MASENO UNIVERSITY

UNIVERSITY EXAMINATIONS 2016/2017

FOURTH YEAR FIRST SEMESTER EXAMINATION FOR DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

MAIN CAMPUS

SCS 436: INTERNAL CONTROLS AND SECURITY ISSUES

Date: 13th December, 2016 Time: 12.00 - 3.00pm

INSTRUCTIONS:

- Answer Question ONE and any other TWO.

Question #1 Compulsory (30 Marks)

a) State and explain each of the three *security goals* [6 Marks]
b) State and explain the three things that an attacker must have to succeed [6 Marks]
c) Explain why both *symmetric cryptography* and *asymmetric cryptography* are both in use [6 Marks]
d) State and explain *Kerckoff's principle* [6 Marks]
e) State the names of any three *cryptographic algorithms* is use [6 Marks]

Question #2

a) What is a *one-way function*? [5 Marks]
b) State all the names used to refer to the output of a *hash function* [6 Marks]
c) State and explain the three *criteria* or *requirements* that a *hash function* must satisfy [9 Marks]

Question #3

a) For each of the terms *diffusion* and *confusion*, define the term and explain its aim. [12 Marks]
b) For each of the components of a modern cipher *P-box* and *S-box*, describe what it does using an example [8 Marks]

Question #4

a) State the *principle of adequate protection* and give an example of where it applies [6 Marks]
b) Explain the following properties of an encryption scheme [14 Marks]
   i) unconditionally secure
   ii) computationally secure

Question #5

The following is an algorithm for creating the decryption key given the encryption key for a transposition cipher. The cipher transforms the plaintext using the idea that the content of the element of the key represents the position in the plaintext and the index of the element of the key is the position in the cipher text.

```
ALGORITHM createDecryptionKey(EncKey[], KeySize)
        index <- 1
        while (index <= KeySize)
                DecKey[EncKey[index]] <- index
                index <- index + 1
        return DecKeyIndex <- 1
```

The following is the ciphertext and the key used to encrypt the original plaintext.

ciphertext: `eemyntaacttkonshitzg`
encryption key: `31452`

REQUIRED:

- Use the algorithm to obtain the key
- Decrypt the ciphertext