PRNG-CBC 與 AES 資料攪亂效能比較之研究

傅振華　　林彥竹　　陳憲洲

國防大學管理學院資訊管理學系

Email:fchemail@gmail.com　Email:stanley1980.lin@gmail.com　Email:s925014@yahoo.com.tw

摘要

資訊安全的議題一直是身為資訊人員所必須瞭解的重要課題之一，而目前許多資訊安全的攻擊都來自於網路駭客的攻擊，面對其攻擊能力和技術不斷精進且翻新，即使企業組織擁有各類功能完備之防火牆、入侵偵測系統及防毒軟體等防護機制也未必能達到企業組織資訊百分之百的安全，對企業組織而言機敏資料仍有可能透過網路或其他方式被竊取。因此，如何確保機敏資料的機密性對於企業組織而言是一項必需重視的問題，本加密研究的目的在為企業組織提供一實現機敏資訊保密的有效方式。

本研究嘗試比較以鏈鎖式區塊加密技術為基之對稱式加密機制（PRNG-CBC）與現行知名之 AES 演算法進行資料攪亂效能比較，研究將利用「明文資料與密文資料位元變化」、「資料字元 ASCII 內碼偏移量比較」及「密文資料字元 ASCII 碼分佈」等三種比較方式，探究 PRNG-CBC 機密機制與 AES 加密機制資料攪亂效能。

關鍵詞：CBC、PRNG、AES、資料攪亂。

1. 緒論

隨著雲端運算快速發展，我們使用電腦及無遠弗屆的網際網路時，充斥著各種危機及隱憂。反推於企業組織，若無一完整的資料加密系統，將無法確保機敏資料在傳輸過程中的安全，其可能對企業組織造成的安全威脅與衍生之問題實不可等閒視之。

目前對稱式加密的編碼方法可依照其對明文編碼方式不同，區分成「串流加密法」(stream cipher)與「區塊加密法」(block cipher)，串流加密法使用的編碼方式，是一次將明文的一個位元(bit)或是一個位元組(byte)變成密文，而區塊加密法的編碼方式則是將明文分成許多固定大小的區塊，然後對區塊進行編碼成為密文，因此密文區塊的大小通常和明文區塊大小是一致的。

PRNG-CBC 加密機制係依據依使用者輸入的單位代碼、加密密碼及時間戳記等三項參數，並配合區塊加密模式的關聯，由系統提供相關之鏈鎖式變化加密方式，藉此增加破密者之困難度；而 AES 為現行知名的對稱式區塊加密機制，為世界各國所採用，廣泛應用於各類型資料加密作業。本研究嘗試經由三種不同資料攪亂成效分析方式，比較 PRNG-CBC 與 AES 加密機的資料攪亂成效，以做為後續進行資料加密作業處理與相關研究之參考。

2. 文獻探討

2.1 對稱式加密

依上述分類方式得知，我們常以金鑰使用個數來做為依據，假如傳送方及接收方使用相同的金鑰來處理加解密作業，我們可說這方法是對稱的、單一金鑰（single-key）、秘密金鑰（serect-key）或是傳統加密系統；反之傳送及接收雙方各使用不同的金鑰，我們則說這系統是一非對稱的、雙金鑰（two-key）或是公鑰（public-key）加密系統。

2.2 常見對稱式加密機制概述

在各種傳統的加密法中，最常用的則為 DES 與 triple DES(3DES)對稱式加密法，但因 DES 易被暴力攻擊法所破，而 3DES 安全強度雖增強，但若用軟體實作的話，因執行上比 DES 多 3 倍的回合數，所以其效能極差，故在 2001 年美國國家標準與技術研究院進行長達四年的甄選，最後採用 DR.Vincent Rijmen 和 DR.Joan Daemen 兩位比利時籍科學家提出的 Rijndael 演算法，做為高等加密標準(Advanced Encryption Standard, AES) 演算法之標準[2][8]。

相較於 DES 支援 56 位元的密鑰長度，AES 可支援 128、192 及 256 位元的密鑰長度，若駭客破壞 DES 加密所需要的時間為一秒鐘，，那麼他要解開 128 位元之 AES 加密資料將會需 146 萬億年的時間，在資料保密上將顯得更有效[5]。AES 為美國資料加密所採用的標準機制，可有效嚴密保護美國關鍵性的資訊基礎建

設，以及確保人民個人資料及隱私權的保密，並加強政府單位及私人企業中，利用自動提款機、網路購物或電子郵件等，透過電腦進行個人資料及金融交易等資料傳輸的安全性。挑選 AES 做為加密演算法的因素，主要是考量到一種兼具安全性、有效性及適應性高的加密標準。NIST 在 21 世紀為了籌備好此一新的加密演算法，判定下列三項標準，分別是 AES 的安全性、成本、演算法與實作特性[6]，本研究將以此做為所提區塊加密機制設計之考量。

2.3 虛擬亂數產生器

密碼學的應用程式通常是以演算法來產生亂數，而這些演算法都具決定性（deterministic），也因此產生的亂數序列都是非統計上的亂數，但若所用的演算法夠好，所產生的亂數將能通過許多合理的亂數測試。而這類數字也因而稱為「虛擬亂數」(pseudo random number)，這類的演算法也稱為「虛擬亂數產生器」(pseudorandom number generator, PRNG)[6]。

而所謂「虛擬亂數」是藉由某種函數所產生一系列的相對應數值，因具備「隨機性」（Randomness）及「不可預測性」（Unpredictability）兩大特性，故在加密應用上已相當普遍。然當產生一連串的數值時，則必須符合以下兩個要求方能算是具備亂數的屬性：

1.平均分佈（uniform distribution）：每一個數字的出現頻率大致是相同的，在一連串的數字中，數字的分佈必須要平均。

2.獨立性（independence）：在一連串的數字中，每個數字出現的機率不會受到其他數字的影響。

2.4 CBC 模式

在 CBC（Cipher Block Chaining）模式之下，每一個區塊加密之前，必須與前一個區塊的密文做一次 XOR 運算，之後再進行加密。因此，每一個區塊的加密結果都會受到之前所有區塊內容的影響。如此一來，雖然在資訊中可能出現多次相同的明文，都會因為受到前文的影響而產生不同的密文。在 CBC(如圖 1)模式之下，為了加密第一個區塊，必須設定一個初值（Initialization Vector，IV）[7]。

由於在 CBC 模式之下，每一個區塊的加密結果都會受到之前所有區塊內容的影響，相對的，在對密文進行解密還原時，也需要考慮到密文區塊的順序性。

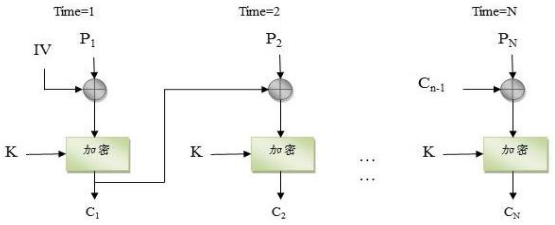


圖 1 CBC 加密模式

3. PRNG-CBC 與 AES 資料攪亂運作說明

本研究將針對以虛擬亂數為基之對稱式鎖鏈式區塊加密機制(PRNG-CBC)與 AES 資料攪亂運作方式做一說明。

3.1 PRNG-CBC 資料攪亂說明

本研究所提 PRNG-CBC 加密機制將依照每位使用者所輸入之單位代碼、加密密碼、與系統產生之時間戳記等三個不同之參數做為亂數種子，將亂數種子輸入 PRNG 後產生虛擬亂數，並依虛擬亂數來動態決定本次加密方法之選定（如：加密功能模組、模組數量、模組順序）；然而同一使用者所輸入之單位代碼、加密密碼等二項會有極大機率相同，因此本研究加入「系統時間戳記」此參數，藉由每次使用者所選擇之機密等級與系統時間戳記交互運算產生之變化方式，避免發生虛擬亂數產生之值完全相同，以確保每次影響加密方法之虛擬亂數會有所不同。

