**NAME : PATRICK GICHINGA KIMANI**

**REG. NO. : C025-01-0966/2015**

**COURSE : BSc. INFORMATION TECHNOLOGY**

**UNIT CODE : BIT 2317**

**UNIT NAME : FUNDAMENTAL OF COMPUTER SECURITY**

**TASK : ASSIGNMENT 2**

**DATE : 25TH JULY, 2018**

**What is SSL?**

Secure Sockets Layer (SSL) is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication. A SSL certificate is used to create SSL connection.

**How SSL works**

1. An end-user asks their browser to make a secure connection to a website e.g. https://www.dkut.ac.com
2. The browser obtains the IP address of the site from a DNS server then requests a secure connection to the website.
3. To initiate this secure connection, the browser requests that the server identifies itself by sending a copy of its SSL certificate to the browser.
4. The browser checks the certificate to ensure:
   1. That it is signed by a trusted CA
   2. That it is valid - that it has not expired or been revoked
   3. That it confirms to required security standards on key lengths and other items.
   4. That the domain listed on the certificate matches the domain that was requested by the user.
5. When the browser confirms that the website can be trusted, it creates a symmetric session key which it encrypts with the public key in the website's certificate. The session key is then sent to the web server.
6. The web server uses its private key to decrypt the symmetric session key.
7. The server sends back an acknowledgement that is encrypted with the session key.
8. From now on, all data transmitted between the server and the browser is encrypted and secure.

**Where it is used.**

1. Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
2. Communication applications such as Email, file transfer, instant messaging and voice over IP.
3. Transferring sensitive information such as credit card numbers, social security numbers and login credentials.
4. The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
5. The connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.