THE UNIVERSITY *of* EDINBURGH

School of Informatics, Computing in the Classroom

Cryptography in the classroom

Security Lesson Plan

Level:	Aimed at S1-S2 Level (Suitable for S1-S5)
Estimated time:	10mins
Materials Needed:	Security Video

Learning Outcomes: This lesson aims to:

- Inform the student of a precise definition of security, covering the core C.I.A security properties.
- Inform the student about why the internet is insecure as a medium for communication.
- Introduce the student to the idea of encryption.

Lesson outline:

1. **Ask the students these questions prior to watching the video :**

   "What does it mean for something to be secure?"

   - Likely answers will be descriptive using adjectives - ie . **safe, protected** .., Answers could also include scenarios - ie. **A locked door, money in a safe**
   - Following your judgement, write these answers on a white board for the students to see and assure the students these are all correct

   "Can you give an example of something you think is secure?"

   - Example answers may include :
     - Physical locks that students use - ie. **Bike lock, door lock, Locker lock..**
     - Places or organisations - **ie. The Bank, The Police, The School..**
     - Their data - ie. **Cloud Photos, Social media drafts, information from Video Game**
   - Follow up for each example answer with another question asking **"What's secure about that?"**
     - If the students answer doesn't relate to a scenario where the security of the system is tested (ie. involves an adversary or "bad guy") then follow up with a question asking **"Can you give a situation where would it not be secure?"** or **"Why would it not be secure?"**, If still not right then use own judgement to write a scenario.
     - Write the students reasoning for each on the board.
     - After 3-4 answers explain that all of these answers are correct and link the reason being because there is an adversary ("bad guy") in each that is trying to do something that we don't like. This is a core concept to understand the following content.

2. **Show the Security Video to the class**

3. **Ask the students these questions after watching the video :**

   "What is cryptography ?" - Tip : It's the science of ...

   - Cryptography is the science of keeping information secure.

   "What is cyber-security ?" - Tip : It uses cryptography where ?

- Cryptography for computers!
- Cyber security is the protection of computer devices, networks, hardware and all data and information.

Write the security properties on the board Con.., Int.., Avail.., Auth.. - "Can anyone give examples when the security properties important?"

- Confidentiality - Data is kept secret from adversary when we want it secret
- Integrity - Data isn't altered by the adversary
- Availability - Data is available as expected, adversary can't stop it
- Authentication - Only authenticated parties can get data not the adversary