自然：數論與密碼畢業考

姓名：＿＿＿＿＿＿＿＿ 系級：＿＿＿＿＿ 學號：＿＿＿＿＿＿＿＿＿＿ 分數：＿＿＿＿＿

♣♢♠♡ 寫出你缺課的次數(核對用) [ ] (正確給4分) ♣♢♠♡

第一部分是非題：在題號左側,對的打◯,錯的打**X;**每題**4**分

1. 位移密碼(Shift Ciphers)是最早的密碼系統之一，通常歸功於凱撒大帝，所以又稱之爲凱撒密碼。

2. 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。

3. 古典密碼術的安全性完全仰賴於鑰匙的秘密性。

4. 密碼系統可分爲公鑰密碼系統(非對稱密碼)與私鑰密碼系統(對稱性密碼)。

5. 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。

6. 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。

7. 一個函數$f(x)$稱之爲單向函數(one-way function), 如果函數值$f(x)$是容易並可快速計算的；但給予y,要找滿足$f(x)=y$的x值在計算上是不可行的。

8. 公鑰密碼之構想最關鍵的人物是費特費德・迪費(Whitfield Diffie)。

9. 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。

10. 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。

11. 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。

12. 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。

13. 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。

14. 艾爾給默 (ElGamal) 密碼系統，是一個非定性的 (non-deterministic) 系統。因爲密文不僅僅與明文有關，而且跟加密者所選取的隨機整數 k 有關。所以同一明文就會產生許許多多不同的密文。

第二部分填請將答案寫在空格上，每格**4**分

1. 寫出所有你知道的私鑰密碼系統 [ ]

2. 公鑰密碼系統中最成功也最有名的就是RSA 演算法，

   乃根基於 [ ] 的困難性。

3. 在RSA 演算法中，公開的鑰匙是一對的數 (n, e)；其中的 n 是 [ ]，而

   e 是 [ ]。

   假設要加密的信息是 m，則密文爲 $c =$ [ ]。

4. 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。

5. 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 $c =$ [ ]。