Information Security, Fall, 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 pycryptodome https://pypi.org/project/pycryptodome/ 或是 OpenSSL https://www.openssl.org/) 實現不同的 cryptographic primitive, 並且量測他們的效率. 我們要測試不同密碼元件實現的速度差別.

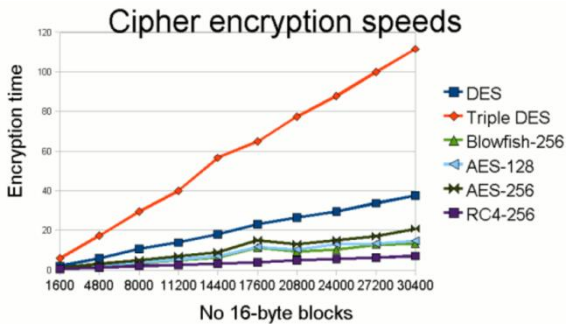
詳細說明

Task 1. 隨機生出一個 size 為 4MB+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 (通常你可能需要同時使用不同 library 如 PyCrypto 與 pycryptodome 才能找到所有規定的 cipher/hash/MAC) 實作出 AES-256-CBC, AES-256-OCB, AES-256-GCM, AES-256-CCM, RSA-1024, RSA-2048, SHA-256, ChaCha20, Poly1305, ChaCha20-Poly1305, HMAC, CBC-MAC 共 11 種密碼元件, 其中 OCB, GCM, CCM 是現行常用的 mode of operation, 而 Poly1305 是 Google 目前正在推行的 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. 課程投影片第 74~76 頁為「Key as IV is Bad」的說明. 請用程式演示這樣的過程.

Task 6. 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.

規定

- ✧ 本次是第一次作業, 請建立一個資料夾, 資料夾名稱為「(assignment1)學號+名字」, 其中學號與名字中間不含+或是空白符號. 譬如你的學號為 12345 且名字為王小明, 則資料夾名稱為「(assignment1)12345 王小明」. 之後將各個程式檔案放置於資料夾內.
- ✧ 請利用 Word 或是任何你熟悉的文書處理軟體撰寫「助教如何執行你的程式之步驟說明」. 由於我們不規定特定的程式語言, 因此可能各位使用的程式語言眾多. 譬如即便是 python, 會有人繳交 py, 也會有人繳交 ipynb. 另外, 助教也會使用不同的輸入來測試你們程式的正確性. 所以明確地告訴助教該更改程式的哪個部分將有助於批改評分. 整體而言, 請利用這個檔案告訴助教該如何批改你的程式. 此說明的檔名則固定為 instruction.docx; 如果你採用其他文書處理軟體撰寫報告則記得命名為 instruction.doc 或是其他格式.
- ✧ 請利用 Word 或是任何你熟悉的文書處理軟體撰寫報告, 報告內該出現你如何安裝 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. 報告的檔名則固定為 report.docx; 如果你採用其他文書處理軟體撰寫報告則記得命名為 report.doc 或是其他格式. 你的報告應該要有至少 https://www.dropbox.com/s/kpvj1awlitw27zp/Information_Security_Cryptographic_primitives.pdf?dl=0 這樣的撰寫品質.
- ✧ 請將 (a) 程式檔, (b) 說明檔, (c) 報告檔都放入資料夾內, 針對資料夾進行 zip 壓縮. 壓縮後的檔名與資料夾的命名相同; 譬如你的學號為 12345 且名字為王小明, 則壓縮檔名稱為「(assignment1)12345 王小明」. 之後將壓縮檔上傳至 new e3.
- ✧ 若是違反上述規定, 則不予給分.
- ✧ 繳交截止日 2020 年 11 月 9 日 23:55:00. 可以遲交一個禮拜, 但扣 20%分數.