此外本研究採用「對稱式之區塊加密法」，定義加密區塊大小為 16*16 位元組，依此做為明文資料區塊切割之依據；傳統對稱式區塊加密機制於明文資料切割後，將最後所剩不足一個區塊大小之部份，以填充（Padding）空白之方式補足。本研究所提加密機制有別於傳統之區塊切割法，是將最後不足一個區塊大小的資料運用串流加密方式處理，如此可達到「節省運算空間及時間」之優點，例如：一個明文資料區塊大小為 2,000 位元組，經過 16*16 區塊切割後還剩 208 位元組，若以傳統填充空白方式需要再加上 48 位元組方可補足最後一個區塊；但若以本研究所提之機制，則所剩之 208 位元組將以串流加密方式處理，相對節省運算空間及時間。

PRNG-CBC 加密機制作業特性係將目前所處理區塊資料的安全強度植基於前一個區塊資料的正確性，唯有當前一個資料區塊能夠正確地被解密還原為明文，方能藉由前一個資料區塊的正確明文內容進行解密當前此一資

料區塊的內容（如方程式 1 所示），藉以強化資料加解密的安全強度，使得各個資料區塊原本獨立進行加解密運算作業可經由鏈鎖式區塊加密機制的運作，讓各個資料區塊之間的加解密作業產生關聯性，增加資料加解密作業的安全強度。為了能夠達到上述的目的，當某一區塊明文資料完成對稱式加密作業時，此一已經加密的進行區塊密文資料需與此一區塊的前一明文區塊進行 XOR 運算（如方程式 2 所示），然後完成單一區塊的加密作業。

$$P_i = D(P_{i-1} \text{ XOR } C_i) \quad (1)$$

$$C_i = E(P_i) \text{ XOR } P_{i-1} \quad (2)$$

- P = 明文 (Plaintext)
- C = 密文 (Ciphertext)
- E = 加密 (Encryption)
- D = 解密 (Decryption)
- i = 第 i 個區塊

假設今有 1 份資料欲進行鏈鎖式區塊加解密作業，該份資料可區分成 n 個區塊進行加解密作業，則其加解密作業可經由下列方程式表示：

加密作業部份：

$$C_1 = E(P_1) \text{ XOR IV} \quad (3)$$

$$C_2 = E(P_2) \text{ XOR } P_1 \quad (4)$$

$$C_n = E(P_n) \text{ XOR } P_{n-1} \quad (5)$$

解密作業部份：

$$P_1 = D(\text{IV XOR } C_1) \quad (6)$$

$$P_2 = D(P_1 \text{ XOR } C_2) \quad (7)$$

$$P_n = D(P_{n-1} \text{ XOR } C_n) \quad (8)$$

P = 明文 (Plaintext)

C = 密文 (Ciphertext)

E = 加密 (Encryption)

D = 解密 (Decryption)

i = 第 i 個區塊

IV = 初始向量(initial vector)

由上面方程式可以推導：

$$P_n = D(D(\cdots D(D(\text{IV XOR } C_1) \text{ XOR } C_2) \cdots \text{XOR } C_{n-1}) \text{ XOR } C_n) \quad (9)$$

因此，當要正確地解密還原第 n 個區塊明文的內容，必須能夠將之前第 n-1 個區塊的密文正確地還原成明文，而第 n-1 個區塊明文的內容還原則需透過第 n-2 個區塊密文的正確還原，依此類推，藉以形成鏈鎖式區塊加解密作業，以達到強化資料加解密作業安全強度的效果。

舉例來說，一個可以分成 3 個區塊大小的資料，透過鏈鎖式區塊加解密機制進行資料的加解密作業，其加解密作業結果每個明文加密區塊與密文解密區塊表示如下：

明文加密成密文部份：

$C_1 = E(P_1) \text{ XOR IV}$

$C_2 = E(P_2) \text{ XOR } P_1$

$C_3 = E(P_3) \text{ XOR } P_2$

密文解密成明文部份：

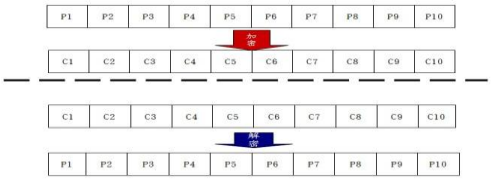
$P_1 = D(\text{IV XOR } C_1)$

$P_2 = D(P_1 \text{ XOR } C_2) =$

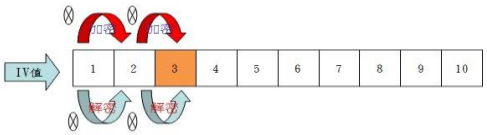
$D(D(\text{IV XOR } C_1) \text{ XOR } C_2)$

$P_3 = D(P_2 \text{ XOR } C_3) =$

$D(D(D(\text{IV XOR } C_1) \text{ XOR } C_2) \text{ XOR } C_3)$



一般區塊加解密機制



鏈鎖式區塊加密機制

圖 2 一般區塊加解密機制與鏈鎖式區塊加密機制比較示意圖

3.2 PRNG-CBC 加、解密功能模組簡介

本研究是依據使用者所輸入之相關參數來決定加、解密功能模組之選取，雖說十一種功能模組之加、解密方式是固定的，但加密流程中每次選定之「功能模組、模組數量、順序」卻會依照使用者所輸入之參數而動態變化，故稱之為「動態」。解密之流程即為加密流程的反向解，只要輸入之相關參數正確，解密核心程式即會依其加密功能模組之反向順序自動解密，加解密作業流程示意圖如圖 3 所示。

加密流程起始於傳送端之使用者輸入加密程式所需之相關參數後，依此產生亂數種子，並將亂數種子輸入 PRNG 後決定加密所需之虛擬亂數，依照虛擬亂數之值來選擇至少五種、至多十一種之不同加密功能模組，再針對已切割之明文資料區塊實施加密處理，各項功能模組分別簡述如下：

- 「一維陣列攪亂運算」功能模組

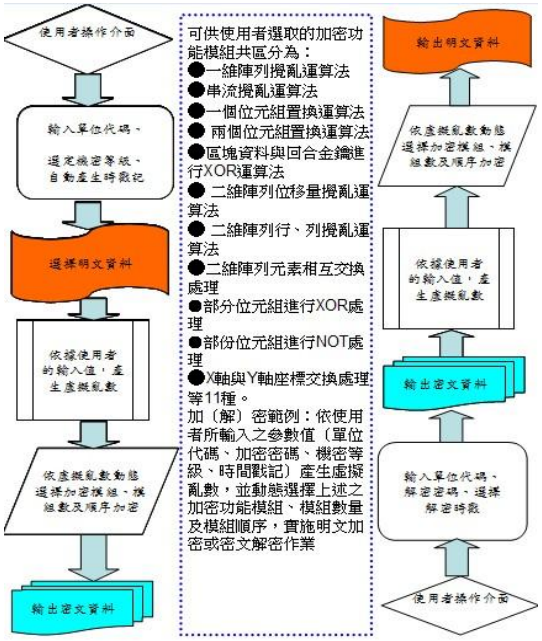


圖 3 加解密作業流程圖

此功能模組之攪亂運算方式為「位置重排」：由使用者輸入相關參數後產生之虛擬亂數，建立 256 位元組之一維陣列，陣列之位置值為 0～255，再依虛擬亂數來重排明文切割後之每個 16 * 16 位元組區塊資料。

● 「二維陣列位移量攪亂運算」功能模組

此功能模組之攪亂運算方式為「位置重排」：運作方式是依序利用「行位移量陣列（向上攪亂）」、「列位移量陣列（向右攪亂）」與「雙對角線位移量陣列（左上右下對角線攪亂及右上左下對角線攪亂）」，運用「位移方向固定」但「位移量變化」之方式來達到資料區塊攪亂之目的，相關位移量之數值大小是虛擬亂數與加密區塊大小經過同餘計算所產生。位移方式計有以下四項：行位移量陣列（向上攪亂）、列位移量陣列（向右攪亂）、雙對角線位移量陣列（左上右下對角線攪亂）、雙對角線位移量陣列（右上左下對角線攪亂）。

