旗標出版股份有限公司

結城浩 著
左瑞麟 譯

密碼學與網路安全 應用

新版暗号技術入門
秘密の国のアリス

- 以大量圖解來解和生活實例說密碼學技術
- 以偵探小說式的手法揭開網路安全原理
- 完整涵蓋網路安全的各項議題
- 保障通訊安全性的技術面實作
- 電子簽章的運作與可靠性探討
- 安全威脅與相對應的密碼學防衛技術
- 理解密碼學的實質應用範疇
- 密碼技術的使用極限與未來發展趨勢

結城浩 著
左瑞麟 譯

密碼學與網路安全應用

新版暗号技術入門
秘密の国のアリス

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「更正啟事」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

密碼學與網路安全應用 / 結城 浩 著 / 左瑞麟 譯.

-- 臺北市：旗標, 西元 2011.08 面； 公分

ISBN 978-957-442-969-1 (平裝)

1. 密碼學 2. 資訊安全

448.761 100012558

作　　者／結城 浩

翻譯著作人／旗標出版股份有限公司

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／陳威吉

監　　督／孫立德

執行企劃／陳彥發

執行編輯／陳彥發

美術編輯／張家騰

封面設計／古鴻杰

校　　對／林佳怡

校對次數／7次

建議售價：520 元

西元 2011 年 10 月 出版

行政院新聞局核准登記-局版台業字第 4512 號

ISBN 978-957-442-969-1

序 Preface

不管是誰都擁有不想被別人知道的資訊—也就是秘密。比如說，銀行存摺的密碼、信用卡號碼、貸款金額、男女之間的關係、犯罪前科、病歷表、電子郵件密碼… 等資料是不想被別人所知道的。也有人不想讓別人知道自己的年齡、身高和體重，因某些原因甚至於連自己的名字也不想被別人所得知。

但現在的社會很多資訊都在電腦裡。把資料放在電腦裡很方便，可以在一瞬間就進行拷貝、也可以簡單地修正錯誤。不管對方在世界的何處都可傳送電子郵件，甚至只要發佈在公開網頁不管是世界上的任何人都可看到。

正因為如此，在現在社會想要保護自己的隱私也變得非常困難。自己的秘密即使被別人拷貝了自己也渾然不知。因為資料並不是不見了，而是這些資訊在電腦上可以很簡單地進行修改，所以個人重要的資料就有被修改的危險性。任何人，如果未經你的同意，將你的秘密用電子郵件傳送給第三者，或在網頁公開的話，那可是非常嚴重的問題。

為了改善這種情況，各種密碼學的技術相繼被開發出來。例如『加密』可保護被竊聽的訊息無法被正確讀取，『單向雜湊函數』可檢查資料是否被修改過，『數位簽章』可確認收到的電子郵件是否真的來自於所信任的一方。本書所介紹的各種密碼技術，就是為了每天使用電腦而生活和工作的我們而存在。這些技術可用來保護我們的秘密，並確認所接收資訊的正確性

可是，再怎麼高明的密碼技術也有其的弱點，那就是『使用的人』。使用者如果沒有正確地運用密碼技術，則安全性也無法維持。無論用多強的密碼技術來保護文件，如果使用者所用的通行碼太弱，再安全的技術也沒有什麼意義。想要正確地使用密碼學技術，就必須對密碼學技術的每一個部份都清楚理解。你必須清楚知道「你現在在做些什麼」、「這個技術所代表的意義為何」。

本書是以淺顯易懂方式介紹密碼學技術的入門書。除了盡量避免介紹複雜的數學問題之外，也盡力使讀者能夠理解各種密碼學技術的功用和意義。密碼，已不再只是專家利用的工具，而是生活於現代的我們所必備的技術。透過本書，讓我們掌握密碼學技術與安全相關的各種基礎知識。

