CISC 367 – Spring 2016

Homework Assignment – Cryptography

1. What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer.

2. Suppose N people want to communicate with each of N − 1 other people using symmetric key encryption. All communication between any two people, i and j, is visible to all other people in this group of N, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. How many keys are required in this case?

3. (a) Using RSA, choose $p = 3$ and $q = 11$, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. (b) Repeat part (a) but now encrypt "dog" as one message m.

4. Consider RSA with $p = 5$ and $q = 11$.

   (a) What are n and z?

   (b) Let e be 3. Why is this an acceptable choice for e?

   (c) Find d such that $de = 1 \pmod{z}$ and $d < 160$.

   (d) Encrypt the message m=8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. Hint: To simplify the calculations, use the fact:

   $$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

5. Use a *nonce* and **public key cryptography** (public and private key pair) to solve the end-point authentication problem by replacing the symmetric sceret key used in protocol *ap4.0*. Diagram the operations of this protocol, using K_X^+ and K_X^- for public and private keys, respectively, for party X.