● 「二維陣列行、列攪亂運算」功能模組

本模組攪亂運算方式為「位置重排」：此功能模組之運作方式是利用所產生之二維矩陣，先執行整行與整行之位置重排方式，再執行整列與整列之位置重排方式。

● 「串流攪亂運算」功能模組

此功能模組之攪亂運算方式為「內容置換」：藉由擴充單位代碼與密碼字串長度之方式，並運用虛擬亂數與明文區塊進行「一個位元組的攪亂」，本研究使用了 XOR（⊕）、加法（+）及減法（-）等運算等方式，並與 ASCII 碼進行攪亂運算以產生亂碼。此功能模組之解密還原之程序與明文攪亂正好相反，採用「方向不同但變化量相同」之還原方式，攪亂還原之參數必須與加密之攪亂參數相符，方能實施密文區塊之還原[3]。

● 「一個位元組置換運算」功能模組

此功能模組之攪亂運算方式為「位置置換」：本功能模組在對明文資料進行位元組置換前，藉由使用者輸入相關參數產生之虛擬亂數建立一個 16*16 位元組之二維矩陣，此二維矩陣數值內容為 0～255。當 16*16 位元組之二維陣列置換對照表完成後，本功能模組將依據明文中一個位元組的 16 進位 ASCII 內碼做為置換對照表之「行、列註標」，找出明文字元相對應之密文置換內容，進行明文/密文置換工作，如圖 4 所示。

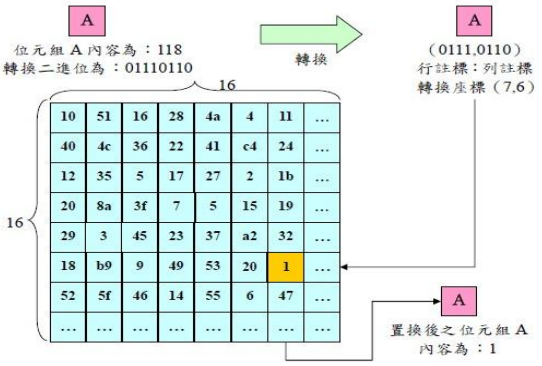


圖 4 一個位元組置換運算示意圖

因其產生之置換對照表內容為 16*16 位元組，因而可採用之置換表內容共有 256！（8.57817775342842654119082271681 23e+506）種方式。

● 「兩個位元組置換運算」功能模組

此功能模組之攪亂運算方式為「位置置換」：所使用之置換表格為一個二維矩陣，內容大小為 256 * 256 位元組，其行與列亦由 256 * 256 位元組所組成，運作方式與「一個位元組置換運算法」相同，差異處在其置換之單位為兩個位元組，置換表之「列註標」為明文第一個位元組之 ASCII 內碼，置換表之「行註標」為明文第二個位元組之 ASCII 內碼，依此找出明文所對應之密文內容進行兩個位元組置換作業，如圖 5 所示[3]。因其產生之置換對照表內容為 256 * 256 位元組，因而可採用之置換表內容共有 65536！（5.16294852309750916500022794327 24e+287193）種方式。

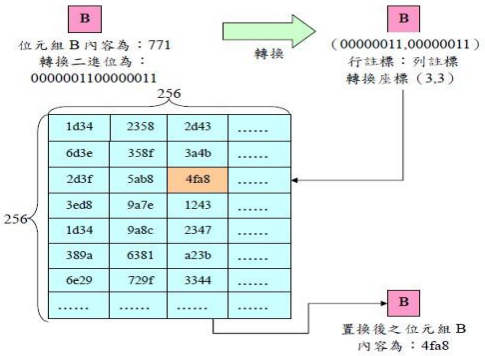


圖 5 兩個位元置換運算示意圖

- 「區塊資料與回合金鑰進行 XOR 運算」功能模組

此功能模組之攪亂運算方式為「內容置換」：本功能模組加密時，會將明文轉成整數後再與虛擬亂數進行 XOR 運算，此運算模組之處理速度快且計算方法簡單為重要特色，此模組加密時將使用回合金鑰對明文資料位元組進行 XOR 運算而成為加密區塊；解密還原作業時，只需將加密區塊與密鑰再進行一次 XOR 運算即可將密文還原[3]。

- 「二維陣列元素相互交換處理」功能模組

此功能模組之攪亂運算方式為「位置重排」：運作方式是依序利用「行位移量陣列（向上攪亂）」、「列位移量陣列（向右攪亂）」與「雙對角線位移量陣列（左上右下對角線攪亂及右上左下對角線攪亂）」，運用「位移方向固定」但「位移量變化」之方式來達到資料區塊攪亂之目的，相關位移量之數值大小是虛擬亂數與加密區塊大小經過同餘計算所產生。

- 「部分位元組進行 XOR 處理」功能模組

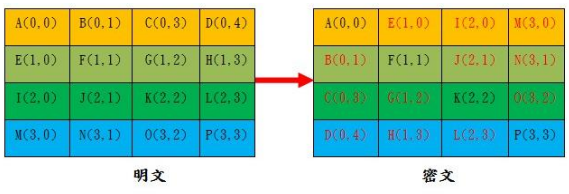
運用隨機方式選部分取位元組實施 XOR。

- 「部分位元組進行 NOT 處理 」功能模組

運用隨機方式選部分取位元組實施 NOT 處理。

- 「X 軸與 Y 軸座標交換處理 」功能模組

如果固定[A(0,0),F(1,1),K(2,2),P(3,3)]這一對角線，然後分別將位對角線兩邊 位移量實施對換，對換後情形如圖 6 所示。



明文二維區塊陣列轉換為密文二維區塊陣列

圖 6 X 軸與 Y 軸座標交換處理

3.3 AES 加密法

AES 是一種非 Feistel 加密法。也就是說，每個回合中的運算都必須是可逆的[1]，運作模式如圖 7 所示，在每回合中執行 4 種運算，其功能分述如下：

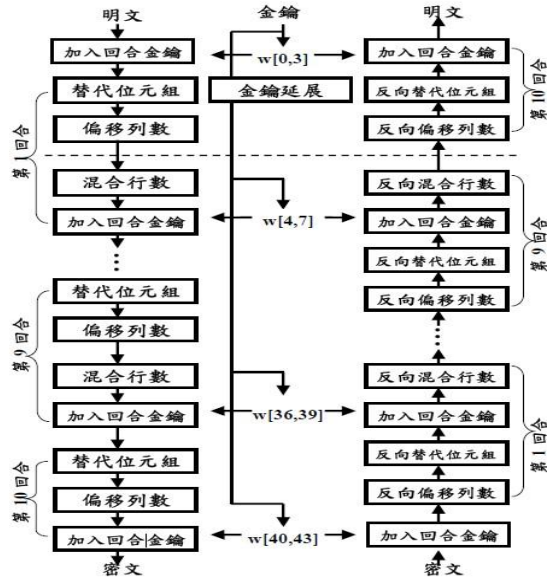


圖 7 AES 之加、解密架構圖

一、替代位元組（Sub Bytes）階段：如圖 8 所示這是一種簡單的查表法，AES 定　義一個 16*16 的位元組矩陣，稱為 S-box，此矩陣包含所有 8 位元的數值，而對映的方法為每位元組的前 4 個位元形成列的編號，後 4 個位元形成行的編號，這組行和列即為 S-box 的索引，用來挑出替代之位元組[6]。

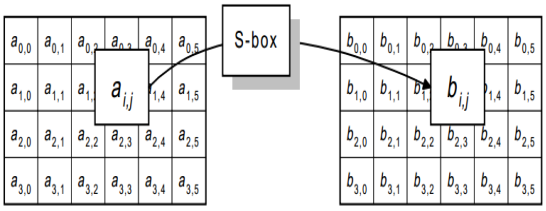


圖 8 位元替代階段示意(資料來源: V. Rijmen, J. Daemen, 1999)

