Name: Class:

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.

**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.

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 |  |
| pjackson1 | monkey |  |
| lgreen3 | !@#$%^&\* |  |
| osmith3 | 123123 |  |
| osmith3 | admin |  |
| osmith3 | 123456 |  |

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/>

Task 5

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

(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?

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

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?

(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.

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

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

(ii) How do you obtain a digital certificate?