預習測驗七

姓名：_____ 系級：_____學號：_____ 分數：_____

預習第五章第二及第九節(pages 116-118, 119-123)並回答下列問題

1. RSA指的是哪三位？上網查詢此三人之近況並簡述之

   R是

   S是

   A是

2. RSA演算法的步驟中，先選取二相異大質數p, q並相乘之得$n = pq$;再選取加密次冪e.

   (a) e的限制條件爲

   (b) 明文信息爲$m < n$,則加密爲

   (c) 密文信息爲c,如何解密？

3. RSA公鑰密碼系統至今有幾年的歷史？

4. 何謂RSA-129? Google之!簡述於下