網路安全的理論與實務

楊中皇 著

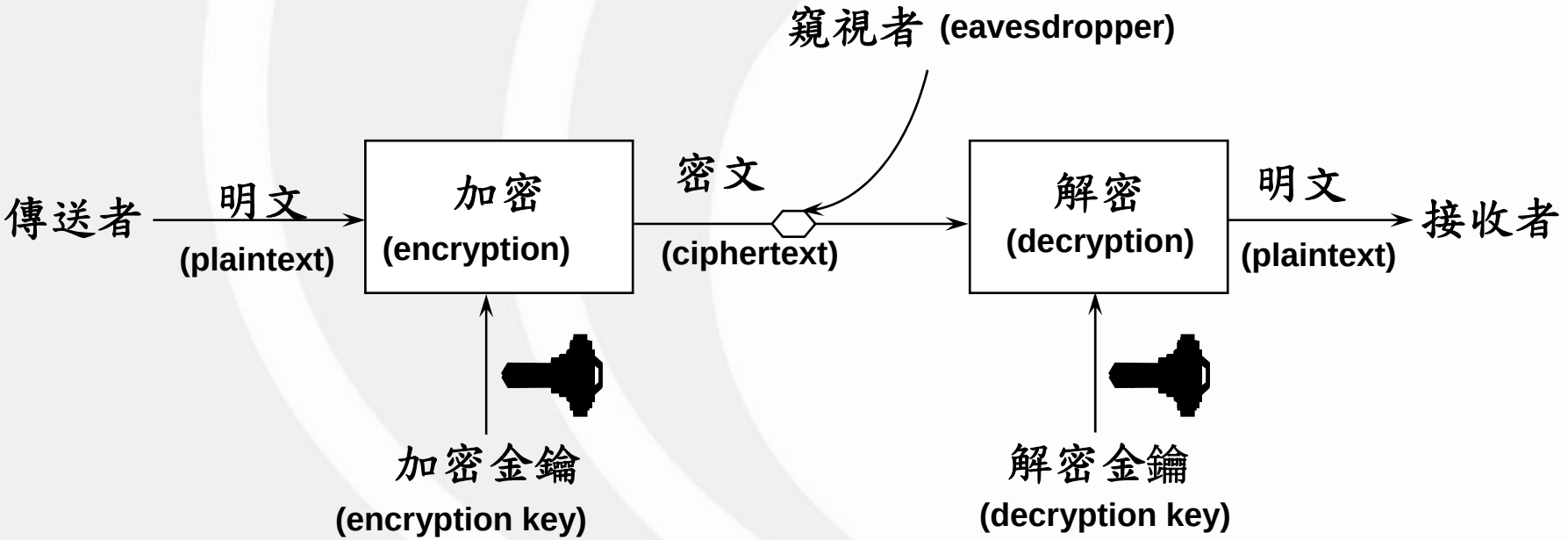
第一章 網路安全概論

http://crypto.nknu.edu.tw/textbook/

第一章 網路安全概論

- 密碼學技術
- 資訊安全服務
- 網路安全模型
- OpenSSL

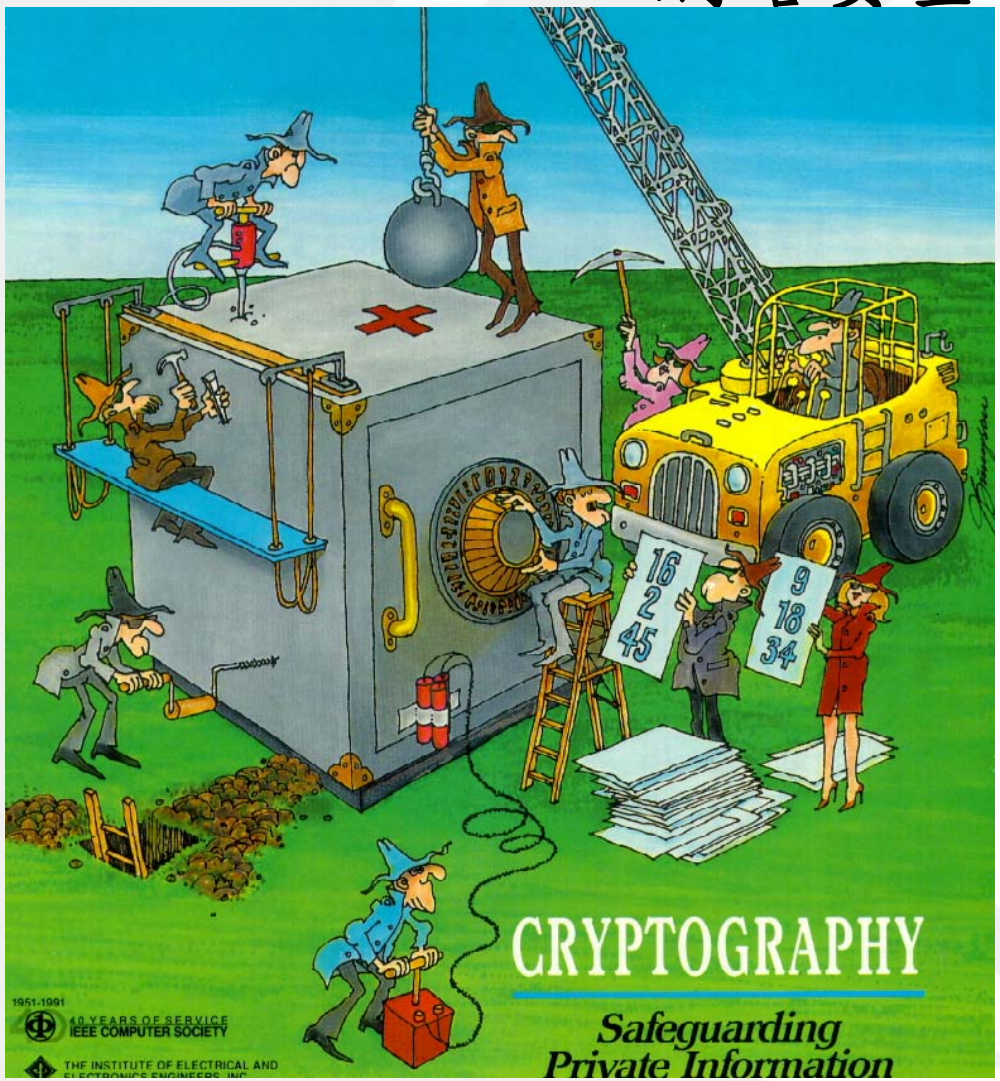
密碼系統示意圖


窺視者 (eavesdropper)
傳送者
明文
(plaintext)
加密
(encryption)
密文
(ciphertext)
解密
(decryption)
明文
(plaintext)
接收者
加密金鑰
(encryption key)
解密金鑰
(decryption key)

名詞說明

- 密碼學，cryptography
- 明文，plaintext
- 密文，ciphertext
- 加密，encryption
- 金鑰， key
- 密碼分析，cryptanalysis
- 僅有密文攻擊，ciphertext-only attack
- 已知明文攻擊，known-plaintext attack
- 自選明文攻擊，chosen-plaintext attack

網路安全系統原則



Key:金鑰(或金匙、密鑰、鍵)

