

Security

資訊與網路安全技術

Information
and Network
Security
Techniques

第二版

- 本書由密碼學基礎開始，進入應用密碼學、電子商務安全、乃至私有網路安全，完整且有序列的介紹相關安全技術。
- 詳述 DES、3DES、RC5、RC6、IDEA、AES、RSA、Diffie-Hellman、MD4、MD5、SHA-1、密碼演算法。
- 解說 MAC-DES、HMAC、RSA、DSS、X.509、Kerberos、PKI、資訊安全技術。
- 分析與實例探討防火牆、入侵偵測、網路病毒、IPsec 安全網路的架設原理。
- 隨書光碟備有各種演算法的程式範例，與 OpenSSL 安全程式開發套件。
- 描述 SSL/TLS、S/MIME、PGP、電子商務安全技術。
- 光碟內附本書範例程式、OpenSSL 套件、DevC++ 套件

粘添壽 著

旗標出版股份有限公司



Security



資訊與 網路安全 技術

資訊與網路安全技術
第1版
第1次印刷

資訊與
網路安全
技術

INFORMATION
AND NETWORK
SECURITY
TECHNOLOGY

第二版

感謝您購買旗標書，記得到旗標網站

www.flag.com.tw

更多的加值內容等著您...

1. 建議您訂閱「旗標電子報」：精選書摘、實用電腦知識搶鮮讀；第一手新書資訊、優惠情報自動報到。
2. 「補充下載」與「更正啓事」專區：提供您本書補充資料的下載服務，以及最新的勘誤資訊。
3. 「線上購書」專區：提供優惠購書服務，您不用出門就可選購旗標書！

買書也可以擁有售後服務，您不用道聽塗說，可以直接和我們連絡喔！

我們所提供的售後服務範圍僅限於書籍本身或內容表達不清楚的地方，至於軟硬體的問題，請直接連絡廠商。

- 如您對本書內容有不明瞭或建議改進之處，請連上旗標網站 www.flag.com.tw，點選首頁的 **讀者服務**，然後再按左側 **讀者留言版**，依格式留言，我們得到您的資料後，將由專家為您解答。註明書名(或書號)及頁次的讀者，我們將優先為您解答。

旗標



旗標網站：www.flag.com.tw

學生團體 訂購專線：(02)2396-3257 轉 361,362

傳真專線：(02)2321-1205

經銷商 服務專線：(02)2396-3257 轉 314,331

將派專人拜訪

傳真專線：(02)2321-2545

國家圖書館出版品預行編目資料

資訊與網路安全技術 / 粘添壽著。-- 第二版。

-- 臺北市：旗標，2008.11 面；公分

參考書目：面 含索引

ISBN 978-957-442-674-4 (平裝)

1. 資訊安全

2. 電腦網路

312.76

97021497

作 者 / 粘添壽

發行人 / 施威銘

發行所 / 旗標出版股份有限公司

台北市杭州南路一段15-1號19樓

電話 / (02)2396-3257(代表號)

傳 真 / (02)2321-2545

劃撥帳號 / 1332727-9

帳 戶 / 旗標出版股份有限公司

總 監 製 / 施威銘

行銷企劃 / 張慧卿

監 製 / 陳煥章

執行企劃 / 黃昕暉

執行編輯 / 黃昕暉

美術編輯 / 林美麗

封面設計 / 古鴻杰

校 對 / 粘添壽、黃昕暉

校對次數 / 7次

新台幣售價：720 元

西元 2008 年 11 月出版

行政院新聞局核准登記 - 局版台業字第 4512 號

ISBN 978-957-442-674-4

版權所有・翻印必究

Copyright © 2008 Flag Publishing Co., Ltd.

All rights reserved.

本著作未經授權不得將全部或局部內容以任何形式重製、轉載、變更、散佈或以其他任何形式、基於任何目的加以利用。

本書內容中所提及的公司名稱及產品名稱及引用之商標或網頁，均為其所屬公司所有，特此聲明。

旗標出版股份有限公司聘任本律師為常年法律顧問，如有侵害其信用名譽權利及其它一切法益者，本律師當依法保障之。

牛溥溥 律師

序

隨著資訊網路的風行，如何增加它的安全性，已成為時下最重要的課題。本書整合資訊與網路安全的相關技術，略盡微薄之力，望能使讀者在研習資訊系統安全方面有所幫助。作者已將本書所有演算法程式範例與相關論文彙集於隨書光碟內。另外，為了方便學校授課，也將書本內重點製作成 PowerPoint 檔，以及輔助教材張貼於教學網站(www.tsnien.idv.tw)，有興趣的讀者可自行下載參考使用（或向旗標公司索取）。