目錄 Contents

第 I 篇　加密

Chapter 1 進入密碼的世界

1-1　密碼 1-2
1-2　對稱式密碼與公開金鑰密碼 1-7
1-3　加解密之外的密碼學技術 1-10
1-4　密碼學者的工具箱 1-12
1-5　隱匿學與數位浮水印 1-14
1-6　關於密碼學與資訊安全方面的常識 1-15
　　問題與討論 1-19

Chapter 2 密碼的歷史 - 做出別人無法正確讀取的文章

2-1　凱撒加密法 2-3
2-2　單一字元替代密碼 2-7
2-3　Enigma 2-16
2-4　延伸思考 2-26
　　問題與討論 2-29

Chapter 3 對稱式密碼 (共通金鑰密碼) - 用一把金鑰加密, 且用同一把金鑰解密

3-1 從字母的加密到位元串的加密 3-3
3-2 單次密碼簿 — 絕對破解不了的密碼 3-6
3-3 DES 3-11
3-4 Triple DES 3-18
3-5 AES 的選定過程 3-23
3-6 Rijndael 3-25
問題與討論 3-30

Chapter 4 區塊加密的模式 - 區塊加密如何重複操作

4-1 區塊加密的模式 4-3
4-2 ECB 模式 4-5
4-3 CBC 模式 4-9
4-4 CFB 模式 4-14
4-5 OFB 模式 4-18
4-6 CTR 模式 4-21
4-7 該使用何種模式 4-24
問題與討論 4-27

Chapter 5 公開金鑰加密演算法 - 公開金鑰用來加密, 密鑰用來解密

5-1 密鑰分配問題 5-3
5-2 公開金鑰密碼 5-8
5-3 時鐘演算法 5-14
5-4 RSA 5-26
5-5 RSA 的攻擊 5-38
5-6 其他公開金鑰密碼 5-45
5-7 關於公開金鑰密碼的 Q & A 5-46
問題與討論 5-51

Chapter 6 混合型密碼系統 - 利用對稱式密碼加快速度, 利用公開金鑰密碼保護會議金鑰

6-1 混合型密碼系統 6-2
6-2 強安全性的混合型密碼系統 6-10
6-3 密碼技術的組合 6-12
問題與討論 6-13

第 II 篇　認證

Chapter 7　單向雜湊函數 - 取得訊息的指紋

7-1　何謂單向雜湊函數 7-3
7-2　單向雜湊函數的應用 7-13
7-3　單向雜湊函數的實際例子 7-16
7-4　單向雜湊函數 SHA-1 7-18
7-5　單向雜湊函數的攻擊 7-26
7-6　單向雜湊函數所不能解決的問題 7-31
問題與討論 7-33

Chapter 8　訊息認證碼 - 訊息是否完整？是否由特定的送信者所送出的呢？

8-1　訊息認證碼 8-2
8-2　關於訊息認證碼的應用 8-6
8-3　訊息認證碼的實現方法 8-6
8-4　HMAC 的詳細解說 8-7
8-5　針對訊息認證碼的攻擊 8-10
8-6　訊息認證碼所不能解決的問題 8-14
問題與討論 8-16

Chapter 9 數位簽章 - 誰是訊息的原始作者

9-1 數位簽章 9-2
9-2 數位簽章的產生與驗證方法 9-9
9-3 針對數位簽章的疑問 9-14
9-4 數位簽章的應用實例 9-19
9-5 RSA 數位簽章 9-22
9-6 其他數位簽章演算法 9-25
9-7 針對數位簽章的攻擊 9-26
9-8 數位簽章和其他技術之比較 9-29
9-9 數位簽章所無法解決的問題 9-31
問題與討論 9-33

Chapter 10 數位憑證 - 以公開金鑰為訊息的數位簽章

10-1 數位憑證 10-2
10-2 實際製作一張憑證 10-6
10-3 公開金鑰基礎建設 (PKI) 10-13
10-4 針對數位憑證的攻擊 10-22
10-5 關於數位憑證的 Q & A 10-28
問題與討論 10-33

