COURSE PROJECT (Cryptography and Security)

1. Who should work on this course project?

   Everyone taking COMP5631 or CSIT5710 must do this project.

2. What is the project?

   The project is to study the so-called "Identity-Based Encryption" and submit a project report.

3. What should you do in this project?

   Step 1: Read the following paper about identity-based encryption
   J. Baek et al., A survey of identity-based cryptography and other materials in the folder IBE.zip

   Step 2: You should focus on Cocks' IBE algorithm, and may not read other IBE encryption systems if you do not have the necessary background in mathematics.

   Step 3: Compare certificate-based public-key encryption with identity based encryption, and address the following questions in your project report:

   Q1: What is the motivation for proposing the identity-based encryption?

   Q2: What are the advantages and disadvantages of the IBE over the traditional certificate-based public-key encryption?

   Q3: Can an IBE system be used for signing digital documents? If yes, can the digital signature be used for nonrepudiation?

   Q4: Do you think IBE will be widely used? Please justify your conclusion.

4. When should you start working on my project?

   You are ready to work on it after Lecture 9.

5. What are the format and length of your project report?

   There is no length requirement. You may write a three-page or four-page report only addressing the four questions above.

6. What are the date and way for submitting your project report?

   Details will be given to you by email from the instructor at due time.