自然：數論與密碼畢業考

姓名：_____ 系級：_____ 學號(序號)：_____ 分數：_____

♣♢♠♡ 注意：下載並獨力完成此次考試，上課時繳交；你必須上課到6/6，交完必須繳的閱讀測驗。 ♣♢♠♡

寫出你缺課的次數(核對用) [ ]

第一部分是非題：在題號左側,對的打○,錯的打**X;**每題**4**分

1. 三毛要傳送信息給四郎，他們沒有事前的接觸，也不希望花時間交信差遞送鑰匙。因此，所有三毛送給四郎的信息都有可能被第三者五爺給攔截。在此種情況之下，三毛是否有可能秘密傳送信息給四郎呢？在所有古典方法中，這是不可能的。

2. 古典密碼術的安全性完全仰賴於鑰匙的秘密性。

3. 古典密碼術最大的致命傷是其加密鑰匙和解密鑰匙是對稱的；也就是說，解密鑰匙很容易就可以從加密鑰匙推導出來，甚至有時候更是單純到解密鑰匙就是加密鑰匙。

4. 歷史學家大衛・坎恩(David Kahn)的破碼者(The Code-breakers)。是第一本詳細探討密碼發展史的書，對初入門的密碼研究者而言，是最佳的入門讀本。

5. 費特費德・迪費不僅提出構想也設計出一套實際可運作的公鑰密碼系統。

6. 之後幾年，陸陸續續有好幾個可執行的方法被提了出來。其中最成功也最有名，根基於分解因數的困難性，由M.I.T.的三位學者Ronald Rivest、 Adi Shamir及Leonard Adleman於1977年5月所提出來的，因而就稱爲RSA演算法。

7. 你若擁有一個單向函數，你要在一份文件上簽名；你就用不公開的(解密)鑰匙拿來完成簽名的動作。任何其他的人，可透過你公開的(加密)鑰匙將其還原成先前的文件，就知道這就是你簽名過的文件。簽過名，但不留一絲痕跡。難以複製的部分彰顯在單向函數的逆方向，而不是字面上複製的意思。

8. RSA演算法的突破誕生在瑞維斯特的腦中，但孕育自他跟沙密爾及葉德曼一年的合作，缺少任何一個人，不會有這項突破。雖然如此，應該只掛上瑞維斯特的名字，可以稱爲瑞維斯特公鑰密碼系統。

9. 令$t \leq w$爲二正整數。所謂的(t,w)-門檻法乃是將信息M分享給w位參與者的一種方法；在此法中，只需其中任何t位就可重建原信息M,若少於t位就無法重建M。

10. RSA密碼系統，是一個定性的(deterministic)系統。一個明文只會產生一個密文，跟加密者完全沒有關係。

第二部分填充題：請將答案寫在空格上，每題**10**分

1. 公鑰密碼系統中最成功也最有名的就是瑞沙葉(RSA)演算法，乃根基於 [ ] 的困難性。在演算法中，公開鑰匙是一對的數(n,e)；其中n是 [ ]，而e是 [ ]。若加密信息是$m < n$，則密文爲$c =$ [ ]。

2. 另一個常用的公鑰密碼系統就是艾爾給默(ElGamal)密碼系統，乃根基於 [ ]

的困難性。在艾爾給默(ElGamal)密碼系統中，公開的鑰匙是一串的數(p, α, β)；其中的p是 [ ]，α是 [ ]，而β是 [ ]。

假設要加密的信息是m，則密文爲$c =$ [ ]。

3. 有一鑰匙分配者使用一沙密爾$(2, 20)$-門檻法來發配一電子保險箱的組合號碼給20位參加者。

(a) 若已知有一不知名的參加者是騙子，其持有的部分是一隨機數對。請問最少需要幾位參與者才能重建此秘密？ [ ]

(b) 如果他們只被允許試一把鑰匙(若錯誤則電子保險箱就永久關閉)，則需要幾位參與者才能開啓這個保險箱？ [ ]

＜注意，這有一些微妙。大多數會選4位，但你需要證明平手不可能發生＞

第三部分計算題：請將答案寫在問題下方，每題**15**分

1. 密文$c = 11915470752366668016 20$乃是RSA演算法加密而成，其公開鑰匙爲

$$n = 5748274425902722853647, \quad e = 971;$$

破解此密碼c。$(a = 00, b = 01, c = 03, \cdots)$

2. 假設在一個房間裡有四個人，其中正好有一個是外國間諜。其他三個人持有對應於一個任何兩個人可決定秘密的沙密爾分享法中的數對。那老外間諜所持有是隨機選出的數對。這些人及數對如下。所有的數都是在模13之下：

$$\text{甲}：(1, 5), \quad \text{乙}：(3, 9), \quad \text{丙}：(5, 7), \quad \text{丁}：(7, 8)。$$

請問老外間諜到底是那一位，而秘密又是什麼？