二、位移列（ShiftRows）：如圖 9 所示區塊中第一列並未改變，第 2 列的每個元素向左位移 1 個位元組，第 3 列的每個元素向左位移 2 個

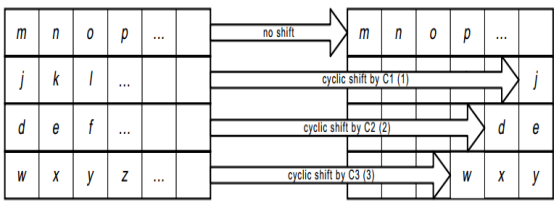


圖 9 位移列階段示意圖(資料來源: V. Rijmen, J. Daemen, 1999)

位元組，第 4 列的每個元素向左位移 3 個位元組[6]。

三、混合行（MixColumns）：一種替代的動作，會依據行裡所有位元形成一函數，用以替代行裡的每一位元[6]，如圖 10 所示。

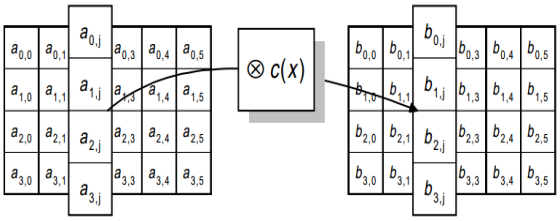


圖 10 混合行階段示意圖(資料來源: V. Rijmen, J. Daemen, 1999)

四、增加回合金鑰（AddRoundKey）：一完整的區塊和回合金鑰的 128 位元進行逐一位元的 XOR 運算[6]，如圖 11 所示。

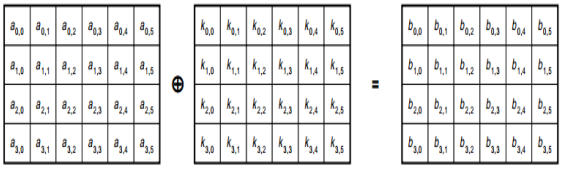


圖 11 增加回合金鑰階段示意圖(資料來源: V. Rijmen, J. Daemen, 1999)

4. 資料攪亂效能分析

本研究依據 PRNG-CBC 加密機制及 AES 加密機制資料攪亂運作模式，分別透過 C 程式語言建立雛型加密程式，藉以針對明文資料進行加密作業，進而獲得此二種加密機制所產生的密文資料，做為後續資料攪亂效能分析比較的資料來源。本研究將利用「明文資料與密文資料位元變化」、「資料字元 ASCII 內碼偏移量比較」及「密文資料字元 ASCII 碼分佈」三種比較分析方法進行資料攪亂效能分析。

4.1 資料攪亂方法說明

本研究將利用「明文資料與密文資料位元變化」、「資料字元 ASCII 內碼偏移量比較」及「密文資料字元 ASCII 碼分佈」三種比較分析方法進行資料攪亂效能分析，此三種比較分析方法說明如下。

- 明文資料與密文資料位元變化

  此一方法係統計經加密後密文資料與原先明文資料間的位元變化情形，以每個位元組做為比較單位，分別統計每個加密區塊中每個資料位元組內各個（1~8）位元的變化情形，最後彙整統計出整個明／密文檔案中每個位元組 1~8 位元的變化情形；藉以瞭解以位元為單位，不同加密機制對於明文資料攪亂的情形，做為分析比較明／密文資料攪亂效能的依據。

  明／密文資料每個位元組內各個（1~8）位元的變化分析係以一個位元組為比較單位，將明文資料與密文資料逐一進行比對，以知曉每個位元組中各個（1~8）位元的變化；每個位元組中特定位元變化判斷依據為當明文資料中資料位元組特定位元值改變（即由０變成１或是由１變成０）。

  通常，明／密文相對應資料中每個位元組中各個（1~8）位元的變化越平均，代表經該加密機制加密過後的密文資料越難被破解，加密機制具備較佳的加密功能。

- 資料字元 ASCII 內碼偏移量比較

  此一方法係比較密文資料與原先的明文資料間的各個位元組 ASCII 內碼值改變的情形，研究利用下列運算式計算出明／密文 ASCII 內碼偏移量：

  資料字元 ASCII 內碼偏移量＝ (10)

  明文資料字元 ASCII 內碼數值－

  密文資料字元 ASCII 內碼數值

  一般而言，資料字元 ASCII 內碼偏移量分布越分散代表加密機制攪亂明文資料的效果越好。

- 密文資料字元 ASCII 碼分佈

  此一方法係統計密文資料中所有 0~255ASCII 內碼的數量，以知曉密文資料中所有字元的分布情形，藉以進一步瞭解明文資料經加密機制資料攪亂的分散狀況；通常而言，密文資料 ASCII 內碼分布越平均，密文資料被破解的機率越低，其意味著加密機制的功能強健性。

4.2 資料攪亂效能比較

分析結果如下，其相關統計資料表請參照附錄 A、B、C：

一、加密內容驗證

為求驗證經解密系統還原之明文檔資料（1KB.TXT.R）與原始明文檔資料（1KB.TXT）是否完全相同，本研究透過 comp 指令（DOS 視窗模式下用來比較兩個檔案或兩組檔案的內容指令）進行「1KB.TXT.R」與「1KB.TXT」兩個檔案之比較，指令為：comp 100KB.TXT.R 100KB.TXT /D /A /L 經比較之結果為「檔案比較無誤」（如圖 12 所示），因此，更可確保原始之明文資料檔案，經本研究之加、解密機制

予以加密攪亂、解密還原之檔案內容將完全相符，且加密後的攪亂情形較 AES 加密法更具不可預測性性及隨機性，攪亂情形如圖 13。

圖 12 利用 comp 指令比較明文原始檔案及密文還原檔案的結果

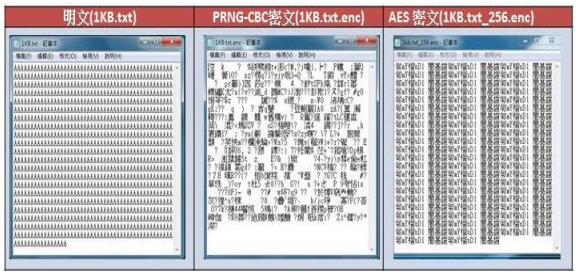


圖 13 PRNG-CBC 與 AES 攪亂結果比較

二、明文資料與密文資料位元變化比較

選擇一資料大小為 26112 位元組的檔案(test.doc)，以一個位元組(8 bits)為計算單位，針對每個位元在加密過程中攪亂的次數做累加計算，詳細比較數據如附錄 A，統計情形如圖 14 所示。

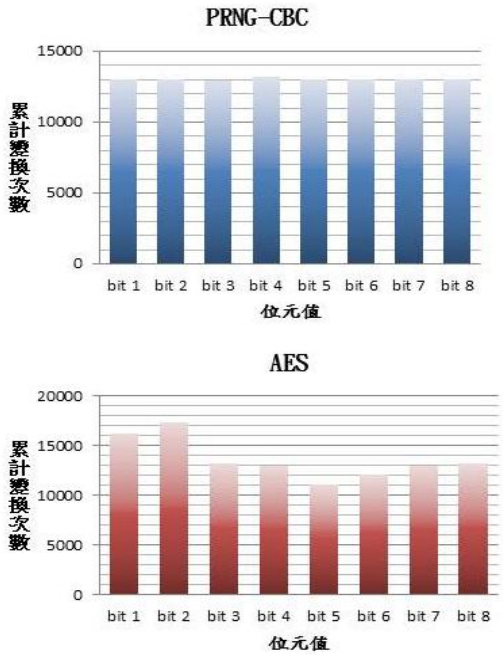


圖 14 PRNG-CBC 與 AES 資料位元攪亂次數統計

三、資料字元 ASCII 內碼偏移量比較

利用 C 程式語言撰寫一程式，進行明文資料字元 ASCII 內碼與密文資料字元 ASCII 內碼的比較，藉以產生明文及密文資料字元 ASCII 內碼的偏移數值，詳細比較數據如附錄 B，統計結果如圖 15 所示。