第 III 篇　金鑰、亂數、應用技術

Chapter 11 金鑰 - 保護機密的根本要素

11-1 何謂金鑰 11-2
11-2 各式各樣的金鑰 11-5
11-3 金鑰的管理 11-10
11-4 Diffie-Hellman 密鑰交換 11-16
11-5 基於通行碼的密碼系統 (PBE) 11-23
11-6 如何產生安全的通行碼 11-30
問題與討論 11-34

Chapter 12 亂數 - 不可預測的根源

12-1 使用亂數的密碼技術 12-2
12-2 亂數的性質 12-3
12-3 虛擬亂數產生器 12-7
12-4 具體的虛擬亂數產生器 12-9
12-5 針對虛擬亂數產生器的攻擊 12-20
問題與討論 12-22

Chapter 13 PGP - 將密碼學技術整合的專業工具

13-1 PGP 的概要 13-2
13-2 金鑰對的產生 13-5
13-3 加密與解密 13-6
13-4 數位簽章的產生與驗證 13-14
13-5『數位簽章的生成與加密』以及『解密與簽章驗證』 13-19
13-6 信任網 13-23
問題與討論 13-31

Chapter 14 SSL/TLS - 安全的通訊

14-1 何謂 SSL/TLS 14-2
14-2 SSL/TLS 的通訊流程 14-8
14-3 針對 SSL/TLS 的攻擊 14-24
14-4 SSL/TLS 在使用上需注意的事項 14-25
問題與討論 14-28

Chapter 15 密碼技術與現實社會 - 生活在不完全安全的當下

15-1 密碼技術的總結 15-2
15-2 期待絕對安全的密碼技術 15-9
15-3 密碼技術就算能達到完美的地步, 人也無法達到完美 15-12
問題與討論 15-18

加密

Chapter 1
進入密碼的世界

6 5 8 2 1 4 5 8 9 6 3 2 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 1 4 5 0 2 3
5 3 6 8 4 2 1 8 5 2 5 2 5 1 8 7 5 2 6 9 5 2 2 3 6 3 2 4 2 3 6 5 8 5 2 1 2 5 2 5 6 6 2 0 0 1 5 9 9 6 8 8
0 6 3 9 5 4 5 6 2 6 4 5 6 5 4 2 3 5 8 0 8 9 6 2 5 5 4 1 4 5 2 3 5 2 6 8 3 4 5 2 1 1 8 8 5 9 5 4 8 5 6 3
2 5 3 2 2 8 8 7 4 7 4 1 5 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 5 6 3 2 6 5 8 8 6 5 2 4 5 5 6 3 6 3 7 3 4 6 0
8 5 2 6 5 2 5 2 4 1 2 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 1 4 5 0 2 3 1
9 3 8 2 7 1 7 9 8 4 6 1 2 3 1 3 1 3 6 5 8 5 4 2 6 9 7 5 2 1 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 2 5 0 0 1 5 3
1 2 2 5 4 4 6 9 6 3 6 6 8 5 7 4 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 8 7 0 0 3 6 3 3 6 2
6 5 8 2 1 4 5 8 9 6 3 2 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 1 4 5 0 2 3
5 3 6 8 4 2 1 8 5 2 5 2 5 1 8 7 5 2 6 9 5 2 2 3 6 3 2 4 2 3 6 5 8 5 2 1 2 5 2 5 6 6 2 0 0 1 5 1 0 5 8 8
0 6 3 9 5 4 5 6 2 6 4 5 6 5 4 2 3 5 8 0 3 2 5 4 5 4 5 8 4 5 8 7 5 2 6 8 3 4 5 2 1 1 8 8 5 9 5 4 5 2 2 3
2 5 3 2 2 8 8 7 4 7 4 1 5 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 5 6 3 2 6 5 8 8 6 5 2 4 5 5 6 3 6 3 7 3 4 6 0
3 6 5 8 5 2 5 2 4 1 2 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 6 2 8 7 8 8 9
9 3 8 2 7 1 7 9 8 4 6 1 2 3 1 3 1 3 6 5 8 5 2 5 6 3 2 8 9 6 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 2 5 0 0 1 5 0
3 3 6 9 7 4 1 2 5 8 4 6 9 6 3 6 6 8 5 7 4 7 5 2 6 9 5 2 1 4 8 6 6 3 6 8 5 5 2 9 8 5 2 2 0 0 0 6 3 3 6 2
6 5 8 2 1 4 5 8 9 6 3 2 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 5 1 4 5 0 2 3
5 3 6 8 4 2 1 8 5 2 5 2 5 1 8 7 5 2 6 9 5 2 2 3 6 3 2 4 2 3 6 5 8 5 2 1 2 5 2 5 6 6 2 0 0 1 5 9 9 6 8 8
0 6 3 9 5 4 5 6 2 6 4 5 6 5 4 2 3 5 8 0 8 9 6 2 5 5 4 1 4 5 2 3 5 2 6 8 3 4 5 2 1 1 8 8 5 9 5 4 8 5 6 3
2 5 3 2 2 8 8 7 4 7 4 1 5 5 1 8 7 5 2 6 9 5 2 1 4 8 9 5 2 5 6 3 2 6 5 8 8 6 5 2 4 5 5 6 3 6 3 7 3 4 6 0
4 6 3 5 5 2 5 2 4 1 2 2 5 6 2 1 1 4 9 5 2 1 4 8 9 5 2 4 5 2 3 6 9 8 5 2 2 0 0 0 2 5 6 2 1 5 2 1 4 2 5 9

