Ph.D Qualification Test "**Advanced Information Security"**

Jan. 4th, 2013

(i) Answer is fine with Korean or English
(ii) 20 points per each

1. Describe why all the classical ciphers can be broken by Ciphertext Only Attack.

2. Describe the duality of Differential Cryptanalysis and Linear Cryptanalysis.

3. Describe the design background of AES.

4. Describe all the known collision finding methods on hash function.

5. Describe how to prove your cryptographic primitive can meet IND-CCA2.