Qualifying Exam “Advanced Information Security”
Fall Semester in 2016

Jan. 13th, 2017

Department: Student ID: Name:

Note

i. Answer is fine with Korean or English
ii. Don’t forget to write your Department, Students ID and Name in answer sheet
iii. You can use the answer sheet numbering with each questions like I-1.

I. Fill the blanks (4 points per each question)

1. ( ) is to try all the possible keys in a cryptosystem until finding the correct secret key for a given pair of plaintext and ciphertext.

2. ( ) is an undisclosed vulnerability that hackers can exploit to adversely affect computer applications.

3. DES was designed to have ( ) bit plaintext and ( ) bit key.

4. ( ) is defined to be for a given sequence *s*, the shortest length of LSFR’s that generate *s*.

5. ( ) are the basic three security requirements for a secure system.

II. Explain the concepts of the following terms. (15 points per each question)

1. Describe Golomb's postulates to define the pseudorandomness of a binary sequence. (15 points)

2. Describe the following security requirements and design goals of AES. (15 points)

   - 4 security requirements for AES. (6 points)
   - 6 design goals of Rijndael. (9 points)

3. Sponge Structure of Keccak Hash Function(15 points)

4. Describe how to prove your cryptographic primitive can meet IND-CCA2(15 points)

III. Explain the concept of the following terms. (10 points for each question)

1. Provable security (10 points)

2. Describe the vulnerabilities of smart (connected) car. (10 points)