Lesson plan

|  |
| --- |
| **Topic 4** **Encryption, protocols, digital certificates** |
| Learning Objectives:* Describe the features, applications and implications of encryption methods used to protect
	+ - Data during transmission
		- Stored data
* Describe processes and techniques of protecting data and systems:
	+ - Digital certificates
		- Protocols
 |
| Content |
| StarterPowerPoint Guide: Topic 4 Encryption, protocols, digital certificates**Starter**Get students to look at the three encrypted messages. Can they decrypt them? If students are struggling, you may like to give some clues such as “try reading down”, “try reading backwards” or “try replacing letters with another in the alphabet”. These methods of encryption are easy for computers to solve; however, this lesson will look at more advanced methods which are used in modern cryptography.MainEncryption terminology Take students through the keywords. You may like to first write these on the board and ask students if they know any of them already. You can then tick them off as they are covered in the lesson.A simple shift cipherEncryption is defined and a simple example of encoding using the very unsophisticated “Caesar cipher” is given. The key is 4, so the algorithm uses letters 4 places on in the alphabet from the plaintext. Ask students to apply the cipher to another name in the class.Private key encryptionThe Caesar cipher is a simple example of private key encryption because the same key is used at both ends by the sender and recipient. The weakness of this is that the key somehow must be communicated to the recipient. If the key exchange is intercepted, then messages can be cracked.The most famous example of private key encryption is the cipher used by the Germans in WWII, using the Enigma Machine. It uses an enormously complicated algorithm. Each month, the Germans sending coded messages would receive a code book outlining the key to be used each day. They used a different key each day, and transmitted the day’s key, encoded twice, to the recipient who could then use the key to decode the message. The cracking of the machine is covered in the film The Imitation Game (2015). Further information about the Enigma cipher can be found at: <http://www.counton.org/explorer/codebreaking/enigma-cipher.php>Man in the middle attackWith private key encryption, a hacker can intercept messages during transmission without either party being aware that this is happening. Public key encryptionThis is much more secure. Two keys (which are numbers or text) are made at the same time. A public key which is known to everyone, used to encrypt a message and a private key, known only to the recipient, used to decrypt the message. Private key encryption is used as part of WhatsApp when messages are sent. The following site gives description of the encryption system and suggests how you can verify that your calls and messages are encrypted and the end to end encryption can be verified: <https://faq.whatsapp.com/en/android/28030015/> If students have WhatsApp installed on their phones, they can try this with a partner.Public key encryptionAn explanation and diagram of the process are given in the following three slides. Students may be interested in how keys are made that make encryption easy but decryption difficult. The algorithms are based on prime numbers. It is very easy to multiply two prime numbers together (e.g. 83\*97=8051). It is far harder to work out which two prime numbers when multiplied together make the number 8051. This principle will be used as part of the algorithm to make sure that it is easy to make the key but very difficult to crack.Some governments have banned strong encryption; China has banned WhatsApp because of its strong encryption. The UK government has at various times considered similar measures.Why protect stored data?Personal data of all kinds needs to be held securely, to protect them from both insider attack and external hackers. Some files, such as a file holding user PINs and user IDs, held on a server need to be kept totally secure so that no one can read them. If they are not encrypted in some way, a dishonest employee may be able to gain access to the file and the data on it.Ask students to complete **Task 1** and **Task 2** on **Worksheet 4**.Topic 4 Worksheet 4Topic 4 Worksheet 4 AnswersStoring passwordsPasswords can be stored in plaintext. The problem with having all passwords stored this way in a database is that if unauthorised access to the database is gained, or a programmer gains access or the storage is stolen the entire database of passwords can be stolen. Passwords could be stored in an encrypted form, but if someone gained the key they could decrypt all the passwords. The solution is to store a ‘hash’ of the password.Hashing“Hashing” is a one-way function. It is a method of encoding data in such a way that it can’t be decoded. It can be used to protect PINs and passwords stored in a database so that they cannot be read by anyone. It is never necessary to decode them. Instead, when a password is entered the hash of it is calculated and compared with the stored hash in the database. As such, no secure website should be able to send you a reminder of your password. Older hashing algorithms such as MD5 (Message digest) and SHA-1 (Secure Hashing Algorithm) are now insecure. SHA-256 which is far stronger is used in SSL.Ask students to complete **Task 3** on **Worksheet 4**.Encryption on mobile devicesPortable devices are easily lost or stolen so both individuals and organisations may consider encrypting data held on them.Case study: FBI-Apple disputeIn 2016 the FBI tried to get Apple to produce an update to their software, so they could crack a terrorist attacker’s iPhone. Apple refused as this would place a vulnerability in their software. Discuss with students where they think the boundaries should be between security and the state in trying to keep people safe. Consider discussing whether politicians, who make these decisions, are qualified to fully understand how cyber security works and the implications of making it less secure. Refer to Topic 2, where students saw that a security vulnerability led to the WannaCry ransomware causing millions of pounds worth of costs to the NHS.Case study: QuadrigaCXQuadrigaCX is a currency exchange for bitcoin and cryptocurrency. When the owner died the only keys to decode the currency were lost with him. Many people lost their money, and within a month the company had filed for creditor protection and was no longer trading. Discuss with students how passwords can be kept secure, but also how people can be trusted to have access to them in the event of death, memory loss or a disgruntled employee who holds them ransom.Ask students to complete **Task 3** on **Worksheet 4**.Protocols and HTTPSDefine “protocol” as a set of rules**. HTTPS** is a secure protocol indicating that all communications are encrypted. HTTPS uses either the SSL or TLS protocol, both of which use public key encryption. You can tell if a site uses this encryption as it will have a padlock next to the web address. Show students this protocol in a web browser as they may not have consciously been aware of its meaning.Website certificatesAn SSL or TLS certificate is an example of a digital certificate used to authenticate websites. Transport Layer Security (TLS) is an improved version of SSL. The two terms are often used interchangeably in the industry. For a more detailed description of digital certificates, see: <https://sites.google.com/site/amitsciscozone/home/security/digital-certificates-explained> Wireless Encryption standardsWEP and WPA, WPA2 and WPA3 are security protocols securing wireless computer networks by encrypting data. Students should be aware that WPA2 or higher should be used on their home routers to be secure. Remind them to check when they go home. WEP is very easy to crack within seconds.Ask students to complete **Task 5** and **Task 6** on the worksheet.PlenaryAsk students to work in pairs and write questions related to the key words used in the lesson.Hand out **Homework 4**.Topic 4 Homework 4Topic 4 Homework 4 Answers |