

# 內容目錄

中文摘要	iii
英文摘要	iv
誌謝辭	v
內容目錄	vi
表目錄	vii
圖目錄	viii
第一章 緒論	1
第一節 研究背景與動機	1
第二節 研究目的	2
第三節 研究範圍與限制	2
第四節 研究架構與流程	3
第二章 文獻探討	4
第一節 資訊安全	4
第二節 密碼學背景	5
第三節 加密技術	6
第四節 資料驗證	11
第五節 數位簽章	12
第六節 密碼破解	13
第三章 研究方法	16
第一節 系統架構	16
第二節 演算法設計	17
第三節 加密演算法	18
第四節 解密演算法	22
第五節 驗證演算法	24
第四章 實驗步驟	28

第五章	系統實做	48
第六章	結論與討論	54
參考文獻		56



# 表 目 錄

表 5-1 加密文章所需時間 . . . . . 53



## 圖目錄

圖 1- 1	研究流程圖	3
圖 2- 1	凱薩加密法字母替換表	7
圖 2- 2	凱薩加密法(Caesar Cipher)的明文和密文轉換	7
圖 2- 3	數字替換法的定義	7
圖 2- 4	數字替換法轉換過程	8
圖 2- 5	英文字母出現之頻率	8
圖 2- 6	柵欄加密法的明文及密文轉換	9
圖 2- 7	柵欄加密法	9
圖 2- 8	DES演算法原理	10
圖 2- 9	驗證碼原理	12
圖 2-10	數位簽章原理	13
圖 3- 1	系統架構	17
圖 3- 2	加密資料表	18
圖 3- 3	格式碼	19
圖 3- 4	驗證碼	20
圖 3- 5	儲存驗證碼表	22
圖 3- 6	比對驗證碼	23
圖 3- 7	使用者資訊資料庫	25
圖 3- 8	新聞資料表	25
圖 3- 9	加密資料表	26
圖 3-10	左移表	26
圖 3-11	驗證碼	26
圖 3-12	驗證碼儲存規則	27
圖 3-13	檢驗碼表	27
圖 4- 1	新聞資料表	28

圖 4- 2	新聞檔案資料表欄位	28
圖 4- 3	類別管理	29
圖 4- 4	新聞資料儲存格式	29
圖 4- 5	新增新聞資料	30
圖 4- 6	設定加密資料表頁面	31
圖 4- 7	設定加密資料表	32
圖 4- 8	分割後的明文	33
圖 4- 9	檔案旋轉	33
圖 4-10	左移	34
圖 4-11	位置交換過程	35
圖 4-12	輸出方向改變過程	35
圖 4-13	驗證碼儲存格式	36
圖 4-14	插入驗證碼過程	36
圖 4-15	新密文格式	37
圖 4-16	加密完成	37
圖 4-17	加密過的密文	38
圖 4-18	獲得加密的檔案	39
圖 4-19	驗證碼	40
圖 4-20	驗證碼表	40
圖 4-21	驗證碼正確，驗證成功	41
圖 4-22	驗證碼長度錯誤，驗證失敗	42
圖 4-23	驗證碼不符合產生規則，驗證失敗	43
圖 4-24	無法讀取驗證碼，驗證失敗	44
圖 4-25	解密成功	45
圖 4-26	資料遭到竄改	46
圖 4-27	解密失敗	46
圖 5- 1	文章列表	48

圖 5- 2	加密前的明文	48
圖 5- 3	設定加密表單	49
圖 5- 4	以格式2加密完成的密文	50
圖 5- 5	以格式5加密完成的密文	50
圖 5- 6	一樣格式5，但是輸出方向改變的密文	51
圖 5- 7	正常解密(驗證碼符合)	52
圖 5- 8	解密成功的明文	52
圖 5- 9	非正常解密的明文	53

