RSA 鑰匙系統操作

- **RSA 鑰匙系統命令彙集**
  - **genrsa**：利用 **RSA** 演算法產生一個鑰匙檔案。
  - **rsa**：處理 **RSA** 鑰匙的格式轉換。
  - **rsautl**：使用 **RSA** 演算法執行加密、解密、簽署與驗證等運算。

產生 RSA 鑰匙配對 - genrsa

- 產生 RSA 鑰匙配對 - genrsa

```
H:\SecureLab>openssl genrsa -out rsaprivate.pem -passout  pass:12345 -des 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
H:\SecureLab>dir/b  rsaprivate.pem
rsaprivate.pem
```

RSA 管理命令 - rsa

- **RSA 管理命令 – rsa**
  - 範例操作。之前吾人利用 **genrsa** 產生一個鑰匙檔案，接著再利用 **rsa** 管理命令，將他轉換成一般文件格式（**Text**，**rsaprivate.txt**），觀察其內容如何。

```
H:\SecureLab\study>openssl rsa -in rsaprivate.pem -passin pass:12345 –text rsaprivate.txt
```