設計完善的網路安全系統，並不會因為設計細節的完全公開，而使其安全性受到威脅。

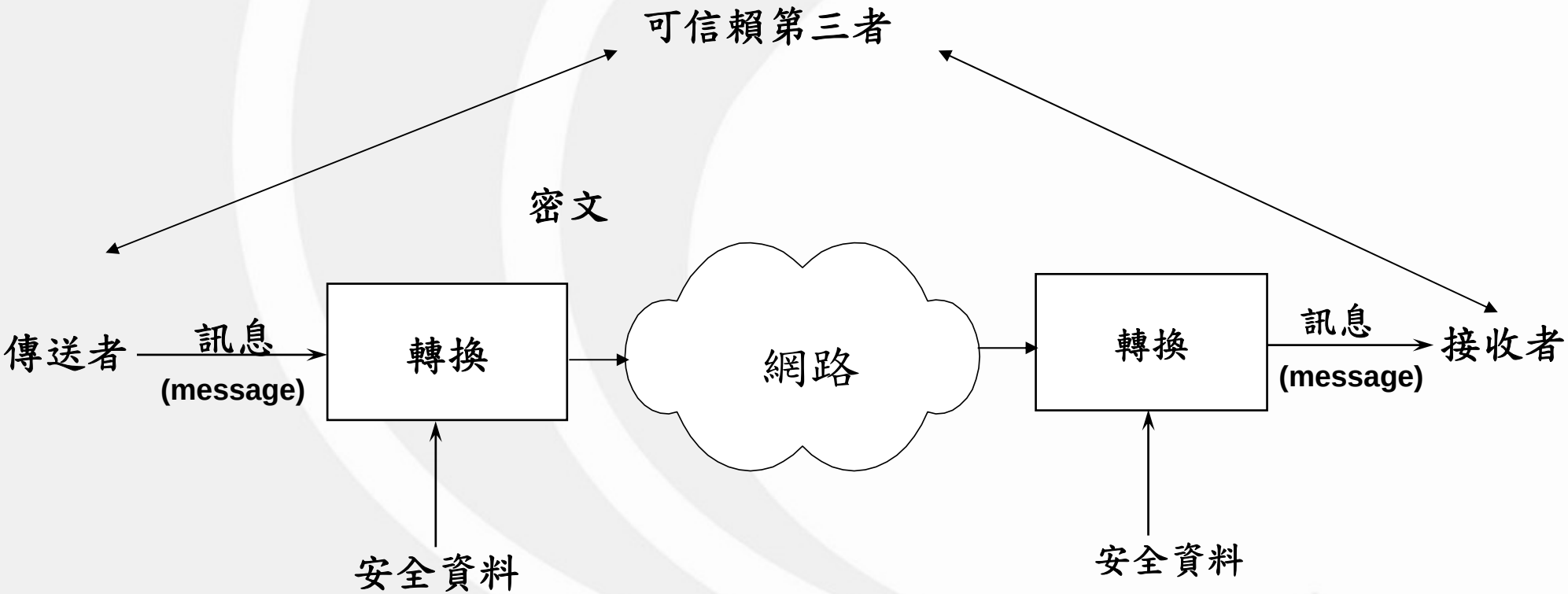
暴力攻擊法尋找金鑰平均的時間

等價金鑰長度(位元)	可能的金鑰數	每秒搜尋 10^6 次 平均破解時間	每秒搜尋 10^{12} 次 平均破解時間
40	$2^{40} \approx 1.1 \times 10^{12}$	6.36 天	0.55 秒
56	$2^{56} \approx 7.2 \times 10^{16}$	1142 年	10.01 小時
128	$2^{128} \approx 3.4 \times 10^{38}$	5.4×10^{24} 年	5.4×10^{18} 年
192	$2^{192} \approx 6.2 \times 10^{57}$	9.95×10^{43} 年	9.95×10^{37} 年
256	$2^{256} \approx 1.2 \times 10^{77}$	$1,84 \times 10^{63}$ 年	1.84×10^{57} 年

資訊安全服務

- 保密性(Confidentiality)
- 確認性（Authentication）
- 完整性(Data Integrity)
- 不可否認性(Non-repudiation)
- 存取控制(Access Control)
- 可用性(Availability)

網路安全模型



SSL

- SSL (Secure Socket Layer)
- 網景公司(Netscape) 1994年提出安全網路協定
- https
- 可用於全球資訊網(WWW)、電子郵件(email)、檔案傳輸(ftp)等
- 網際網路標準組織(IETF) TLS (Transport Layer Security)，RFC 2246 ，1999

