	COURSE: Information Security Auditing			**MARKS**:
	CODE: ITCS4340	**ASSESSMENT:** Lab 4	**DURATION:** 2 Hours	
Cryptography				

Lab Objectives:

Through this lab sheet, student will have the ability to:

1. Study the cryptographic tools.
2. Learn cryptography concept and application.
3. Investigate some common attacks and analysis for cryptography.

Tasks:

(A)

1. Install CrypTool (SetupCrypTool_1_4_30_en.exe). Download it from this site (*https://www.cryptool.org/en/ct1-downloads*)
2. The application CrypTool is a comprehensive educational program about cryptography and cryptanalysis. You can use it to apply and analyze cryptographic algorithms.
3. Apply and Use this tool to learn cryptography concept for :
   a. Classic Crypto (Caesar, Playfair ,Vigenere and Permutation/transposition cipher)
   b. Modern Crypto

(B)

1. Search on net other cryptographic tools available and their features. Features may be in terms of size, speed, different algorithms, etc.
2. Do findings on the tool and compares it with the given tool in task A; CrypTool.

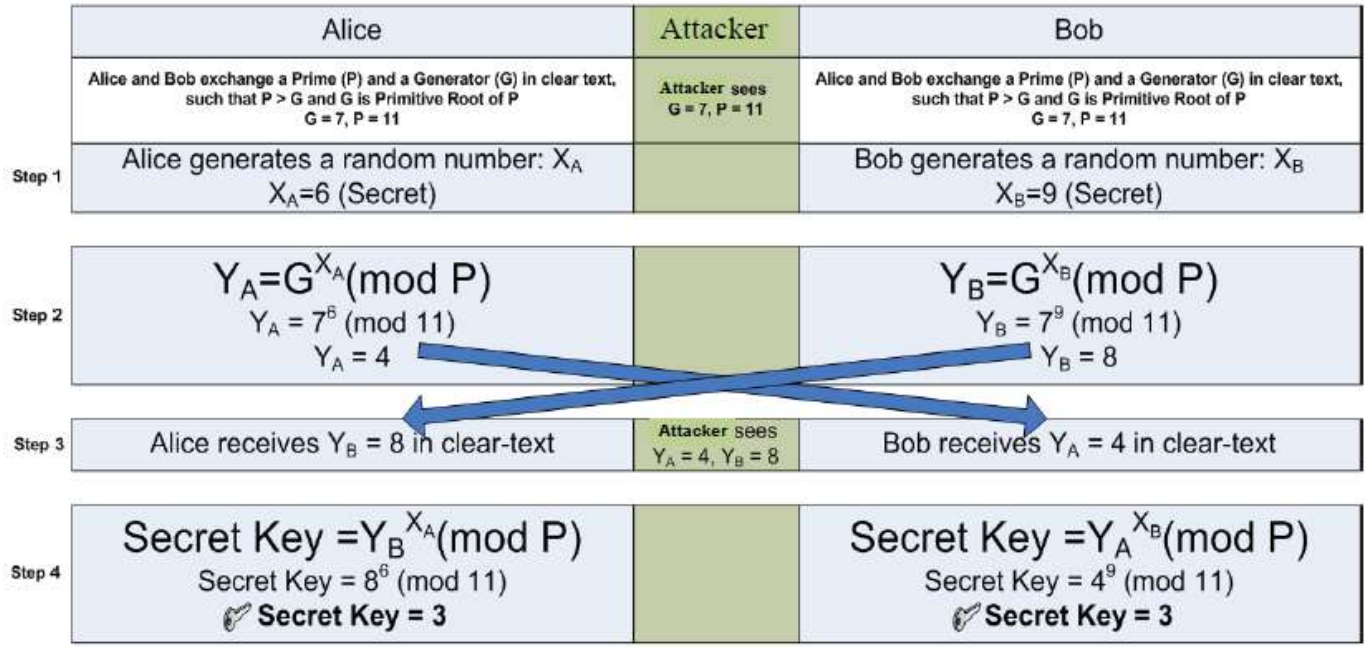
(C)

Certificates for HTTPS/TLS 2.a

1. Use Chrome to open a webpage that supports TLS. For example, https://commbank.com.au/ Click on the lock shown on the left from the address bar.
   - Who is the issuer of the certificate and how long is it valid?
   - Which cipher suite is used? You might need to reload the page to see connection information.
2. Can you find the list of all certification authorities that are installed in Chrome?

(D)

Write a program in VB to Implement Diffie-Hellman key exchange algorithm.



End of Lab 4