

SSL, private key and public key encryption



Step 1 A customer decides that they want to buy an item from an online shop

Step 2 The customer chooses the items from the website and clicks 'make payment'

Step 3 The customer is taken to a secure page with https in the address and a padlock symbol in the corner

Step 4 The secure page is using Secure Socket Layer (SSL) protocols (rules) and the customer can feel safe entering their credit card details

Step 5 The customer enters their credit card details and their personal information into the web form.

Step 6 The information entered by the customer hasn't yet been encrypted. At this stage it is called 'plain text'

Step 7 When the customer is ready, they press the submit or send button. A message usually appears which says 'processing order'

Step 8 When the 'submit order' button has been pressed, the SSL sends a message to the shop asking for the public key to be sent back to the customer

Step 9 The shop's public key is received by the customer's SSL. It is applied to the 'plain text' typed in by the customer earlier.

Step 10 The plain text containing the customer's personal and financial details are encrypted. They are now called 'cipher text'

Step 11 The customer's browser now sends the encrypted cipher text safely over the internet to the shop.

Step 12 Even if hackers were to intercept the message, the encryption is so secure that they would not be able to decipher it.

Step 13 The SSL on the shop's server recognises that the shop's public key has been used to encrypt the message.

Step 14 The shop's ecommerce system uses the shop's 'private key' to decrypt the cipher text back into plain text so that it can be understood.

SSL, private key and public key encryption task



1. How does the customer know that they are on a secure site?
2. What happens when the customer presses the 'submit' button?
3. What is the purpose of the 'public key'?
4. What is the purpose of the 'private key'?
5. At what stage in the process is the customer's information encrypted?
5. Should customers be concerned about hackers intercepting their information whilst it is being sent across the internet?

Name Form

You may:

- Guide teachers or students to access this resource from the teach-ict.com site
- Print out enough copies to use during the lesson

You may not:

- Adapt or build on this work
- Save this resource to a school network or VLE
- Republish this resource on the internet

A subscription will enable you to access an editable version and save it on your protected network or VLE