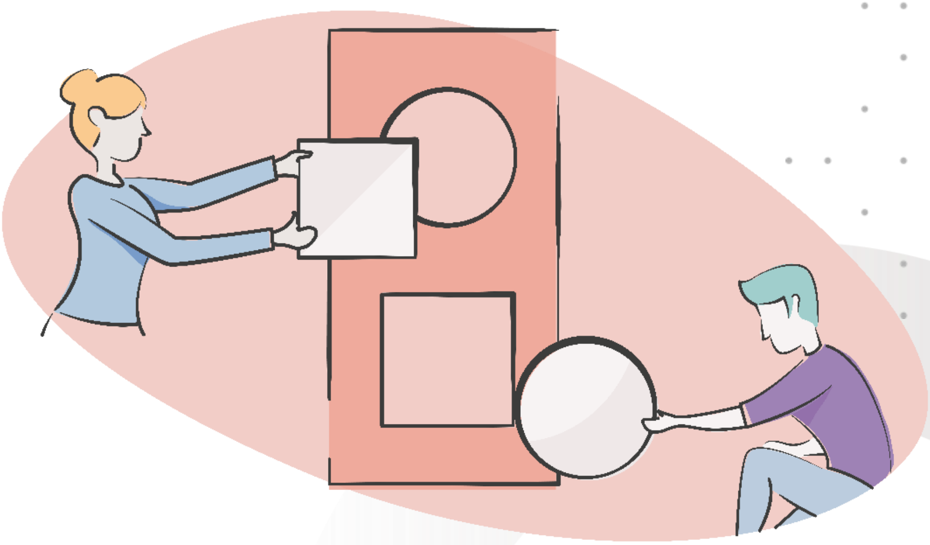
Binary risk assessment

- **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.



Understanding Financial Impact - Definitions

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

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 organisations make informed decisions on risk management and resource allocation.

BPP

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

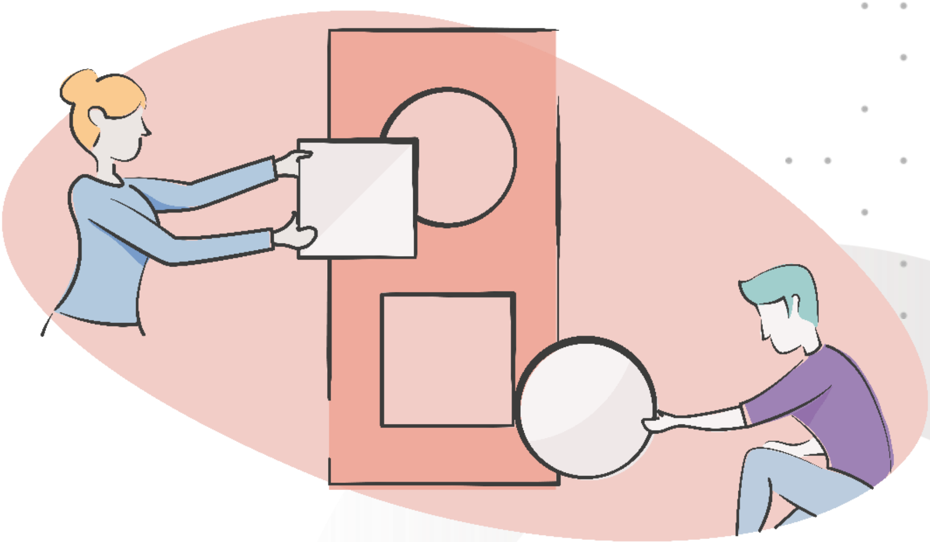
Using digital signatures

- **Calculating ROI:**
  - **Formula:** ROI = (ALE before control - ALE after control) / Cost of control
- **Example:**
  - **Scenario:** Implementing an anti-phishing solution costing £10,000 reduces ARO to 0.1.
  - **Calculation:**
    - **New ALE for Ransomware:** £50,000 * 0.1 = £5,000
    - **ROI for Anti-phishing Solution:** (£10,000 - £5,000) / £10,000 = 0.5 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.



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

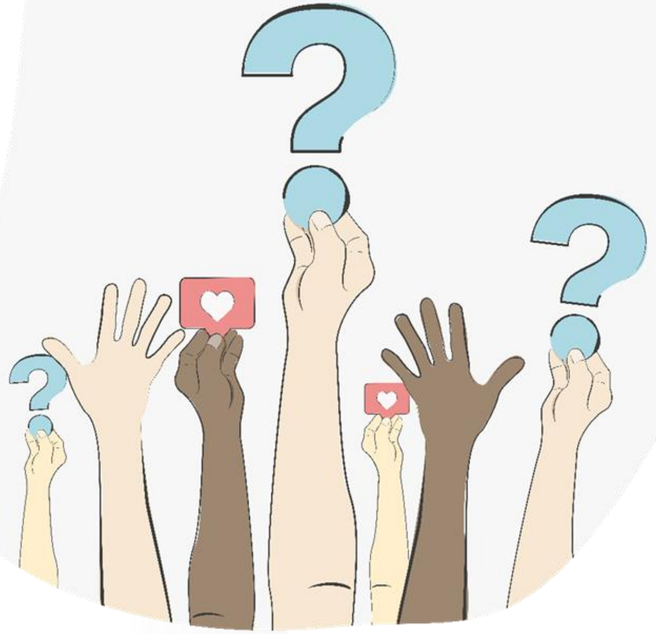
- SIEM Systems
- IDS/IPS Tools
- Encryption Software

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)



Any questions or feedback?