本書適合大學三、四年級授課，也可作為研究所研習網路安全用書，更是一般專業訓練不可或缺的好教材。本書共計 17 章，劃分為四大篇，各篇大綱如下：

- ❶ **第一篇 密碼學基礎**：本篇利用五個章節分別針對秘密金鑰系統、公開金鑰系統、雜湊與亂數演算法做深入淺出的介紹，無論是專門研習密碼學或資訊安全技術，本篇都給予一個既完整且基礎性的概念。
- ❷ **第二篇 資訊安全技術**：本篇介紹如何將密碼學運用到資訊安全領域的相關技術，內容包含訊息確認、數位簽章、數位憑證、認證系統與公鑰基礎架構等五個章節；瞭解這些技術是進入資訊與網路安全的必備門檻。
- ❸ **第三篇 電子商務安全技術**：具備資訊安全技術之後，本篇繼續使用二個章節介紹建構安全網頁與安全電子郵件系統等相關技術。
- ❹ **第四篇 私有網路安全技術**：固定位置之私有網路的架設防火牆與入侵偵測系統，以及整合建構遍佈全球各地的分屬機構之虛擬私有網路，本篇以五個章節分別介紹相關的安全技術。

本書第一版原是由兩位作者協力完成，但吳順裕博士忙於其它研究，無暇修正本書，則將此重任交付作者獨自完成，也感謝他繼續提供許多寶貴意見與研究成果。最後對於旗標公司的協助潤筆與修飾，並允諾出版本書致最高的謝意。

本書並非經典之作，僅就自己所學將過去工作經驗彙集成書，書中難免有遺珠之憾，望讀者 / 教師給予不吝指教。

粘添壽 謹識

2008 年 9 月 28 日 於高雄

如何研讀本書

- ❶ **隨書光碟**：包含本書程式範例與 OpenSSL 套件。每一目錄下包含該演算法程式範例，以及相關規格書或論文。程式範例內有註明與書本相對應的章節或圖表，任何 C 編譯器都可以編譯執行（Windows 或 Linux 皆可）。也請讀者詳閱規格文件，這對了解該演算法很有幫助。
- ❷ **程式範例**：各演算法範例皆是最基本程式架構，讀者可將其擴充其他功能。譬如 DES 程式可擴充成 DES-CBC、3DES 或 MAC-DES 程式。
- ❸ **實習環境**：本書採用 OpenSSL 公用程式作為密碼系統的實習環境，包含各種對稱密碼系統、公開密碼系統、安全郵件、以及憑證發行與認證等等，這對我們學習資訊安全很有幫助，請讀者依照書本介紹方法，儘速將該系統安裝完成，並實際演練。
- ❹ **教學範圍**：不分學系，第一、二篇是必備的入門課程，其中三、四兩章，因涉及較複雜的密碼學，授課老師可依學生學習狀況斟酌。就管理學系而言，作者建議教學範圍以第三篇為主，第四篇為輔；反觀就工程學系而言，則需偏重四篇。當然，一切還是依授課老師為主，作者的建議僅供參考。
- ❺ **電子書**：為了減少本書篇幅，不得已將第十六章與十七章內容，製作成 PDF 檔案，儲存於隨書光碟 PDF 資料夾內，請讀者自行列印閱讀。深感歉意！！
- ❻ **RFC 網站**：本書共參考八十幾篇 RFC 規範（附錄 B），讀者若有需要更進一步瞭解的話，請到 RFC 網站下載原版規範(www.rfc-edit.org)。
- ❼ **教學網站**：為使授課老師方便教學，作者已完成 PowerPoint 簡報檔製作（請向旗標公司索取），並陸續蒐錄其他輔助教材、論文、規範、或新增程式範例，張貼於作者教學網站，歡迎讀者多加利用。

