Wi-Fi security 1

Practice 2

James works as a financial adviser at Security Guru. There are two company Wi-Fi networks:

1. **security_guru** - an encrypted end-to-end WiFi that uses WPA3 technology,
2. **secur1ty_guru_guests** - openly available and does not require any type of authentication.

James is currently out of range for **security_guru** but has the option to use **secur1ty_guru_guests** to send a work email.

Based on the scenario above, select the **two** correct pieces of advice.

- [ ] James should not connect to the network 'secur1ty_guru_guests' to send his business email or any important or sensitive information.
- [ ] James could connect to the network 'secur1ty_guru_guests', but he needs to know that it does not protect against attacks or encrypt data.
- [ ] James could connect to the network 'secur1ty_guru_guests', but only to check his personal email and to log into his social media accounts.
- [ ] James could connect to the network 'secur1ty_guru_guests' without concerns as it is very secure.

Wi-Fi security 3

Practice 1

Mo is planning a festive light extravaganza for the outside of his house. There will be flashing snowmen, reindeer, santas, bells, stars, and a whole lot more.

The lighting sequence will be controlled by a program which Mo has written to run on a Raspberry Pi; this computer will be configured to act as a server. Each individual set of lights will be set up as a node on the lighting network. Wireless communications will allow each node to receive messages from the server to control its activity.

How should Mo ensure that his system cannot be hacked by someone who might wish to take control of the lights?

- Use the CSMA/CA protocol
- Use the CSMA/CD protocol
- Use the WEP protocol
- Use the WPA2 protocol

Quiz:
STEM SMART Computer Science Week 34

Penetration testing 2

Practice 1

The following table describes some examples of how criminals explore human and technical vulnerabilities to gain unauthorised access to data.

Human vulnerability
Scanning social media for hobbies, interests, and home address
Scanning for personal and work email addresses to identify friends and colleagues
Scanning for personal and work phone numbers to help identify linked accounts and associates
Scanning online activity to find usernames and passwords
Scanning for work colleagues, their responsibilities, and hierarchy
Technical vulnerability
Scanning the system to identify weak spots and open doors
Gaining access to the system then expanding access once within it
Extracting copies of data, documents, and/or information for future analysis and exploitation
Establishing a route to get back into the system easily in future should this be required
Covering tracks, so the means of access and activities carried out are hard to determine even for an expert

Which type of penetration test can be done to simulate or identify cyberattacks from an internal perspective, where the tester already has knowledge about and access to the system and knows how the network topology is designed?

- White-box penetration testing
- Grey-box penetration testing
- Black-box penetration testing

Quiz:
STEM SMART Computer Science Week 34

Biometric types

Practice 1

Fill in the gaps to describe the types of biometrics:

Biometrics use _____ human characteristics to identify a user. Biometric measurements can include voice recognition, facial recognition , retina scanning, and _____.

Fingerprint recognition scans the _____ and valleys of your fingerprint. Facial recognition scans the _____ of key facial features such as eyes and nose.

Items:

unique ridges fingerprint detection measurements

Quiz:
STEM SMART Computer Science Week 34

Biometric advantages and disadvantages

Practice 1

LLM marked question

Biometric authentication works by using unique biological characteristics of an individual to verify their identity. This process involves capturing and storing a biometric sample, such as a fingerprint or facial image, and then comparing this sample to the stored biometric data.

Explain one advantage and one disadvantage of using facial recognition technology for biometric authentication

[2 marks]

Quiz:
STEM SMART Computer Science Week 34

Substitution cipher decrypt

Practice 2

At Bletchley Park, Alan has sent Joan a message that he has encrypted. He has used a substitution cipher where each letter has been substituted by another. This is **not** a Caesar cipher. The substitutions are non-sequential, but the same substitution is always made. For example, he has substituted the letter H with the letter I.

Joan observes that one letter appears more than any other and uses her knowledge of **letter frequencies** as a starting point to decrypt the message. Alan always writes his messages in English.

DTTM DT OF MIT QOMEITF

Can you help Joan decrypt the message? Type your answer in the space provided, leaving a single space between each of the plaintext words.

Quiz:
STEM SMART Computer Science Week 34

Asymmetric encryption 2

Practice 2

Select the **two** statements about asymmetric encryption that are **true**.

- [ ] A message encrypted with a public key can only be decrypted by a related private key.
- [ ] The private key must be used to encrypt the message.
- [ ] Asymmetric encryption uses the same key for encryption and decryption.
- [ ] Asymmetric encryption uses two keys: a public key and a private key.

Quiz:
STEM SMART Computer Science Week 34

Public key cryptography 1

Practice 2

Alma wants to send a message to Byron using an encryption method that involves public and private keys. Which key does she use to encrypt the message?

- Her own public key
- Byron's public key
- Byron's private key
- Her own private key

Quiz:
STEM SMART Computer Science Week 34

Sender authentication

Challenge 2

Ewan wants to send Kasia a message containing some secret information.

- Ewan needs to be sure that only Kasia can decrypt the message
- Kasia must have confidence that the message has definitely come from Ewan

Put the statements in order to describe the asymmetric encryption process Ewan and Kasia should use so that Ewan can be authenticated as the sender.

Available items

- Ewan encrypts with Kasia's public key.
- Ewan and Kasia publish their public keys.
- Kasia decrypts with Ewan's public key.
- Ewan sends the ciphertext message to Kasia.
- Kasia decrypts with her own private key.
- Ewan encrypts with his own private key.

Quiz:
STEM SMART Computer Science Week 34

Symmetric vs asymmetric 3

Practice 1

Complete the table below by dragging and dropping the statements into the correct cells in the table to show the differences between the **symmetric** and **asymmetric** encryption techniques.

Differentiator	Symmetric encryption	Asymmetric encryption
Number of keys		
Speed of execution		
Security		
Length of keys		

Items:

The private key is not shared, and the overall process is more secure

Slower, but allows the sender to be authenticated

Uses a related set of keys, one public and one private

Uses the same key for both encryption and decryption

The secret key is shared, so the risk of compromising is higher

Faster because it uses simple mathematical operations

The length of the keys used is typically 128 or 256 bits

The length of the keys used is larger, typically 2048 bits or higher