# Ph.D Qualifying Exam “Advanced Information Security”

Jan. 2016

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

I. Fill the blanks (5 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. AES was designed to have ( ) bit plaintext and ( ) bit key.
3. ( ) means the number of difference between 2 binary strings.
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.

2. Describe the security requirements of AES.

3. Explain the following side channel attacks and their countermeasures. (7.5 points per each)

- Timing Attack

- Power Attack

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

1. Kerckhoff's principle

2. What is the birthday paradox?

3. What were the security requirements for call-for SHA-3.