# Answers

Task 1

Give **three or more** examples of organisations or individuals that might need to protect data that they hold on their computers by encrypting it?

In each case, state what the data could be and why they would need to protect it.

* Businesses use encryption to protect corporate secrets from industrial espionage.
* Exam Boards could use it to protect exam papers before the exam is taken.
* Newspapers might protect communications from their journalists and articles or photographs stored on their server.
* Banks and credit card companies need to protect their customers’ personal details.
* Individuals may protect data on their mobile phones and other portable devices to keep them safe from identity theft or from gaining access to contact lists, emails or messages, photos, confidential information of all kinds.
* Terrorists, spies, criminals, police and MI5 may use encryption to protect secret, classified or confidential information and identities.
* Websites with logins will use encryption to store passwords, so that even if the data is stolen, hackers will not be able to see the actual plaintext password.

**Task 2**

Bartek is shopping on the Internet and goes to a new website he has never visited before. The website is located in the USA and needs his credit card details in order to make a purchase. If these details aren’t encrypted, anyone with access to the network connections between his computer and the server in the USA would be able to read the card details.

Describe how it is possible for card details to be transmitted in encrypted form when Bartek has never been sent any kind of password from the website.

1. Public key encryption is used.
2. The website will send Bartek’s computer a public key which anyone can find out.
3. Bartek’s computer will take personal details such as his credit card number and encrypt these with the public key.
4. The encrypted information is sent to the website.
5. The website’s server will use a private key to decrypt the contents of the message.
6. Bartek’s computer and the server will store the necessary keys so that Bartek is unaware of the encryption being carried out.

Task 3

Websites should only store the hash of a password rather than the actual password.

The following table shows attempts to log in by users.

(a) Open the file usernamespasswords.xls

(b) Go to the website: <https://passwordsgenerator.net/sha1-hash-generator/>

(c) For each of the username and password log in attempts in the table below, state whether the user should successfully be logged in or not. You will need to type their password into the website to check if the hash matches that stored in the database. The first attempt has been done for you.

|  |  |  |
| --- | --- | --- |
| Log in attempts | |  |
| Username | Password | Correct password? |
| mjohnson1 | iloveyou | Yes (the hash in the file matched the hash generated on the website) |
| lwilson1 | donald | No |
| pjackson1 | monkey | Yes |
| lgreen3 | !@#$%^&\* | Yes |
| osmith3 | 123123 | No |
| osmith3 | admin | No |
| osmith3 | 123456 | Yes |

Task 4

Discuss arguments for and against enabling governments and security services to access messages secured by end-to-end encryption. You may find the following website helpful before you discuss this:

<https://www.zdnet.com/article/the-uncrackable-problem-of-end-to-end-encryption/>

**For:**

Secure end-to-end communication means that police and security services cannot access information that they need to detect and prevent crime and terrorist attacks.

This makes it easier for criminals and terrorists to plan and communicate securely.

**Against:**

To allow police access to those messages, companies such as WhatsApp would have to change the way they use encryption, and they would then be able to decode every message. That makes everyone using such a service less secure than they were before.

Hackers and foreign governments, as well as the security services, would be able to decode the messages.

End-to-end encryption is essential for preventing data being accessed illegally in ways that can harm consumers, business and our national security.

A further problem is that most tech companies are not based in the UK, and UK laws may not apply, even if such a law is passed.

Task 5

(a) Look up **three or more** websites. Which of them have a padlock symbol indicating that all communications are encrypted?

Student answers will vary.

(b) Websites that use SSL encryption and security certificates will have a padlock next to their web address. Click this padlock to show the information. What information is provided?

Information about their security certificate (who it is issued to and who it is issued by, when it is valid from and to).  
The public key used by the website.  
Information about cookies and site settings may also be given.

(c) Find **two** websites that use the HTTP protocol and therefore do not use encryption.

Students may struggle these days to find a website that only uses HTTP. There may be some for smaller sites that don’t wish to pay for a security certificate or do not need one as they do not require any personal data to be transferred.

**Task 6**

Look up PayPal’s security measures designed to ensure that payments cannot be intercepted by hackers intercepting a connection request and diverting payment to themselves.

<https://www.paypal.com/us/webapps/mpp/security/security-protections>

(a) What methods are used to make sure that data is secured by PayPal?

TLS/HTTPS encryption  
Key pinning (the app can only connect to true PayPal servers  
PCI-DSS (industry encryption requirements)  
PayPal security key (two factor authentication) – delivered by SMS/text message to a mobile

(b) PayPal states:

**TLS Connection**

When you register or log into PayPal from your computer or mobile device, we make sure you’re connecting with TLS 1.0 or higher and only make HTTPS connections (HSTS).

Explain what TLS means.

Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL). It is a cryptographic protocol that enables secure communications over the Internet. This means that data is encrypted between the user’s browser and the web server.

(c) Search the Internet for more information on digital certificates.

(i) What is the purpose of a digital certificate?

Purpose of a digital certificate:

* Make sure that you are connected to a web server that has obtained a valid SSL/TLS certificate
* (for extended validation certificates) Make sure that the organisation is verified by an independent company – in this case, the web address or padlock will turn green
* Digital certificates can also be used to verify the sender of other electronic data such as email
* The cryptography public key is associated to the name of the person or organisation that it belongs to

(ii) How do you obtain a digital certificate?

* The digital certificate is issued by the certification authority (CA)
* A fee needs to be paid for the certificate
* Other documents may be needed to verify the identity of the person/organisation applying for the certificate