編後語

記得，剛進入中山大學電研所就讀碩士班時，實驗室裡總放置一部謝文雄教授所組裝的收音機，每天不斷播放著中廣音樂網，吵得讓我無法專心看書（謝老師一向很節儉捨不得買音響）。每當謝老師離開實驗室，我就將收音機關掉；但當他回來時，他又隨即打開收音機，每天就這樣反反覆覆經過數年。十幾年過後的今天，自己當上了老師，每天陪伴著我雖然不是中廣音樂網（我組裝的收音機更不能聽），但已由鄧麗君懷念歌曲、台灣懷念老歌、古箏佛讚，進步到目前的霹靂布袋戲原聲帶。此時的我，終於頓悟，原本當老師是多麼孤單、作研究又是那麼無聊，唯有此道，足以讓自己得到這麼一點點的成就。在此向全國所有老師致最高敬意，由於您們默默無聞的努力奉獻，培養出眾多優秀學生，使能有效提昇台灣的技術水準，進而擠身國際高科技列強之中。半路出家的我，必須好好向您們學習。

第 0 章 OpenSSL 實習環境建置

0-1	OpenSSL 簡介	0-2
0-2	OpenSSL 編譯與安裝	0-3
0-2-1	Linux 安裝與編譯	0-3
0-2-2	Windows 安裝與編譯	0-4
0-3	OpenSSL 命令語法	0-7
0-3-1	命令格式	0-7
0-3-2	通行碼輸入	0-8
0-3-3	訊息格式	0-9
0-4	對稱密碼系統操作	0-10
0-4-1	命令彙集	0-11
0-4-2	命令格式 - enc	0-12
0-4-3	操作範例	0-13
0-5	RSA 公鑰演算法操作	0-14
0-5-1	公鑰演算法命令彙集	0-14
0-5-2	產生 RSA 鑰匙配對 - genrsa	0-15
0-5-3	RSA 管理命令 - rsa	0-15
0-5-4	RSA 操作命令 - rsautl	0-19
0-5-5	RSA 加密與簽章範例	0-19
0-6	DH 公鑰演算法操作	0-21
0-6-1	產生鑰匙材料 - gendh	0-21
0-6-2	管理 DH 命令 - dh	0-22
0-6-3	管理 DH 參數 - dhparam	0-23
0-7	DSA 公鑰演算法操作	0-24
0-7-1	產生 DSA 鑰匙參數 - dsaparam	0-24
0-7-2	產生 DSA 鑰匙配對 - gendsa	0-26
0-7-3	管理 DSA 鑰匙 - dsa	0-27
0-8	訊息摘要操作	0-28
0-8-1	命令格式 - dgst	0-28
0-8-2	操作範例	0-29
0-9	數位簽章與驗證操作	0-30
0-9-1	RSA 簽署與驗證文件	0-30
0-9-2	DSA 簽署與驗證文件	0-31
0-10	結論	0-32

第一篇 密碼學基礎

第 1 章 安全性資訊系統簡介

1-1	何謂安全性資訊系統	1-2
1-2	安全性工具	1-4
1-2-1	密碼系統	1-4
1-2-2	雜湊函數	1-7
1-2-3	亂數產生	1-8
1-3	訊息的安全性	1-8
1-3-1	訊息加密	1-9
1-3-2	訊息完整性檢查	1-10
1-3-3	訊息確認	1-10
1-3-4	數位簽章	1-11
1-4	作業系統的安全性	1-12
1-4-1	安全性措施	1-12
1-4-2	安全性等級	1-13
1-4-3	封閉性用戶認證	1-14
1-4-4	開放性用戶認證	1-15
1-5	電子化系統的安全性	1-17
1-5-1	安全性網頁系統	1-17
1-5-2	安全性電子郵件	1-18
1-5-3	安全性電子交易	1-18
1-6	私有網路的安全性	1-20
1-6-1	防火牆與入侵偵測	1-21
1-6-2	虛擬私有網路架構	1-21
1-7	結論	1-22

第 2 章 傳統秘密金鑰系統

2-1	密碼學概論	2-2
2-2	密碼系統的安全性	2-3
2-3	密碼破解技巧	2-6
2-4	傳統密碼學的基本原理	2-7
2-4-1	換位加密法	2-7
2-4-2	取代加密法	2-10
2-5	區塊加密法的基本原理	2-13

2-5-1	乘積加密法	2-14
2-5-2	Feistel 加密法	2-15
2-6	DES 密碼系統	2-18
2-6-1	DES 的演算流程	2-19
2-6-2	初始與終結排列	2-20
2-6-3	加密處理	2-22
2-6-4	子鑰匙產生	2-28
2-7	DES 操作模式	2-31
2-7-1	電子密碼書模式	2-31
2-7-2	密文區塊串接模式	2-33
2-7-3	J- 位元密文反饋模式	2-35
2-7-4	J- 位元輸出反饋模式	2-37
2-8	DES 密碼系統的實現	2-39
2-8-1	DES 製作摘要	2-39
2-8-2	DES 程式範例	2-40
2-8-3	OpenSSL 操作範例	2-50
2-9	秘密鑰匙分配	2-50
2-9-1	公鑰系統傳送秘密鑰匙	2-51
2-9-2	鑰匙中心分配	2-52
2-9-3	協商建立秘密鑰匙	2-54

