Computer Law and Ethics (COSC-3325)
Assessment of Lesson 3

Exercise 1. What encryption and decryption mean? Give examples for each technique.

Exercise 2. What cryptography and cryptanalysis mean?

Exercise 3. What is a cryptosystem? Give an example.

Exercise 4. What conventional cryptography means? Give examples of conventional cryptography.

Exercise 5. What is a session key? How it is created?

Exercise 6. Let us consider the prime number p=29 and base g=5. Suppose Alice sends Bob the value A = 8. Calculate how much Bob gets as his session key provided that he chooses b = 7. If Alice choose a = 4, calculate Alice's session key. Is Bob's session key the same as Alice's session key? Why or why not?

Exercise 7. How to make the Diffie–Hellman's protocol more secure?

Exercise 8. What is a password-authenticated key agreement?