對稱密碼系統操作

命令彙集

```
H:\SecureLab\study>openssl
OpenSSL> ?
…
Cipher commands (see the `enc' command for more details)
aes-128-cbc    aes-128-ecb    aes-192-cbc    aes-192-ecb    aes-256-cbc
aes-256-ecb    base64         bf             bf-cbc         bf-cfb
bf-ecb         bf-ofb         cast           cast-cbc       cast5-cbc
cast5-cfb      cast5-ecb      cast5-ofb      des            des-cbc
des-cfb        des-ecb        des-ede        des-ede-cbc    des-ede-cfb
des-ede-ofb    des-ede3       des-ede3-cbc   des-ede3-cfb   des-ede3-ofb
des-ofb        des3           desx           idea           idea-cbc
idea-cfb       idea-ecb       idea-ofb       rc2            rc2-40-cbc
rc2-64-cbc     rc2-cbc        rc2-cfb        rc2-ecb        rc2-ofb
rc4            rc4-40
```

命令格式 - enc

- **命令格式 - enc**

```
openssl enc -ciphername [-in filename] [-out filename] [-pass arg] [-e]
    [-d] [-a] [-A] [-k password] [-kfile filename] [-K key] [-iv IV] [-p] [-salt]
    [-P] [-bufsize number] [-nopad] [-debug]
```

命令格式 - enc

操作範例

```
H:\SecureLab\study>type data.txt            【顯示原明文內容】
012345678901234567890123456789
H:\SecureLab\study>openssl rc4 -in data.txt -out cipher.txt     【加密處理】
enter rc4 encryption password:              【輸入加密鑰匙：1234567】
Verifying - enter rc4 encryption password:       【重複輸入加密鑰匙】
H:\SecureLab\study>openssl rc4 -d -in cipher.txt -out plain.txt     【解密處理】
enter rc4 decryption password:            【輸入解密鑰匙】
H:\SecureLab\study>type plain.txt           【顯示解密後明文】
012345678901234567890123456789
```