第 3 章 進階秘密金鑰系統

3-1	密碼系統的安全性	3-2
3-1-1	演算法的複雜度	3-3
3-1-2	分散式暴力攻擊法	3-4
3-2	秘密鑰匙系統的摘要	3-4
3-3	Triple DES 密碼系統	3-6
3-3-1	Two-Keys 3DES	3-6
3-3-2	Three-keys 3DES	3-8
3-4	IDEA 密碼系統	3-8
3-4-1	加密運作程序	3-9
3-4-2	加密子鑰匙產生	3-10
3-4-3	解密子鑰匙產生	3-11
3-4-4	編碼器的設計	3-14
3-4-5	操作模式	3-16
3-4-6	IDEA 加密程式範例	3-16

3-5	RC5 密碼系統	3-18
	3-5-1 RC5 參數	3-19
	3-5-2 編碼程序	3-19
	3-5-3 操作模式	3-21
3-6	AES 密碼標準	3-24
	3-6-1 基本架構	3-25
	3-6-2 基本元素	3-28
	3-6-3 數學基礎	3-30
3-7	AES 加密演算法	3-33
	3-7-1 位元組取代運算	3-35
	3-7-2 移位列運算	3-37
	3-7-3 混合行運算	3-38
	3-7-4 回合鑰匙加法運算	3-40
	3-7-5 鑰匙擴充	3-41
	3-7-6 AES 加密程式範例	3-45
3-8	AES 解密演算法	3-45
	3-8-1 InvShiftRows() 函數	3-46
	3-8-2 InvSubBytes() 函數	3-47
	3-8-3 InvMixColumns() 函數	3-48
	3-8-4 AES 解密程式範例	3-49
3-9	AES 相關規範	3-50
3-10	RC4 串流密碼系統	3-51
	3-10-1 串流加密系統模型	3-52
	3-10-2 RC4 演算法	3-53
	3-10-3 RC4 程式範例	3-55
3-11	其它密碼系統	3-56

第 4 章 現代公開金鑰系統

4-1	公開鑰匙系統簡介	4-2
	4-1-1 公鑰系統之架構	4-2
	4-1-2 公鑰系統之應用	4-4
	4-1-3 公鑰系統之演算法	4-6
4-2	數論與密碼學	4-7
	4-2-1 質數與互質數	4-7
	4-2-2 同餘算術	4-8
	4-2-3 相關定理	4-16

目錄

contents

4-3	RSA 演算法	4-18
4-3-1	RSA 演算法推演	4-19
4-3-2	RSA 參數問題	4-23
4-3-3	RSA 安全性	4-25
4-4	實現 RSA 演算法	4-26
4-4-1	步驟一：產生 p 、 q 與 n	4-27
4-4-2	步驟二：產生 $\psi(n)$ 函數	4-28
4-4-3	步驟三：選定公開鑰匙 e	4-29
4-4-4	步驟四：選定私有鑰匙 d	4-29
4-4-5	步驟五：實現 $M^k \bmod n$ 運算	4-29
4-4-6	鑰匙配對驗證	4-32
4-5	Diffie-Hellman 鑰匙交換法	4-33
4-5-1	DH 演算法推論	4-33
4-5-2	中間人攻擊	4-35
4-5-3	防禦中間人攻擊	4-36
4-5-4	實現 DH 演算法	4-37
4-6	PKCS 標準	4-39
4-7	公開鑰匙分配	4-41
4-7-1	公開聲明	4-42
4-7-2	公用目錄	4-42
4-7-3	公開鑰匙授權	4-43
4-7-4	公開鑰匙憑證	4-45

第 5 章 雜湊與亂數演算法

5-1	雜湊函數	5-2
5-2	簡單的雜湊函數	5-3
5-3	MD5 訊息摘要	5-4
5-3-1	MD5 運作原理	5-5
5-3-2	MD5 演算法	5-6
5-3-3	MD5 壓縮函數	5-9
5-3-4	實現 MD5 演算法	5-11
5-4	MD4 訊息摘要	5-12
5-5	SHA-1 演算法	5-14
5-5-1	暫存器起始值	5-15
5-5-2	輸入常數	5-16
5-5-3	訊息擴充	5-16