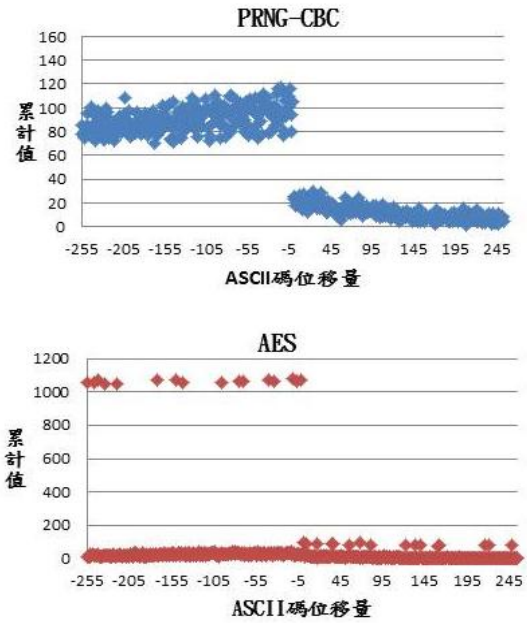


圖 15 PRNG-CBC 與 AES 明文及密文資料字元 ASCII 內碼的偏移數值統計

四、密文資料字元 ASCII 碼分佈

針對加密後的密文資料，統計其資料字元 ASCII 內碼的分佈情形，詳細比較數據如附錄 C，統計結果如圖 16 所示。

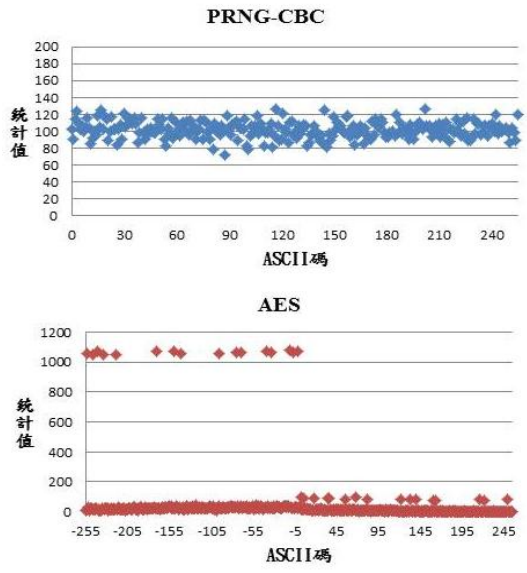


圖 16 PRNG-CBC 與 AES 密文資料字元 ASCII 內碼分佈

4.3 分析比較總結說明

從上述的比較分析圖中可知，本研究針對明文資料中相同且重覆的字元，在加密後的密文資料中，均更換為不同的亂碼，相較於 AES 加密後的密文資料，更具不規則性及隨機性，

大幅增加檔案判讀的困難度。

另分別利用 PRNG-CBC 加密機制及 AES 加密機制對內容不同且不具重複性的明文資料檔進行加密作業，然後利用研究所提三種比較分析方法進行資料攪亂效能分析，分析結果發現：

就每一個明／密文資料位元變化比較而言，PRNG-CBC 及 AES 加密機制所產生密文資料中每個位元組的 1~8 位元變化相對平均，沒有特定的位元變化特別高或是低；然進一步比較此二機制的位元變化數值，PRNG-CBC 機制 1~8 位元變化數值較 AES 機制平均，PRNG-CBC 機制於明／密文資料位元變化比較優於 AES 機制。

在比較資料字元 ASCII 內碼偏移量方面，PRNG-CBC 機制的 ASCII 內碼偏移量分布較為平均，相對地，AES 機制的 ASCII 內碼偏移量分布較為集中，且有部分的 ASCII 內碼偏移量的累計次數相對較高，故在比較資料字元 ASCII 內碼偏移量方面，PRNG-CBC 機制優於 AES 機制。

在統計密文資料字元 ASCII 內碼分佈方面，PRNG-CBC 機制的密文資料字元 ASCII 內碼分佈較為平均，相對地，AES 機制的密文資料字元 ASCII 內碼分佈不如 PRNG-CBC 機制的密文資料字元 ASCII 內碼分佈，其密文資料字元 ASCII 內碼有集中於部分 ASCII 內碼情形。

縱觀上述分析比較說明，可以發現 PRNG-CBC 加密機制資料攪亂效能優於 AES 加密機制，其意味著 PRNG-CBC 加密機制具有較佳的資料攪亂的安全強健性。

5. 結論

本研究主要嘗試比較 PRNG-CBC 加密機制及 AES 加密機制資料攪亂效能，研究分別利用三種明／密文資料比較分析方法：「明文資料與密文資料位元變化」、「資料字元 ASCII 內碼偏移量比較」及「密文資料字元 ASCII 碼分佈」，進行資料攪亂效能分析。

研究分別利用 PRNG-CBC 加密機制及 AES 加密機制對明文資料檔進行加密，產生密文資料檔，經由檢視比較密文內容，然後利用前述三種方法進行資料攪亂效能分析比較；可以發現下列結果：

- 當明文資料為相同且重覆的字元時，檢視經 PRNG-CBC 與 AES 加密機制加密後的密文資料中，此二機制產生不具可讀性的密文內容，然進一步比較相較其密文內容，發現經 AES 機密加密後的密文內容出現規則性的重複現象，相對地，PRNG-CBC 機制所產生的密文內容則無此一現象，其密文資料更具不規則性及隨機性。
- PRNG-CBC 及 AES 加密機制所產生密文資料中每個位元組的 1~8 位元變化相對平均，但 PRNG-CBC 機制 1~8 位元變化數值較 AES 機制平均，就每一個明／密文資料位元變化比較而言，PRNG-CBC 機制優於 AES 機制。
- PRNG-CBC 機制的 ASCII 內碼偏移量分布較 AES 機制的 ASCII 內碼偏移量為平均，在比較資料字元 ASCII 內碼偏移量方面，PRNG-CBC 機制優於 AES 機制。
- PRNG-CBC 機制的密文資料字元 ASCII 內碼分佈較 AES 機制為平均，在統計密文資料字元 ASCII 內碼分佈方面，PRNG-CBC 機制優於 AES 機制。

參考文獻

[1]李南逸等譯，Behrouz A. Forouzan 原著，網路安全與密碼學概論，美商麥羅格.希爾國際股份有限公司，2008。

[2]林祝興、葉義雄、楊國鴻， Rijndael 加密演算法的介紹，資訊安全通訊，第六卷第四期，2000。

[3]陳易佑，以虛擬亂數為基動態變化方式之對稱式區塊加密機制研究，國防大學碩士論文，2010。

[4]陳憲洲，應用動態虛擬亂數於鏈鎖式對稱式區塊加密機制之研究，國防大學碩士論文，2011。

[5]楊政穎譯，Atul Kahate 原著，網路安全與密碼學，美商麥羅格.希爾國際股份有限公司，2007。

[6]賴榮樞譯，William Stallings 原著，密碼學與網路安全，第四版，開發圖書有限公司，2007。

[7]賴榮樞譯，William Stallings 原著，2009，網路安全精要應用與標準第四版，香港，培生教育出版亞洲股份有限公司。

[8]Jagannath Pisharath, “Linear Congruential Number Generators”, NewerMath, Fall 2003, pp.1~10, 2003.

