# COMP 189: Homework 7

Assigned March 30, 2020

Due midnight April 13, 2020

30 points total

# Technical Exercises

*For each problem, show all your work (required for credit). For answers requiring written answers, while no more than five or six sentences are expected, sufficient justification must be given for any position, opinion, or perspective taken.*

## 1. Encryption (12 pts)

Show all your work - in particular, show all the binary sequences you generate and use along the way. Feel free to use an online ascii-to-binary calculator to compute the bits required.

1. Convert your first name into ASCII-formatted binary (1 byte per letter). Write the binary sequence out, grouping bits into groups of 4, as was done with the word ``HELLO'' in the lecture. (2 pts)

My first name is YE, so the ASCII index are 89,69.

The binary sequence of Y is 01011001

The binary sequence of E is 01000101

The binary sequence of YE is 0101 1001 0100 0101

1. Generate a random binary key with the same number of bits as your binary-encoded name. (2 pt)

The generated random binary key is: 0011 0101 1100 1010

1. Encrypt your name using the XOR function as was shown in class. (4 pts)

binary sequence: 0101 1001 0100 0101

random key: 0011 0101 1100 1010

XOR encryption: 0110 1100 1000 1111

1. Now decrypt your name using the XOR function as was shown in class. (4 pts)

XOR encryption: 0110 1100 1000 1111

random key: 0011 0101 1100 1010

binary sequence: 0101 1001 0100 0101 “YE”

## 4. SSL (8 pts)

Diagram and explain the way encryption is established in the simplified SSL protocol we covered in class. Explain each step in the process. A close up of text on a whiteboard

Description automatically generated

The user first send a request to the website, say CIBC online bank. Then, the website will respond the request and send back a public key for encrypting the information. After receiving the public key, the user now is able to generate the information needed to send to CIBC and then encrypt the information by using the public key sent by CIBC. Once the CIBC online bank reveiced the encrypted information, it will decrypt the information by the same key. After doing so, the CIBC online bank will receive the information sent by the user. Right now, the website and the user are able to communicate with each other by this way.

## 5. SSL key exchange (5 pts)

The SSL protocol does not involve the client (you) sending a public key. Why would this be a bad design?

It is undoubtedly a bad idea to involve the client sending a public key. If the public key is sent by the client side, the server of the website will receive tremendous amounts of public keys. Takes the CIBC online bank for an example again. If every client of CIBC sends a special key to CIBC online bank, the server of the online bank will receive lots of keys, which is really inefficient. However, if the public key is sent by the server side, it can use the same public key for every client, which is much more efficient.

# Discussion

In the following questions, give a written answer (not bullet points).

## 1. Symmetric encryption (5 points)

Explain why we can’t use ONLY symmetric encryption to keep all content secret on the internet. Be precise – what aspect of symmetric encryption makes it impossible to keep secrets on the internet.

Since the principle of the symmetric encryption, both the process of encryption and decryption will use the same key. By doing so, we have to exchange the public key to the other side. Say if the clients want to use the CIBC online bank, the CIBC has to send the public key to the client first. The process of sending the key will not ensure the security of the public key. However, if we use the asymmetric key, we do not need to exchange the key. The encryption process will use the public key, and the decryption process will use the private key. Since there is no need to exchange the key, so it will be safer than the symmetric key.