SECURITY IN COMPUTING COSC2536/2537

ASSIGNMENT #1

Total Marks: 15 (Contributes 15% of the total Grade)

Submission Deadline: Week 4, Friday the 10th August 2018 11:59pm

Special Instructions:

- **You are required to show all of the steps and intermediate results for each question.**
- **Please DO NOT provide codes as an answer.**

Q1

(a). [Double Transposition Cipher] (Marks 1.5)

Decrypt the following ciphertext using the **double transposition cipher** (as discussed in the Lecture-1 and Tute-1) using a matrix of **11 rows** and **7 columns**.

SOGIUNBCNUODLMIXOTSINCRHINPEHNWRTOAROSATNPHAIITSSOB

OFEDUOOTSPIIELMXNAPESATLRN

Hint: The first word in the plaintext is "THIS".

(b) [Cryptanalysis on Simple Substituion Cipher] (Marks 1)

Find the **plaintext** and the **key** for the following ciphertext using the concept of *simple substitution cipher* as discussed in Lecture-1:

UMYTMHUZSRGZ

(c) [Cryptanalysis on Substituion Cipher] (Marks 2)

Assume that the following **ciphertext** has been produced using a substitution cipher. Please note that it may not be a simple 'shift by *n*'substitution. The ciphertext is as follows:

XDJ MJXDGSGQGVK FJDHNS OBJECJNTK UNUQKWHW BJQHJW GN XDJ OUTX XDUX HN UNK QUNVCUVJ, JUTD QJXXJB DUW HXW GRN ZJBWGNUQHXK. XDJ MGWX GFIHGCW XBUHX XDUX QJXXJBW DUIJ HW XDJ OBJECJNTK RHXD RDHTD XDJK UZZJUB HN U QUNVCUVJ. TQJUBQK HN JNVQHWD XDJ QJXXJB "L" UZZJUBW OUB QJWW OBJECJNXQK XDUN, WUK, "U". HN XHMJW VGNJ FK, HO KGC RUNXJS XG OHNS GCX XDJ OBJECJNTHJW GO QJXXJBW RHXDHN U QUNVCUVJ, KGC DUS XG OHNS U QUBVJ ZHJTJ GO XJAX UNS TGCNX JUTD OBJECJNTK. NGR, DGRJIJB, RJ DUIJ TGMZCXJBW XDUX TUN SG XDJ DUBS RGBP OGB CW. FCX HN OUTX, RJ SGN'X JIJN NJJS XG SG XDHW WXJZ, UW OGB MGWX QUNVCUVJW XDJBJ UBJ SUXUFUWJW GO XDJ QJXXJB OBJECJNTHJW, RDHTD DUIJ FJJN TUQTCQUXJS FK QGGPHNV UX MHQQHGNW GO XJAXW, UNS UBJ XDCW IJBK DHVDQK UTTCBUXJ.

Find the **plaintext** by **frequency analysis technique** as discussed in Lecture-1 and tutorial-1.

Q2 [Application of Hash Algorithm] (Marks 2)

Assume that Alice, Bob and Trudy want to participate in an online auction to purchase an item. The idea here is that these are supposed to be **sealed bids**, *i.e.* each bidder gets one chance to submit a secret bid. In order to submit a secret bid, a bidder generates hash value of their bid amount using **SHA-256** hash algorithm, and sends the hash value as their bid to the auctioneer. All of the bids are revealed when all of the participants send their secret bid to the auctioneer. Trudy is a smart person who is certain that Alice and Bob will both place their bids between $95 and $103. Trudy captures the following hash values of Alice and bob:

Hash value of Alice:

8C1F1046219DDD216A023F792356DDF127FCE372A72EC9B4CDAC989EE5B0B455

Hash value of Bob:

454F63AC30C8322997EF025EDFF6ABD23E0DBE7B8A3D5126A894E4A168C1B59B

i. Describe a **forward search attack** **step-by-step** by which Trudy can determine Alice's and Bob's bid from their respective hash values. Use the concepts of forward search attack that is discussed in Lecture-2 and Tutorial-2.

ii. Describe how the above bidding procedure cane be modified to prevent a forward search attack.

Q3 [RSA Encryption algorithm] (Marks 1.5)

Bob is a receiver and Alice is a sender. Bob generates public and private keys using RSA encryption algorithm and sends the public key to Alice. Alice has a message $M=7415$ to send. Bob uses parameter $p=443$ and $q=503$, and chooses a small public key parameter e. What are the values of suitable public and private keys**?** How would Alice encrypt message $M=7415$? How would Bob decrypt the encrypted message C with the private key? Use the concept that is discussed in Lecture-3 and Tutorial-3.

Q4 [Breaking RSA Encryption algorithm] (Marks 2)

Recently, researchers have successfully decrypted the RSA ciphertext without knowing the private key. In this question, we would like to examine your understanding on one of the RSA cryptanalysis techniques, called **prime factorization**. Assume that Alice wants to send a message to Bob. Bob generates public and private keys using RSA Encryption algorithm and publishes the public key

(***n=3901***, ***e=11***). Alice has a secret message ***M*** to send. Nobody knows the value of ***M***. She encrypts the message ***M*** using the public key and sends the encrypted message ***C=1602*** to Bob. Trudy is an intruder who knows RSA and prime factorization well. She captures the encrypted message ***C=160***. She also has the public key (***n=3901***, ***e=11***) because it is known to all. How can she decrypt the encrypted message ***C*** and find the value of ***M***? Show all the steps. Use the concept that is discussed in Lecture-3.

Q4 [ElGamal Encryption algorithm] (Marks 2.5)

Alice has a message ***M*=59** to send to Bob securely using ElGamal encryption algorithm. Bob chooses ***p*=8467**, ***g*=7919**, ***x*=91**. Alice chooses ***r*=51**. Show the encryption and decryption steps. Use the concept that is discussed in Lecture-4 and Tutorial-4.

Q5 [Paillier Encryption algorithm] (Marks 2.5)

Alice has a message ***M*=1234** to send to Bob securely using Paillier encryption algorithm. Bob chooses ***p*=61**, ***q*=97**, and selects an integer ***g* =119**. Alice selects a random number ***r*=67**. Show the encryption and decryption steps. Use the concept that is discussed in Lecture-4 and Tutorial-4.