OpenSSL

- http://www.openssl.org/
- 開放原始碼的工具
- SSL及TLS的實作
- Unix/Linux與Windows 98/ME/NT/2000/XP等多種平台
- 具有密碼學技術功能
- 前端直接以命令列(Command-line)的方式來使用

OpenSSL於Linux的安裝

1. 首先下載OpenSSL套件，目前最新的版本是openssl-0.9.8。
2. 將OpenSSL解壓縮

> tar zxvf openssl-0.9.8.tar.gz

3. 進入OpenSSL目錄

> cd openssl-0.9.8

4. 執行OpenSSL的安裝

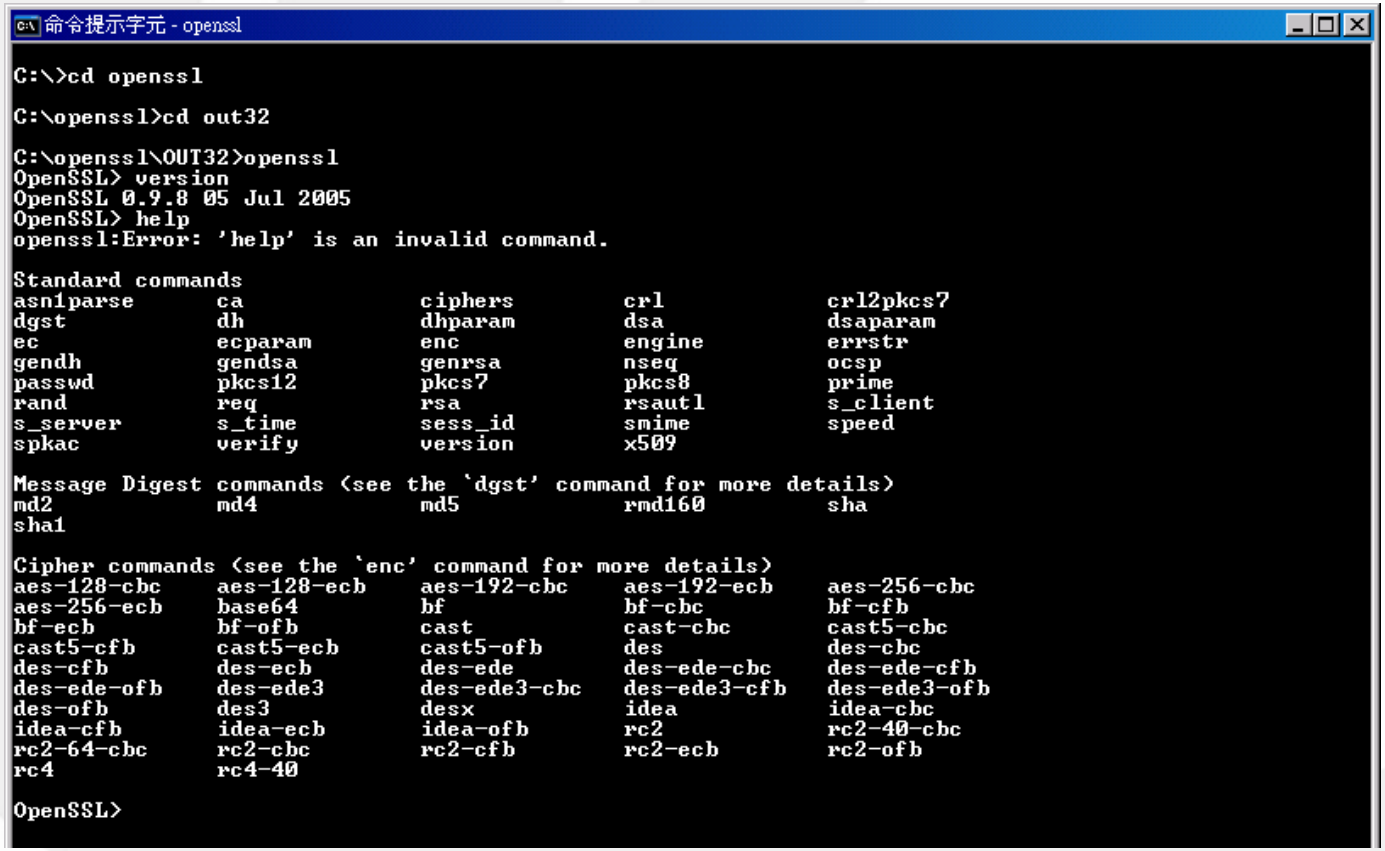
> ./config --prefix=/usr/local -- openssldir=/usr/local/openssl

