臺北市立大直高中 107 學年度第 1 學期高一「密碼學」補考試題卷

一年＿＿＿班＿＿＿號 姓名＿＿＿＿＿＿＿＿

※請將此檔案以 A4 雙面列印，並用黑色原子筆作答。每一題都要作答！

※請於 1 月 30 日(三)中午 12 點前交至教務處教學組。逾時不候！

1. 請利用古典加密的方法解密：

   (1) 循路徑換位： IALDHFIETE(密文 C)→＿＿＿＿＿＿＿＿＿＿.(明文 P)

   (2) 凱薩密碼：(金鑰 $3x+1$) HAVUGRTABUWV(密文 C)→＿＿＿＿＿＿＿＿＿＿.(明文 P)

   (3) 維吉尼爾密碼：(密鑰：MATH) OONYEE(密文 C)→＿＿＿＿＿＿＿＿＿＿.(明文 P)

   密碼表：

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

   (4) 請將上面三段明文組合成一句英文，並翻譯之。

   英文：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿.

   中文：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿.

   (5) 請將以下明文用凱薩加密成密文：(密鑰：$5x+a$ ，$a \equiv$ 你的座號 (mod 9))

   There is no royal road to learning. 學無坦途 (明文 P)

   →＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿.(密文 C)

2. 進位轉換：

   (1) 二進位→十進位：$101111001_2 =$ ＿＿＿＿＿＿＿＿$_{10}$

   (2) 十六進位→十進位：$35C_{16} =$ ＿＿＿＿＿＿＿＿$_{10}$

3. 邏輯運算：

(1) 1011 or 1100 = ＿＿＿＿.	(2) 1011 and 1100 = ＿＿＿＿.	(3) 1011 xor 1100 = ＿＿＿＿.

4. 模數運算：

(1) $837 \equiv$ ＿＿＿＿ (mod 5)	(2) $-43 \equiv$ ＿＿＿＿ (mod 3)	(3) $2+9 \equiv$ ＿＿＿＿ (mod 3)
(4) $2-9 \equiv$ ＿＿＿＿ (mod 5)	(5) $2 \times 9 \equiv$ ＿＿＿＿ (mod 7)	(6) $2 \div 9 \equiv$ ＿＿＿＿ (mod 11)

5. 期末回顧：

   (1) 自我反省與檢討：請自己檢討為什麼成績不及格的原因，像是作業缺交、上課不認真、上課態度不佳...等，請確實說明並檢討，若有需要老師協助的部分也請提出。

   (2) 這學期介紹了凱薩加密、DES、AES、RSA，請從這四個主題中選一個主題，詳細說明它的(a)原理、(b)用到哪些數學知識、(c)在生活中的應用。(至少 300 字以上)

   (1)、(2)兩題請書寫在下面格子中，並標明題號，總字數需 600 字以上。