Information Security, Spring, 2020

Department of Information Management and Finance
National Chiao Tung University

Assignment 1

本次作業目標在於熟悉如何使用上課講到的各式 cryptographic primitive. 具體來說, 請你利用現有的 library (譬如 PyCrypto https://pypi.org/project/pycrypto/ 或是 cryptography https://pypi.org/project/cryptography/ 或是 OpenSSL https://www.openssl.org/) 實現不同的 cryptographic primitive, 並且量測他們的效率. 我們要測試 1 個 symmetric cipher 搭配 3 種 mode of operations, 1 個 asymmetric cipher , 2 個 stream cipher, 2 個 hash function, 2 個 MAC. 譬如可以 AES-256-CBC, AES-256-CTR, AES-256-GCB, RSA-2048, SHA-128, SHA-256, CBC-MAC, HMAC 之類的組合.

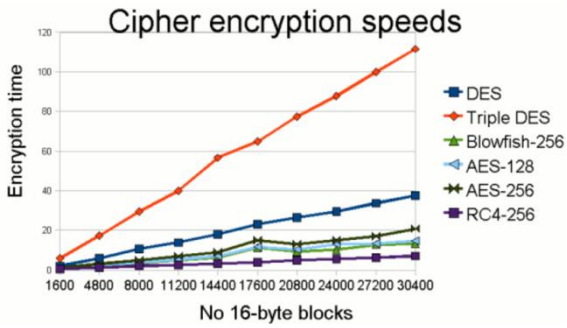
詳細說明

Task 1. 隨機生出一個 size 為 32MB+7bit (或適當 size) 的 random file. 這樣奇怪大小的目的在於讓你等等做加密時的最後一個 block 需要 padding.

Task 2. 用你選擇的 library 實作出 1 個 symmetric cipher 搭配 3 種 mode of operations, 1 個 asymmetric cipher , 2 個 stream cipher, 2 個 hash function, 2 個 MAC. 在過程中, 如果有可以 call 的 function 來實作則請使用 function 即可.

Task 3. 在實現以上功能時, 因為會有需要 padding 的需求, 請用 PKCS padding 當作關鍵字找尋資料, 尋找適當的 padding 來加入你的程式內, 讓 padding 是符合規範的 padding.

Task 4. 請測量以上 implementation 應用在你的 random file 的時間並且畫出類似下列的圖示.



Task 5. 請撰寫報告 (可以接受 Word 與 Latex) 搭配 screenshot 與程式碼解說你怎麼決定各式參數.

甚麼該出現在你的 report 裡?

✧ 你的 report 該出現你如何安裝 library, 以及貼上你的 code, 並且針對你的 code

盡量做逐行或是逐段解釋.

- ✧ Report 內也要出現時間比較圖.
- ✧ 請視這份 report 為一份教學文件, 下個學期的學弟妹也許將會看你的 report 來安裝與使用 PyCrypto and Cryptography 這 2 個 package, 以及看你的 report 來實作出你選擇的 cryptographic primitive.

該怎麼繳交 (若不符合規定則恕不接受)?

- ✧ Code 與報告一同壓縮後, 上傳至 e3 系統
- ✧ 繳交截止日 2020 年 5 月 12 日 23:59:59. 可以遲交一個禮拜, 但扣 20%分數.