附錄 A

明文資料與密文資料位元變化統計表

PRNG-CBC									AES								
Block	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8	Block	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8
0	136	117	126	127	122	123	134	117	0	115	119	115	100	113	118	103	119
1	130	131	129	128	125	129	134	131	1	112	112	112	80	112	112	96	112
2	127	115	129	117	140	136	127	120	2	138	128	127	128	136	126	126	134
3	132	124	129	129	138	122	135	130	3	113	123	111	125	123	137	130	136
4	124	133	135	121	135	131	133	118	4	131	126	136	134	125	115	117	141
5	126	121	138	124	120	124	123	125	5	149	156	115	126	113	123	131	129
6	117	108	118	138	120	138	123	122	6	136	146	121	130	122	120	127	130
7	131	120	120	125	135	139	136	129	7	148	157	121	122	108	106	123	112
8	119	119	125	136	127	126	146	129	8	176	192	128	128	96	112	128	128
9	133	121	122	127	137	117	135	131	9	176	192	128	128	96	112	128	128
10	135	129	130	133	117	140	121	128	10	139	134	138	117	115	133	121	125
11	123	126	125	140	126	132	125	122	11	129	129	136	126	133	126	121	126
12	124	116	139	131	130	123	129	126	12	140	123	133	146	126	122	127	125
13	136	124	125	128	121	125	118	136	13	136	137	129	128	125	124	127	127
14	141	137	143	137	129	121	129	129	14	107	131	126	126	115	122	118	129
15	132	152	128	119	128	132	122	120	15	129	133	125	132	122	114	123	125
16	128	131	130	146	143	112	127	125	16	157	178	121	124	100	126	123	132
17	121	120	119	122	134	135	127	127	17	159	170	138	139	107	115	126	132
18	133	123	114	129	128	132	132	122	18	128	130	118	127	139	118	111	135
19	122	126	126	131	128	123	141	125	19	163	183	135	124	102	115	126	126
20	133	119	117	133	135	117	135	129	20	171	189	130	127	95	113	121	128
21	139	135	127	111	126	117	128	141	21	173	188	130	130	99	114	131	130
22	111	133	122	123	128	143	130	124	22	131	125	130	127	122	144	127	134
23	134	129	137	118	135	119	125	133	23	120	139	135	123	137	120	136	127
24	131	132	139	122	125	133	132	137	24	120	136	120	125	130	122	131	126
25	125	130	142	142	139	127	136	136	25	170	184	128	128	96	116	128	130
26	137	122	137	139	126	140	120	124	26	160	178	131	133	106	114	130	134
27	116	135	130	123	118	129	123	117	27	176	192	128	128	96	112	128	128
28	132	131	132	128	129	123	144	126	28	176	192	128	128	96	112	128	128
29	133	139	124	131	115	120	131	124	29	176	192	128	128	96	112	128	128
30	118	122	135	128	120	134	137	130	30	176	192	128	128	96	112	128	128
31	121	128	131	121	127	128	140	123	31	176	192	128	128	96	112	128	128
32	120	118	122	124	132	130	144	124	32	176	192	128	128	96	112	128	128
33	145	132	128	125	139	135	132	139	33	176	192	128	128	96	112	128	128
34	132	122	128	124	120	111	134	142	34	176	192	128	128	96	112	128	128
35	118	142	120	129	132	136	132	139	35	176	192	128	128	96	112	128	128

明文資料與密文資料位元變化統計表(續)

PRNG-CBC									AES								
Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1
36	128	134	131	133	137	136	122	137	36	176	192	128	128	96	112	128	128
37	136	134	119	130	128	143	116	121	37	176	192	128	128	96	112	128	128
38	128	138	129	115	119	122	134	129	38	176	192	128	128	96	112	128	128
39	131	136	125	134	130	129	113	134	39	176	192	128	128	96	112	128	128
40	121	124	123	127	113	120	119	116	40	176	192	128	128	96	112	128	128
41	123	140	123	125	131	117	125	123	41	176	192	128	128	96	112	128	128
42	124	116	120	131	140	137	123	139	42	176	192	128	128	96	112	128	128
43	138	129	118	117	134	150	108	124	43	176	192	128	128	96	112	128	128
44	111	139	127	135	111	103	136	141	44	165	187	131	129	99	116	126	124
45	115	126	124	127	134	135	117	117	45	176	192	128	128	96	112	128	128
46	140	127	112	141	141	135	131	109	46	153	149	121	126	122	121	126	121
47	128	119	132	133	127	118	119	122	47	130	138	133	115	137	126	111	123
48	121	123	112	129	133	121	126	141	48	123	123	131	141	124	124	134	148
49	133	123	127	129	120	131	114	139	49	127	135	120	125	122	107	132	142
50	123	133	138	136	124	123	137	132	50	139	127	131	127	134	153	123	132
51	132	138	133	123	119	119	129	127	51	148	131	149	124	135	124	126	125
52	132	133	130	127	122	138	141	140	52	137	134	130	138	126	125	144	123
53	119	121	119	127	136	123	140	118	53	140	141	117	125	138	131	127	134
54	141	125	118	121	129	119	127	115	54	139	133	116	134	136	131	134	132
55	137	131	131	131	124	119	126	127	55	137	148	141	126	118	121	128	126
56	138	135	138	130	133	150	129	130	56	145	155	129	119	123	119	124	128
57	134	127	126	137	126	147	126	110	57	160	173	128	134	114	118	127	124
58	134	121	122	126	140	131	134	148	58	176	192	128	128	96	112	128	128
59	108	137	122	126	116	125	123	124	59	176	192	128	128	96	112	128	128
60	124	122	134	120	143	112	122	133	60	126	124	118	141	134	121	134	120
61	122	134	129	125	126	127	111	115	61	146	155	121	130	111	127	119	132
62	142	128	136	142	140	129	125	129	62	176	192	128	128	96	112	128	128
63	137	135	132	138	128	137	122	138	63	176	192	128	128	96	112	128	128
64	128	133	132	132	128	128	123	127	64	176	192	128	128	96	112	128	128
65	123	131	127	131	130	132	135	133	65	176	192	128	128	96	112	128	128
66	130	145	130	143	122	110	121	135	66	176	192	128	128	96	112	128	128
67	139	142	131	135	125	133	110	133	67	176	192	128	128	96	112	128	128
68	131	141	133	117	132	124	117	119	68	176	192	128	128	96	112	128	128
69	136	108	127	134	124	138	128	136	69	176	192	128	128	96	112	128	128
70	121	120	122	115	112	123	110	133	70	176	192	128	128	96	112	128	128
71	135	131	133	138	131	125	138	130	71	176	192	128	128	96	112	128	128
72	124	132	133	117	117	118	147	133	72	176	192	128	128	96	112	128	128
73	128	129	132	128	141	136	122	120	73	176	192	128	128	96	112	128	128

明文資料與密文資料位元變化統計表(續)

PRNG-CBC									AES								
Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1	Block	bit 1
74	127	131	121	124	131	120	127	144	74	176	192	128	128	96	112	128	128
75	133	119	126	134	132	117	127	123	75	176	192	128	128	96	112	128	128
76	125	136	117	129	136	121	143	131	76	136	134	129	141	132	133	124	125
77	124	126	123	131	131	130	133	127	77	176	192	128	128	96	112	128	128
78	119	118	129	122	137	124	120	129	78	176	192	128	128	96	112	128	128
79	129	131	127	124	135	134	113	137	79	176	192	128	128	96	112	128	128
80	137	112	122	111	128	123	119	122	80	176	192	128	128	96	112	128	128
81	119	129	128	119	124	135	119	132	81	176	192	128	128	96	112	128	128
82	132	128	123	123	135	121	129	127	82	176	192	128	128	96	112	128	128
83	115	121	127	125	128	139	132	124	83	176	192	128	128	96	112	128	128
84	119	123	123	120	120	141	119	127	84	176	192	128	128	96	112	128	128
85	138	117	113	139	111	125	129	125	85	176	192	128	128	96	112	128	128
86	132	129	128	125	132	130	140	124	86	176	192	128	128	96	112	128	128
87	133	133	122	117	121	126	126	125	87	176	192	128	128	96	112	128	128
88	125	133	141	136	125	128	123	121	88	176	192	128	128	96	112	128	128
89	132	134	126	127	128	129	138	120	89	176	192	128	128	96	112	128	128
90	111	125	134	132	128	114	137	121	90	176	192	128	128	96	112	128	128
91	126	117	121	144	127	122	118	120	91	176	192	128	128	96	112	128	128
92	128	136	126	143	117	133	145	116	92	130	123	130	116	132	130	121	124
93	127	126	122	145	126	124	115	123	93	112	112	112	80	112	112	96	112
94	120	132	125	125	115	139	144	133	94	143	150	126	123	109	115	133	118
95	126	130	120	129	125	124	126	116	95	148	155	133	122	121	113	124	127
96	110	118	127	152	117	118	129	129	96	142	158	124	126	115	111	123	116
97	124	129	122	119	114	140	119	119	97	167	171	129	126	97	110	131	126
98	124	127	114	131	135	115	137	142	98	110	113	114	83	115	115	96	114
99	133	123	132	140	125	139	125	125	99	112	112	112	80	112	112	96	112
100	131	140	122	143	132	107	128	128	100	153	168	142	135	112	111	123	129
101	115	123	134	131	118	130	130	113	101	176	192	128	128	96	112	128	128
									102	12	13	8	9	7	7	9	9