本章重點

密碼學關連技術種類繁多且彼此相互關連。本章先不對細微部分做介紹，而從宏觀的角度帶讀者進入密碼學的世界。

1-1 密碼

Alice 與 Bob

在說明加解密等密碼協議的執行過程中，對參與資訊交換的人或電腦，我們必須賦予他們適當的名稱以方便進行解說。如果僅單純利用 A 或 B 等記號作定義似乎過於單調。在本書中，我們將使用如 Alice 或 Bob 等人名來表示密碼系統中各個環節的參與成員並進行解說 (Fig.1-1)。

Fig.1-1 ● 本書主要登場人物

Alice	一般的參與成員
Bob	一般的參與成員
Eve	竊聽者：可以竊聽所有傳輸的資訊
Mallory	主動式攻擊者：可以妨礙資訊的傳輸或偽造、竄改傳輸中的訊息
Trent	可信賴的第三者
Victor	驗證者

送信者、接收者、竊聽者

假設 Alice 欲利用電子郵件 (email) 送信給 Bob，此時因為 Alice 是送信的一方，我們稱 Alice 為**送信者** (sender)。另外，Bob 為收信的一方，所以此時我們稱 Bob為**接收者** (receiver)。

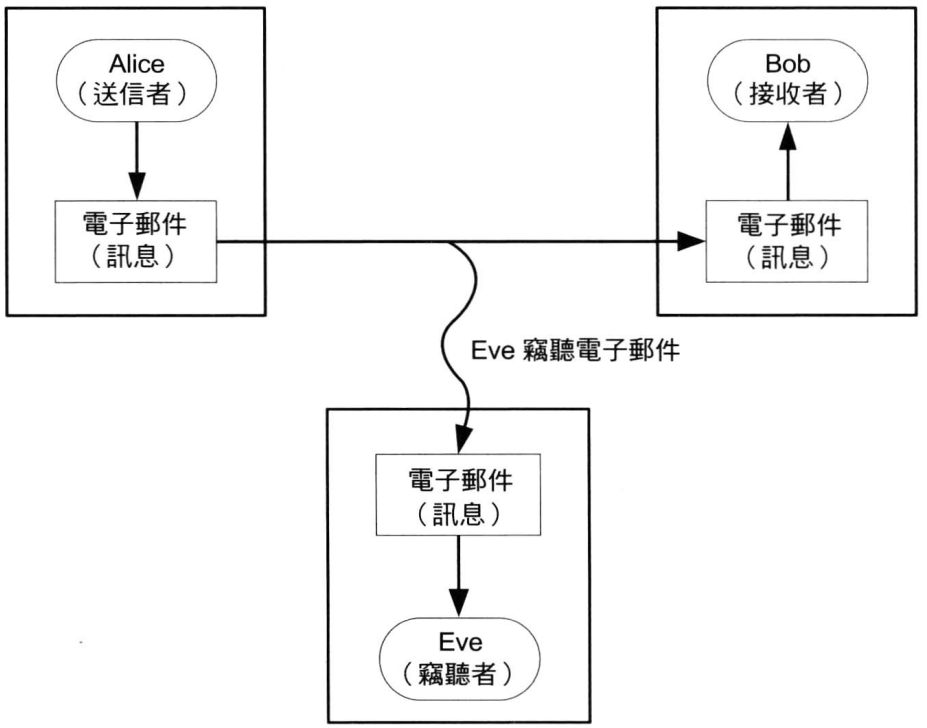
送信者、接收者等用語並不只限定於使用在郵件傳輸的時候，只要有任何資訊要從一人傳送到另一人手中時，送出資訊的一方就稱為**送信者**，而接收的一方就稱為**接收者**。而我們用資訊或訊息 (message) 來表示欲傳送的資訊的總稱 (Fig.1-2)。

當電子郵件由 Alice 的電腦，經由網路傳送到 Bob 的電腦時，途中必定會經過許多台電腦、伺服器及通訊設備。在這傳輸過程中，電子郵件很有可能在通訊雙方不知不覺的情況下，被惡意的**竊聽者** (eavesdropper) 中途攔截並讀取 (Fig.1-3)。

取英文竊聽者 (eavesdropper) 的諧音，本書中將以 Eve 來表示這樣一個竊聽者。

Fig.1-2 ● Alice 與 Bob 通訊的示意圖 (送信者, 接收者)

Fig.1-3 ● Eve 竊聽郵件示意圖 (竊聽者)



