**CSCE 4013/5013 Applied Cryptography – Homework 5**

**Due date: November 11, 2018**

**1. (20 points)** Suppose an aggregator wants to know the sum of *n* users’ ages. Design a scheme which allows the aggregator to obtain the sum without revealing any individual user’s age to any other party. Assumptions about the system: users can communicate to each other; no party is trusted; at most two users can collude; no user colludes with the aggregator; no party can eavesdrop the communications between any two users. You must design your own solution. Do not copy from any publication.

**2. (16 pts)** Suppose Merkle hash tree is used to authenticate eight messages, m1, m2, …, m8. The eight messages are used to build the Merkle tree, and the root of the tree is signed with a digital signature s. i) To authenticate m3, besides m3 itself and the signature s of the tree root, which elements should be included in the message? How can the receiver verify the integrity of m3? ii) To authenticate m8, besides m8 itself and the signature s of the tree root, which elements should be included in the message? How can the receiver verify the integrity of m8?

**3. (12 pts)** Suppose user A is broadcasting packets to n recipients B1, …, Bn. Privacy is not important but integrity is. In other words, each of B1, …, Bn should be assured that the packets he is receiving were sent by A. User A decides to use a MAC.

a. Suppose user A and B1, …, Bn all share a secret key k. User A MACs every packet she sends using k. Each user Bi can then verify the MAC. Explain why this scheme is insecure, namely, show that user B1 is not assured that packets he is receiving are from A.

b. Suppose user A has a set S = {k1, …, km} of m secret keys. Each user Bi has some subset Si of the keys. When A transmits a packet she appends m MACs to it by MACing the packet with each of her m keys. When user Bi receives a packet he accepts it as valid only if all MAC's corresponding to keys in Si are valid. What property should the sets S1, …, Sn satisfy so that the attack from part (a) does not apply? We are assuming all users B1, …, Bn are sufficiently far apart so that they cannot collude.

c. Show that when n = 10 (i.e. ten recipients) the broadcaster A need only append 5 MAC's to every packet to satisfy the condition of part (b). Describe the subsets S1, …, S10 of set {k1, …, k5} you would use.

**4. (12 pts)** In the HORS one-time signature (refer to the slide deck of Module 9 for details), let *t*=16, *l*=128, *k*=4, and let H() be a hash function that creates 16-bit long hash values. Suppose a message m’s hash value is 0110 1001 0011 0010. Then what is this message’s signature? How to verify the signature?

**5. (20 pts)** Revise the Onion Routing protocol presented in the slides of Module 11 to have one new protocol that meets two requirements: (i) there are only two relays N1 and N2; (ii) the source Alice doesn’t want N2 know the content of the request m. Give the request sending and data reply process.