附錄 B

資料字元 ASCII 內碼偏移量統計表

ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數
-255	86	8	**-127**	90	24	**1**	25	35	**129**	9	4
-254	78	1060	**-126**	101	22	**2**	23	99	**130**	10	6
-253	78	15	**-125**	97	20	**3**	24	17	**131**	8	4
-252	80	28	**-124**	86	30	**4**	18	13	**132**	6	4
-251	75	12	**-123**	89	46	**5**	23	92	**133**	12	80
-250	82	19	**-122**	92	24	**6**	19	17	**134**	10	7
-249	95	23	**-121**	108	23	**7**	22	20	**135**	10	3
-248	85	26	**-120**	89	24	**8**	26	16	**136**	12	7
-247	80	16	**-119**	82	31	**9**	22	13	**137**	8	7
-246	80	1054	**-118**	105	23	**10**	17	20	**138**	13	2
-245	82	18	**-117**	96	24	**11**	23	14	**139**	11	0
-244	76	20	**-116**	83	33	**12**	14	15	**140**	9	81
-243	101	19	**-115**	76	33	**13**	27	14	**141**	8	6
-242	83	26	**-114**	99	20	**14**	19	18	**142**	9	5
-241	95	1072	**-113**	90	26	**15**	18	12	**143**	11	5
-240	86	10	**-112**	97	26	**16**	22	10	**144**	5	1
-239	88	13	**-111**	85	24	**17**	22	7	**145**	7	3
-238	72	11	**-110**	84	26	**18**	12	92	**146**	11	5
-237	83	12	**-109**	96	24	**19**	19	12	**147**	11	2
-236	98	21	**-108**	98	31	**20**	19	14	**148**	6	2
-235	80	18	**-107**	94	32	**21**	25	15	**149**	11	5
-234	92	1048	**-106**	107	35	**22**	16	16	**150**	6	3
-233	87	23	**-105**	97	34	**23**	20	9	**151**	4	9
-232	93	17	**-104**	99	27	**24**	30	13	**152**	8	6
-231	76	20	**-103**	100	40	**25**	26	15	**153**	15	7
-230	94	21	**-102**	83	27	**26**	23	22	**154**	5	2
-229	85	20	**-101**	72	18	**27**	22	12	**155**	6	3
-228	73	8	**-100**	77	20	**28**	20	17	**156**	9	2
-227	73	19	**-99**	99	25	**29**	15	10	**157**	6	2
-226	100	15	**-98**	101	12	**30**	16	8	**158**	8	5
-225	85	25	**-97**	95	30	**31**	19	15	**159**	4	4
-224	96	16	**-96**	94	36	**32**	15	10	**160**	9	77
-223	74	18	**-95**	88	1059	**33**	18	12	**161**	10	5
-222	91	21	**-94**	111	24	**34**	29	8	**162**	7	1
-221	79	13	**-93**	92	24	**35**	19	89	**163**	8	79
-220	89	18	**-92**	94	27	**36**	16	90	**164**	8	1
-219	78	1047	**-91**	89	30	**37**	22	17	**165**	7	5
-218	81	19	**-90**	105	29	**38**	20	8	**166**	9	2
-217	85	18	**-89**	100	26	**39**	20	10	**167**	6	3
-216	72	28	**-88**	75	26	**40**	12	12	**168**	7	4
-215	78	20	**-87**	86	24	**41**	12	13	**169**	8	7
-214	84	18	**-86**	99	34	**42**	22	10	**170**	8	2
-213	79	15	**-85**	94	24	**43**	12	8	**171**	3	4
-212	84	19	**-84**	96	30	**44**	16	13	**172**	2	9
-211	80	18	**-83**	102	32	**45**	18	12	**173**	14	3
-210	93	22	**-82**	85	41	**46**	19	14	**174**	8	2
-209	92	23	**-81**	76	33	**47**	20	17	**175**	5	1
-208	82	9	**-80**	97	41	**48**	19	12	**176**	8	4
-207	79	16	**-79**	82	28	**49**	14	14	**177**	6	4
-206	82	19	**-78**	97	31	**50**	16	12	**178**	11	1
-205	94	15	**-77**	94	32	**51**	18	7	**179**	9	3
-204	85	24	**-76**	110	33	**52**	13	10	**180**	10	6
-203	89	25	**-75**	80	1067	**53**	13	14	**181**	7	0

資料字元 ASCII 內碼偏移量統計表(續)

ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數
-202	108	21	**-74**	111	36	**54**	9	9	**182**	7	4
-201	80	15	**-73**	91	30	**55**	14	83	**183**	10	3
-200	90	27	**-72**	98	24	**56**	14	18	**184**	10	6
-199	86	18	**-71**	90	31	**57**	12	8	**185**	8	3
-198	98	34	**-70**	107	1066	**58**	10	12	**186**	6	1
-197	82	32	**-69**	85	36	**59**	6	13	**187**	8	8
-196	76	29	**-68**	102	21	**60**	15	12	**188**	5	3
-195	83	16	**-67**	99	30	**61**	16	13	**189**	6	2
-194	82	17	**-66**	103	30	**62**	11	12	**190**	5	3
-193	78	22	**-65**	102	28	**63**	13	10	**191**	11	0
-192	87	11	**-64**	104	28	**64**	24	13	**192**	6	1
-191	80	20	**-63**	97	23	**65**	20	13	**193**	5	3
-190	88	31	**-62**	85	36	**66**	14	15	**194**	8	3
-189	79	27	**-61**	92	25	**67**	12	11	**195**	12	3
-188	96	28	**-60**	101	22	**68**	12	95	**196**	9	0
-187	84	13	**-59**	90	30	**69**	21	7	**197**	10	4
-186	94	14	**-58**	80	26	**70**	11	9	**198**	6	5
-185	80	14	**-57**	105	32	**71**	15	13	**199**	4	1
-184	81	28	**-56**	96	36	**72**	15	4	**200**	5	2
-183	78	22	**-55**	85	33	**73**	12	11	**201**	8	2
-182	84	20	**-54**	77	17	**74**	16	11	**202**	7	2
-181	87	19	**-53**	84	28	**75**	15	12	**203**	11	2
-180	80	24	**-52**	107	45	**76**	12	8	**204**	7	0
-179	87	21	**-51**	104	25	**77**	16	8	**205**	6	0
-178	95	23	**-50**	102	29	**78**	22	8	**206**	15	4
-177	92	25	**-49**	98	38	**79**	24	11	**207**	6	2
-176	77	23	**-48**	81	20	**80**	13	13	**208**	9	2
-175	85	23	**-47**	96	27	**81**	12	11	**209**	4	5
-174	93	26	**-46**	95	36	**82**	13	80	**210**	1	2
-173	89	30	**-45**	108	33	**83**	14	7	**211**	9	4
-172	92	-28.0702	**-44**	86	29	**84**	9	8	**212**	4	2
-171	82	-30.6981	**-43**	96	18	**85**	18	4	**213**	12	3
-170	81	20	**-42**	75	24	**86**	12	12	**214**	5	4
-169	86	25	**-41**	97	27	**87**	13	7	**215**	9	4
-168	97	26	**-40**	107	32	**88**	15	10	**216**	8	81
-167	70	26	**-39**	89	1075	**89**	18	6	**217**	8	0
-166	84	17	**-38**	78	26	**90**	12	7	**218**	11	3
-165	90	23	**-37**	99	35	**91**	12	11	**219**	6	3
-164	77	27	**-36**	112	32	**92**	14	6	**220**	12	3
-163	90	33	**-35**	98	20	**93**	13	8	**221**	8	78
-162	79	26	**-34**	107	33	**94**	13	6	**222**	4	2
-161	90	23	**-33**	104	1063	**95**	14	11	**223**	14	1
-160	92	28	**-32**	102	26	**96**	16	9	**224**	5	1
-159	81	28	**-31**	97	27	**97**	16	17	**225**	9	3
-158	102	23	**-30**	108	36	**98**	18	5	**226**	6	0
-157	94	30	**-29**	79	24	**99**	14	6	**227**	11	3
-156	90	29	**-28**	101	31	**100**	9	10	**228**	4	1
-155	83	37	**-27**	96	35	**101**	18	8	**229**	3	2
-154	93	28	**-26**	80	35	**102**	11	2	**230**	6	3
-153	92	37	**-25**	92	28	**103**	11	13	**231**	7	0
-152	101	22	**-24**	94	31	**104**	11	9	**232**	3	2
-151	92	27	**-23**	102	28	**105**	16	5	**233**	4	5
-150	103	1070	**-22**	96	21	**106**	8	4	**234**	9	0