竊聽者 Eve 並不限定是一個實體的人，他可能只是一個被裝在某個通訊設備中的竊聽器，也可能僅是一個外掛在郵件軟體或郵件伺服器中的一段程式碼 (program)。

如果不採取一些預防的措施，則原本僅屬於送信者與接收者才可知的訊息，就有可能暴露於被第三者所竊聽的危險之中。

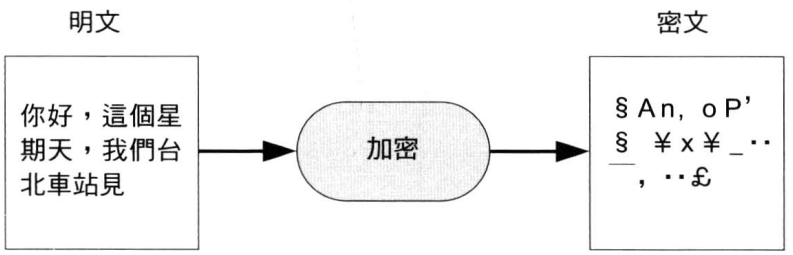
加密與解密

Alice 因為不希望自己的電子郵件內容被第三者所看到，所以將郵件內容先**加密** (encrypt) 之後才送出去。

在密碼學中，加密之前的訊息，我們稱之為**明文** (plaintext)，而經過加密之後的訊息，則稱之為**密文** (ciphertext)。

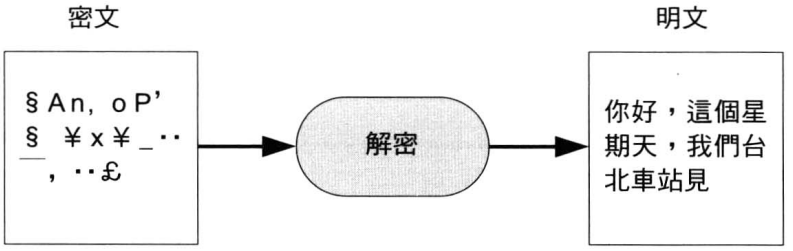
任何人都可以輕易從明文瞭解訊息的內容，但無法從密文本身瞭解原始訊息的內容。

Fig.1-4 ● 明文經過加密後，即成為語意不詳的密文



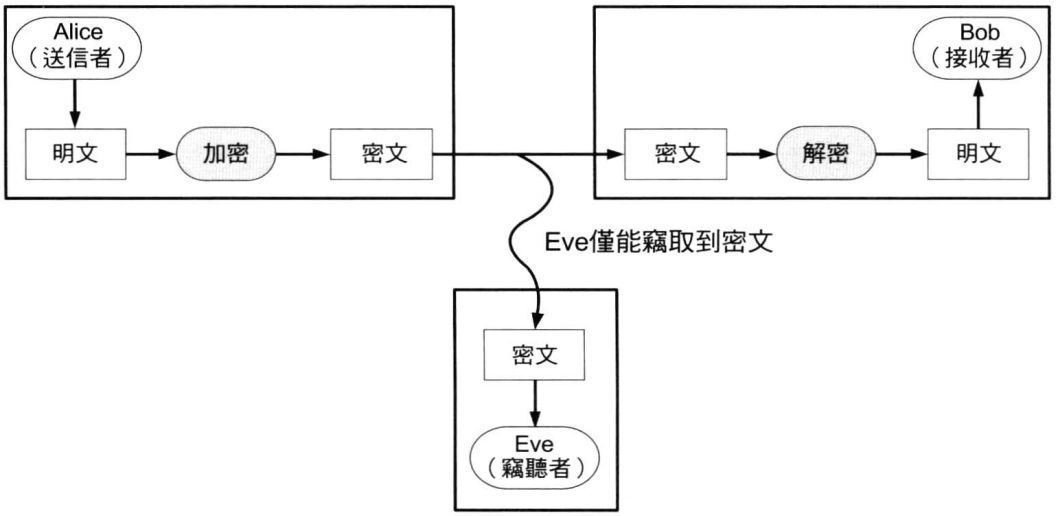
之後，Bob 收到了 Alice 寄來經過加密後的訊息 (密文)，但因為 Bob 無法直接從密文讀取訊息，所以需要先將密文**解密** (decrypt)，恢復成明文之後才可以讀取其內容。將密文恢復成明文的過程，就稱之為**解密**。