> make

> make install

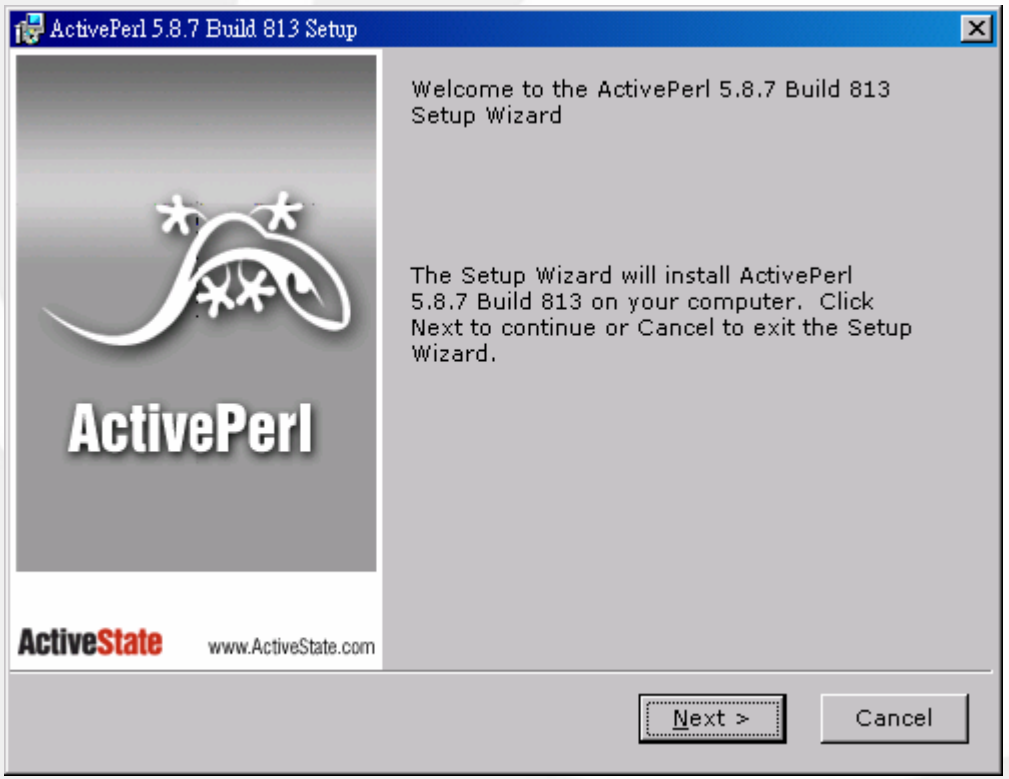
OpenSSL於Windows的安裝

- 先安裝ActivePerl
- ms\bcb4; make -f bcb.mak



ActivePerl安裝

- http://www.activestate.com/ActivePerl/
- 安裝ActivePerl-5.8.7.813-MSWin32-x86-148120.msi



參考資料

- 教科書網站 http://crypto.nknu.edu.tw/textbook/
- 美國國家標準技術局(NIST)電腦安全資源中心 http://csrc.nist.gov/
- 電腦網路危機處理中心 http://www.cert.org/
- 網際網路標準組織 http://www.ietf.org/
- 網路駭客DVD