5-5-4	壓縮函數	5-17
5-5-5	實現 SHA-1 演算法	5-18
5-6	各種演算法的比較	5-20
5-7	破解雜湊函數	5-21
5-7-1	生日攻擊法	5-21
5-7-2	中途相遇攻擊法	5-22
5-8	亂數產生器	5-23
5-8-1	典型亂數產生器	5-24
5-8-2	DES 加密器的亂數產生	5-25
5-8-3	ANSI 亂數產生	5-26

第二篇 資訊安全技術

第 6 章 訊息確認

6-1	訊息確認簡介	6-2
6-2	完整性檢查值 - ICV	6-2
6-2-1	明文計算 ICV	6-3
6-2-2	密文計算 ICV	6-3
6-3	訊息確認碼 - MAC	6-4
6-4	MAC-DES 演算法	6-5
6-5	HMAC 演算法	6-6
6-5-1	HMAC 設計概念	6-7
6-5-2	HMAC 架構	6-8
6-5-3	HMAC 的安全性	6-10
6-5-4	實現 HMAC-MD5	6-11
6-6	MAC 操作方式	6-12
6-6-1	明文與 MAC 傳送	6-12
6-6-2	明文與 MAC 加密後傳送	6-13
6-6-3	密文與 MAC 傳送	6-13
6-6-4	密文計算 MAC 後傳送	6-14
6-7	MAC 演算法強度	6-14
6-7-1	暴力攻擊法	6-14
6-7-2	生日攻擊法	6-16

第 7 章 數位簽章與數位憑證

7-1	數位簽章簡介	7-2
-----	--------------	-----

目錄

7-2	RSA 數位簽章	7-3
7-2-1	RSA 簽章演算法	7-4
7-2-2	RSA 安全性考量	7-5
7-3	DSS 數位簽章	7-5
7-3-1	DSA 演算法	7-6
7-3-2	DSA 安全性考量	7-9
7-4	數位簽章的仲裁機制	7-9
7-4-1	直接仲裁	7-10
7-4-2	第三者仲裁	7-11
7-5	數位憑證	7-14
7-5-1	數位憑證的種類	7-15
7-5-2	數位憑證的格式	7-16
7-6	憑證與私鑰的儲存	7-17
7-6-1	儲存元件	7-17
7-6-2	智慧卡儲存	7-18
7-7	憑證認證的運作	7-19
7-7-1	單向認證	7-20
7-7-2	相互認證	7-21
7-8	憑證授權中心	7-22
7-8-1	CA 服務項目	7-23
7-8-2	憑證的產生與認證	7-24
7-8-3	憑證的註銷	7-25

第 8 章 公鑰基礎架構 - PKI

8-1	公鑰基礎架構簡介	8-2
8-1-1	PKI 憑證標準	8-3
8-1-2	PKI 相關技術	8-4
8-2	PKI 系統架構	8-5
8-2-1	PKI 元件	8-5
8-2-2	PKI 管理項目	8-6
8-3	X.509 v3 憑證	8-8
8-3-1	X.509 命名格式	8-8
8-3-2	X.509 v3 憑證格式	8-10
8-3-3	X.509 v3 延伸欄位	8-13
8-4	X.509 v3 憑證註銷列表	8-18
8-4-1	X.509 CRL 格式	8-18

8-4-2	X.509 CRL 延伸欄位	8-20
8-4-3	X.509 CRL 項目延伸	8-22
8-5	PKI 授信模式	8-22
8-6	PKI 認證路徑	8-25
8-6-1	名稱鏈路	8-25
8-6-2	鑰匙識別鏈路	8-26
8-6-3	領域內認證路徑	8-27
8-6-4	領域間認證路徑	8-30
8-7	X.500 目錄服務	8-31
8-7-1	目錄資訊樹	8-32
8-7-2	目錄模式	8-33
8-7-3	訊息模式	8-33
8-7-4	X.500 運作模式	8-37
8-8	LDAP 協定	8-38
8-8-1	LDAP 協定元件	8-40
8-8-2	LDAP 運作程序	8-41
8-9	OCSP 協定	8-44
8-9-1	OCSP 協定運作	8-45
8-9-2	OCSP 命令封裝	8-46