Fig.1-5 ● 密文經過解密後，即復原為原始的明文



訊息經過加密之後才送出的話，就算中途被竊聽者所竊聽或盜取了，竊聽者所能得到的，也僅止於加密過後的密文而已。竊聽者是無法從密文瞭解原始訊息 (即明文) 的內容的。

Fig.1-6 ● 訊息經過加密後送出，則竊聽者僅能得到密文



使用密碼加密保障訊息的機密性

在上述的例子中，Alice 將訊息（即電子郵件）加密，而 Bob 將訊息解密。這個過程是為了防止竊聽者 Eve 竊取到原始電子郵件的內容。Alice 和 Bob 在此利用到了**密碼**（cryptography）的技術，保障了電子郵件的**機密性**（confidentiality）。

密碼解讀

訊息經過加密之後，Eve 除了密文就得不到其他的了。Eve 如果想要知道明文的內容，就必須想辦法將密文恢復回原始的明文才行。

前面提過，真正的接收者將密文復原回明文的過程稱之為『解密』。但如果是接收者以外的第三人欲將密文復原回明文的過程，則稱之為**密碼破解**（cryptanalysis）。也稱為**解讀**，或稱為**密碼解析**。

進行密碼解讀的人稱之為**密碼破解者**（cryptanalyst）。密碼破解者並不限定於有惡意的第三方。密碼學的研究者，有時為了研究某些密碼的強度（密碼破解困難度），也會進行密碼的解讀。在此情況下，密碼的研究者就是密碼破解者。