112 學年下學期 資訊安全與密碼學第四次作業

繳交方式：程式碼及書面報告都要。書面報告的內容手寫題請附過程，程式題請說明執行的方式，包含輸入與輸出的格式(請自訂)，報告電子檔請依以下方式命名：「HW04_學號_姓名」。 繳交時間：6/5 下午 5:00 前。遲交一周內 7 折，逾一周不計分。

1. (9%) (Feistel 加密) 假設明文和密文的長度各是 5 位元，而金鑰的長度是 4 位元，令混合器的函數取金鑰的第二和第三位元，將此二位元解釋成十進位的數字，再將該數字平方，以二進位的 5 位元表示結果。如果原始的明文是 10110，而混合器的函數金鑰是 0110，請顯示加密和解密的結果。

2. (15%) (Euler 函數) 令 n 為一正整數，定義 $\phi(n)$ 為小於 n 且與 n 互質的正整數的個數，即：$\phi(n) = \{m \mid 0 < m < n \text{ and } \gcd(m,n) = 1\}$。假設 p 為質數，試證明對任意正整數 k，$\phi(p^k) = p^k - p^{k-1}$。

3. (16%) (Euler 定理) 假設 x 與正整數 n 互質，則 $x^{\phi(n)} \bmod n = 1$。
   (1) 驗證當 $n = 12$、$x = 1$、5、7、11 時，上式的正確性。
   (2) 假設正整數 d 與 $\phi(n)$ 互質，且 e 為模 $\phi(n)$ 下 d 的乘法反元素 (即 $de \bmod \phi(n) = 1$)，試證明對任意整數 $x \in [0, n-1]$，$(x^d)^e \bmod n = x$。

4. (35%) (區塊加密) 在 AES 中，給定一明文 $\{000102030405060708090A0B0C0D0E0F\}$及金鑰 $\{01010101010101010101010101010101\}$，請求出下列初始運算之值。
   (1) 原始狀態(State)為何？(以 4×4 矩陣表示)
   (2) 經過初始 AddRoundKey 後的狀態(State)為何？
   (3) 根據下一頁的表 1，經過 SubBytes 後的狀態(State)為何？
   (4) 經過 ShiftRows 後的狀態(State)為何？
   (5) 經過 MixColumns 後的狀態(State)為何？

表 1：SubBytes 的查表

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*A*	*B*	*C*	*D*	*E*	*F*
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

5. (25%) (質數測試) 請用任何程式語言實作一個質數測試的程式，如果使用者輸入的數字是質數則列出是質數，否則列出不是質數。一個整數要為質數，其必須滿足不可被最小質數 2 至 $n-1$ 的任何數字給整除。請設計防呆機制去限制使用者不得輸入小於 2 的整數，並且在輸出結果是否為質數時，也輸出一共分析了幾次？原則上所需判斷質數的分析次數越少，分數越高，但必須在書面報告裡解釋為何只需要這些分析次數？

   P.S. 分析次數定義為程式中 if (else if) 的次數

   另外實作上有以下限制：

   輸入方式從檔案輸入，且每個測試的數以行區分，而輸出方式是螢幕輸出，可能輸出的情況：

   1. 該數是質數，輸出 PRIME <分析次數>
   2. 該數不是質數，輸出 COMPOSITE
   3. 例外情況，在該行輸出 EXCEPTION

測資範例：

輸入檔案內容

```
2
4
1
17
32
```

輸出 (螢幕內容)

```
PRIME 1
COMPOSITE
EXCEPTION
PRIME 5
COMPOSITE
```