

自然：數論與密碼期中考

系級：_____ 姓名：_____ 學號：_____ 分數：_____

♣♦♠♥ 注意：請將所有的過程詳細寫出來，每小題 10 分；超過 100，以 100 計。 ♣♦♠♥

1. 考慮質數 103。

(a) 試找出整數 x 與 y 使得 $17x + 103y = 1$ 。(b) 試找出 $17^{-1} \pmod{103}$ 。

2. 考慮質數 29。

(a) 解同餘方程式 $5d = 1 \pmod{28}$ 。(b) 假設你將一信息表示成模 29 之下的一個整數 $m \pmod{29}$ 。將明文 m 加密為密文 $c = m^5 \pmod{29}$ 。請問你如何將密文 $c = 21$ 解密？(提示：解密可將密文 c 在模 29 之下取一整次冪來完成。)3. 將 $2^{23590121}$ 除以 101, 餘多少？4. 計算 $\gcd(8765, 23485)$ 。



5. 試找出整數 x 與 y 使得 $65537x + 71101y = 1$ 。

6. 下面密文是由位移密碼器所得：LCLLEWLJAZLNNZMVYIYLHRMHZA 試用頻率分析來猜測此密文所用的鑰匙，並用 MATHEMATICA 來測試你的猜測。請問解密之後的明文為何？

7. 下面密文是由仿射密碼器所得：EDSGICKXHUKLZVEQZVKXWKZUKCVUH
已知明文的最後兩個字是 er。試破解之。

8. 使用仿射函數 $9x + 2 \pmod{26}$ 來加密信息，密文為 UCR, 試找出明文來。

9. 下面密文是由維吉內爾密碼器加密所得，鑰匙是 cipher=(2,8,15,7,4,17)，試破解之。

VPXZGIAXIVWPUBTTMJPWIZITWZT