期中 Assignment

請於 4/20 日 24:00 前決定並寄給我，否則將由我指定

1. 實作(Shamir's) ID-based signature scheme (可最多三人一組)

   (1). System parameter 由系統生成。 n=pxq with two large primes p, q, |p|=|q|=512bits

   (2). User's public key 可由 user 自選

   (3). 系統生成 signing key (secret key) corresponding to the public key

   (4). about the user interface:

   i. 有訊息輸入框及簽名輸出框

   ii. input a public key, a message m and a signature s, it can verify the correctness of the signature

   iii. can sign a file and verify the corresponding signature.

   (5). 課堂上 Demo

2. Presentation

   (1). Digital Watermarking （可最多三人一組，依人數不同深度要求亦會不同）

   i. 用途簡介，原理（理論）介紹，相關軟體介紹等

   (2). ISO27001 (Will be introduced by 曾同學)

   (3). 參加 Info Security 2009 會議並擇一報告(可兩人一組)

   http://www.secutech.com/09/twmain/sem_list.aspx?fm=2&ff=2

   需理解內容並涉獵相關（背景）資料

3. Paper Report （可最多三人一組）

(1). Security proof of RSA-PSS with message recovery (see the paper we have introduced at class)