資料字元 ASCII 內碼偏移量統計表(續)

ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數
-149	87	23	**-21**	85	26	**107**	10	6	**235**	7	0
-148	73	25	**-20**	101	29	**108**	19	5	**236**	9	2
-147	85	38	**-19**	112	31	**109**	9	13	**237**	11	3
-146	75	33	**-18**	95	36	**110**	12	7	**238**	6	0
-145	105	29	**-17**	116	35	**111**	10	9	**239**	4	2
-144	71	18	**-16**	98	33	**112**	9	8	**240**	2	1
-143	90	31	**-15**	117	37	**113**	11	10	**241**	8	1
-142	82	25	**-14**	90	35	**114**	11	8	**242**	11	1
-141	88	1058	**-13**	94	29	**115**	9	7	**243**	6	3
-140	89	26	**-12**	77	41	**116**	13	5	**244**	3	1
-139	96	17	**-11**	81	1081	**117**	9	9	**245**	3	0
-138	87	31	**-10**	106	32	**118**	7	6	**246**	4	1
-137	85	19	**-9**	112	22	**119**	10	4	**247**	3	1
-136	76	20	**-8**	93	20	**120**	9	4	**248**	2	1
-135	75	36	**-7**	95	1067	**121**	16	7	**249**	11	80
-134	93	36	**-6**	95	24	**122**	10	82	**250**	6	2
-133	101	17	**-5**	110	30	**123**	12	2	**251**	8	0
-132	98	20	**-4**	101	29	**124**	11	4	**252**	7	0
-131	81	25	**-3**	116	29	**125**	13	4	**253**	8	1
-130	97	29	**-2**	94	22	**126**	7	4	**254**	9	0
-129	81	22	**-1**	80	1070	**127**	13	7	**255**	5	0
-128	83	36	**0**	105	34	**128**	5	7			

附錄 C

密文資料字元 ASCII 碼分佈統計表

ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數
0	102	28	**65**	101	36	**130**	106	32	**195**	98	27
1	91	1071	**66**	112	27	**131**	97	20	**196**	91	44
2	115	31	**67**	96	41	**132**	102	28	**197**	100	33
3	124	28	**68**	113	24	**133**	108	104	**198**	108	39
4	109	24	**69**	103	37	**134**	107	33	**199**	110	28
5	103	32	**70**	107	1079	**135**	82	39	**200**	105	108
6	107	111	**71**	91	30	**136**	86	29	**201**	102	28
7	100	1071	**72**	100	28	**137**	96	28	**202**	127	39
8	104	26	**73**	102	29	**138**	97	35	**203**	106	34
9	116	30	**74**	113	43	**139**	106	25	**204**	105	29
10	104	35	**75**	90	1074	**140**	96	31	**205**	106	35
11	85	1082	**76**	113	34	**141**	99	1070	**206**	93	28
12	92	43	**77**	111	34	**142**	89	25	**207**	99	31
13	100	25	**78**	99	34	**143**	95	43	**208**	106	19
14	96	31	**79**	91	27	**144**	85	21	**209**	103	32
15	119	38	**80**	102	43	**145**	125	42	**210**	109	31
16	105	37	**81**	78	39	**146**	81	35	**211**	93	29
17	125	31	**82**	109	33	**147**	97	47	**212**	108	24
18	103	34	**83**	100	36	**148**	89	25	**213**	99	25
19	118	39	**84**	104	36	**149**	95	30	**214**	110	24
20	114	26	**85**	96	24	**150**	117	1079	**215**	91	36
21	89	23	**86**	106	36	**151**	102	24	**216**	88	51
22	100	30	**87**	101	28	**152**	110	30	**217**	103	29
23	117	38	**88**	72	36	**153**	106	41	**218**	103	28
24	103	22	**89**	119	32	**154**	107	33	**219**	98	1150
25	102	29	**90**	101	32	**155**	100	43	**220**	115	105
26	84	35	**91**	96	39	**156**	99	45	**221**	101	27
27	103	31	**92**	108	99	**157**	117	34	**222**	109	33
28	108	44	**93**	109	24	**158**	119	38	**223**	94	24
29	90	23	**94**	112	37	**159**	93	40	**224**	112	25
30	121	36	**95**	89	1141	**160**	102	28	**225**	97	31
31	105	43	**96**	104	43	**161**	106	30	**226**	116	35
32	116	30	**97**	104	31	**162**	84	40	**227**	89	30
33	109	1080	**98**	102	25	**163**	96	45	**228**	89	28
34	113	108	**99**	114	32	**164**	97	36	**229**	92	34
35	109	23	**100**	82	38	**165**	107	30	**230**	115	45
36	116	30	**101**	78	31	**166**	103	29	**231**	97	28
37	109	32	**102**	94	34	**167**	85	32	**232**	109	42
38	86	29	**103**	106	27	**168**	104	39	**233**	109	29
39	98	1144	**104**	99	33	**169**	95	34	**234**	96	1067
40	116	32	**105**	106	26	**170**	93	28	**235**	98	25
41	98	25	**106**	119	35	**171**	91	1079	**236**	107	37
42	90	29	**107**	97	37	**172**	112	29	**237**	107	101
43	103	28	**108**	109	39	**173**	96	111	**238**	95	26
44	97	34	**109**	104	35	**174**	114	33	**239**	107	39
45	104	30	**110**	83	35	**175**	107	32	**240**	107	27
46	100	45	**111**	98	32	**176**	105	37	**241**	109	1080
47	98	25	**112**	99	29	**177**	114	36	**242**	100	40
48	98	24	**113**	103	41	**178**	110	37	**243**	120	38
49	114	33	**114**	109	35	**179**	99	20	**244**	97	36
50	108	31	**115**	81	113	**180**	93	39	**245**	107	42
51	103	25	**116**	94	34	**181**	93	33	**246**	100	1074
52	114	46	**117**	126	37	**182**	99	35	**247**	101	29

密文資料字元 ASCII 碼分佈統計表(續)

ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數	ASCII CODE	CBC 筆數	AES 筆數
53	90	27	**118**	106	25	**183**	99	27	**248**	103	38
54	83	22	**119**	89	32	**184**	100	34	**249**	104	28
55	104	46	**120**	91	17	**185**	94	28	**250**	99	113
56	97	29	**121**	121	24	**186**	120	28	**251**	87	26
57	116	31	**122**	102	101	**187**	99	108	**252**	104	42
58	92	32	**123**	99	54	**188**	111	34	**253**	99	108
59	97	28	**124**	86	28	**189**	97	36	**254**	89	1080
60	110	30	**125**	110	31	**190**	103	48	**255**	120	35
61	101	25	**126**	112	24	**191**	103	36			
62	94	28	**127**	96	30	**192**	97	18			
63	109	24	**128**	100	44	**193**	91	29			
64	111	31	**129**	92	23	**194**	108	24			