FACTFILE:
GCE DIGITAL TECHNOLOGY

AS2: FUNDAMENTALS OF DIGITAL TECHNOLOGY: WEB TECHNOLOGY AND MULTIMEDIA

Rewarding Learning

WEBSITE DEVELOPMENT 2

Learning Outcomes

Students should be able to:
- Encryption (including public and private keys);
- Hypertext transfer protocol secure (https);
- Secure Sockets Layer (SSL);
- Digital signature or digital certificate.

Content in Web Applications 2

- ✔ Encryption as a method of security over the Internet
- ✔ Digital Signature and Digital Certificate
- ✔ Hypertext Transfer Protocol Secure (https) and Secure Socket Layer(SSL)

Encryption as a method of security over the Internet

Cryptography is the science of hiding information. The process of transformation itself is called encryption. To encrypt the data an algorithm or cipher is used.

Encryption is a method of providing security for data both when it is stored electronically and whilst it is being transmitted. The data is 'scrambled' using an encryption key. This encrypted data is meaningless to anyone accessing it. The data must be decrypted using a key, so that it can be understood. Some systems use the same key for encryption and decryption, particularly if the number of users is small.

Public key cryptography uses two different keys, one for encrypting the data and a different one for decrypting the data. This Public and Private key pair are linked and both keys are needed to encrypt and decrypt data.

The Public Key is available to everyone but the Private Key is confidential and specific to a particular receiver. The key pair is mathematically related, so, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

If user A wants to send an encrypted message to user B, user A will encrypt the data using user B's Public Key. Only user B has the matching Private Key to decrypt the message. Therefore, if a third party accesses the encrypted data, they will not be able to read or decrypt it as they do not have the Private Key. The Public Key is available to anyone so, it is possible that a forged message could be sent to user B. In order to prevent this, digital signatures are used.

Digital Signature

A digital signature is a part of a message that is encrypted by the sender. It is used to confirm that the sender is who they say they are. The receiver first verifies the signature using the sender's public key. After ensuring the validity of the signature, the receiver then retrieves the data through decryption using his/her own Private Key.

Digital Certificate

A digital certificate is also used to verify a sender's authenticity. It is used widely with websites. Companies or individuals requiring digital certificates apply to a trusted third party called a Certificate Authority (CA), a company which provides online certification. An example of a CA is Verisign. The CA provides an encrypted digital certificate which contains, among other things, the user's public key. This connects an individual or website with a particular public key therefore the trusted third party verifies their identity. When a company asks for a certificate, they have to give information about the web server and the location of the company. CA will authenticate this information. The CA authority then creates and signs the certificate. The certificate is given back to the company who installs it on the server.

Browsers are shipped with information about the certificates. In particular the Public Key for the certificates and so they can check the authenticity of most certificates.

Digital certificates can be:

- Personal – used by individuals who need secure email;
- Organisation – used by organisations for employees who need secure email and web transactions;
- Server to prove ownership of a domain name or for use with SSL
- Developer – to prove ownership of software/ programs

Hypertext Transfer Protocol Secure (https) and Secure Socket Layer(SSL)

All data transmitted across HTTP connections are in 'plain text' and can be read by any individual who can hack into the connection between a browser and a website. Hypertext Transfer Protocol Secure(https) is used to encrypt data when it is being transferred across the Internet. A page displaying https:// at the beginning of the web address will make use of encryption to secure data transmission. HTTPS web pages use SSL (or TLS –Transport Layer Security). During this process, a Public and Private Key are utilised together with a digital certificate. This ensures that if a hacker did break into the connection, they could not decrypt any of the data.

SSL is a protocol used to open a secure channel or encrypted link between two computers online. It is used when a web browser needs to connect securely to a web server. SSL certificates exist to encrypt data and identify websites. This allows a web browser to trust a website so that sensitive data can be transmitted safely. The goal is end to end trusted communication.

SSl instantly encrypts plain text like credit card numbers into data that only the user and website can decrypt. SSL ensures that the data is not modified and it authenticates websites. To verify that SSL is protecting a page, look for a web address beginning https:// and a closed padlock icon. Companies using an extended validation display the data in a green address bar. An SSL digital certificate shows that the website is secure and visitors can be re-assured that their data will be protected whilst using it.

If a website is not using SSL, any data being transmitted can be accessed by any computer on the network. When doing online banking we are using SSL and HTTPS. The following steps occur:

- The client computer requests an SSL connection
- The server answers and provides an SSL certificate which contains a public key
- The client computer validates the certificate and public key
- The client computer generates a session key and submits it to the server
- The SSL connection is established

Questions

1 Browsers are shipped with digital certificates. Explore what certificates are shipped in a computer and describe how this contributes to the overall security of data when using the Internet.

2 Create a graphic representation which describes the process of data encryption and decryption using public and private keys.

3 Investigate how the following browsers facilitate secure data transfer.

- Safari
- Opera
- Firefox
- Internet Explorer

Bibliography
BCS Academy Glossary Working Party, 2013, *BCS Glossary of Computing and ICT*, 13th Edition, Swindon, BCS Learning and Development Ltd