第 9 章 憑證發行與管理 — OpenSSL CA

9-1	數位憑證與 CA 管理	9-2
9-1-1	憑證發行簡介	9-2
9-1-2	憑證的包裝類型	9-3
9-1-3	憑證相關命令	9-5
9-2	OpenSSL CA 規劃檔	9-6
9-2-1	基本參數設定	9-6
9-2-2	自我簽署憑證設定	9-9
9-3	產生憑證請求 - req	9-10
9-3-1	命令格式	9-10
9-3-2	範例說明	9-11
9-4	建立 CA 系統目錄	9-14
9-4-1	CA 系統結構	9-14
9-4-2	產生 CA 系統目錄	9-16
9-4-3	管理 CA 命令 - ca	9-18
9-5	CA 管理操作範例	9-21

目錄

contents

9-5-1	產生自我簽署憑證	9-21
9-5-2	Root CA 發行用戶憑證	9-27
9-5-3	產生 subCA 系統與憑證	9-31
9-5-4	subCA 簽發用戶憑證	9-32
9-5-5	註銷憑證	9-33
9-6	憑證管理操作	9-36
9-6-1	X.509 憑證命令 - x509	9-36
9-6-2	X.509 CRL 命令 - crl	9-38
9-6-3	PKCS #12 憑證管理 - pkcs12	9-39
9-6-4	PKCS #7 憑證管理 - pkcs7	9-41
9-7	憑證驗證操作	9-43
9-7-1	憑證驗證命令 - verify	9-43
9-7-2	線上憑證狀態命令 - ocsp	9-44

第 10 章 認證協定與系統 -Kerberos

10-1	用戶認證簡介	10-2
10-2	使用者密碼	10-4
10-2-1	共享密鑰建立	10-4
10-2-2	驗證雙方共享密鑰	10-6
10-2-3	密碼破解	10-8
10-2-4	密碼處理技巧	10-9
10-3	單向認證協定	10-12
10-3-1	單向共享密鑰認證	10-13
10-3-2	單向公開鑰匙認證	10-16
10-4	相互認證協定	10-18
10-4-1	相互共享密鑰認證	10-18
10-4-2	相互公開鑰匙認證	10-20
10-5	KDC 的基本概念	10-21
10-5-1	主機使用者的確認	10-21
10-5-2	工作群組使用者的確認	10-22
10-5-3	網域使用者的確認	10-23
10-6	KDC 認證協定	10-24
10-6-1	KDC 基本認證協定	10-25
10-6-2	Needham-Schroeder 認證協定	10-26
10-6-3	擴展型 Needham-Schroeder 協定	10-28
10-6-4	公開鑰匙認證協定	10-30

10-7	Kerberos V4 認證系統	10-34
10-7-1	Kerberos 動機	10-35
10-7-2	Kerberos V4 認證程序	10-37
10-7-3	Kerberos 領域	10-41
10-8	Kerberos V5 認證系統	10-43
10-8-1	Kerberos V5 增加功能	10-43
10-8-2	Kerberos V5 運作程序	10-44
10-8-3	Ticket 旗號	10-47
10-8-4	安全機制選項	10-48
10-9	結論	10-51

第三篇 電子商務安全技術

第 11 章 安全性網頁系統

11-1	WWW 系統安全簡介	11-2
11-2	SSL/TLS 安全協定	11-3
11-2-1	電子商務的安全考量	11-3
11-2-2	Secure Web 的運作程序	11-5
11-3	SSL 協定堆疊	11-6
11-4	SSL 訊息封裝	11-7
11-4-1	握手層訊息格式	11-7
11-4-2	記錄層訊息格式	11-11
11-4-3	紀錄層的封裝程序	11-12
11-5	SSL 會議連結識別	11-13
11-6	SSL 握手協定運作	11-14
11-6-1	第一階段：協商安全套件	11-16
11-6-2	第二階段：伺服器確認與鑰匙交換	11-18
11-6-3	第三階段：客戶端確認與鑰匙交換	11-18
11-6-4	第四階段：完成	11-19
11-6-5	簡化的協議方式	11-20
11-7	SSL 主密鑰產生	11-20
11-7-1	產生前置主密鑰	11-21
11-7-2	主密鑰的計算	11-24
11-8	SSL 會議鑰匙的計算	11-25
11-8-1	鑰匙區塊產生	11-25
11-8-2	計算相關鑰匙	11-26
11-8-3	鑰匙產生範例	11-27