Information Security and Cryptography, Fall, 2017

Department of Computer Science and Engineering
National Chung Hsing University

Assignment 1

- ✧ This is a team-based project
- ✧ You are required to write a report in Latex (only accept Latex-compiled document, MS Word document is not allowed)
- ✧ You are required to complete the following tasks by writing programs, instead of using command line operations.

The objective of this project is to have a performance comparison of two python cryptography packages, PyCrypto and Cryptography. You can find PyCrypto in https://pypi.python.org/pypi/pycrypto and Cryptography in https://pypi.python.org/pypi/cryptography

詳細說明

Task 1. 隨機生出一個 size 為 512MB+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 2 個 packages 實作出 AES-256-ECB, AES-256-CBC, AES-256-CTR, RSA-2048, SHA-512 這 5 個 algorithm. 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 2 個 packages 實作出 AES-256-ECB, AES-256-CBC, AES-256-CTR, RSA-2048, SHA-512 這 5 個 algorithm 應用在你的 random file 的時間.

甚麼該出現在你的 report 裡?

- ✧ 你的 report 該出現你如何安裝 PyCrypto and Cryptography 這 2 個 package, 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 2 個 packages 實作出 AES-256-ECB, AES-256-CBC, AES-256-CTR, RSA-2048, SHA-512 這 5 個 algorithm 的時間比較表.
- ✧ 請視這份 report 為一份教學文件, 下個學期的學弟妹將會看你的 report 來安裝與使用 PyCrypto and Cryptography 這 2 個 package, 以及看你的 report 來實作出 AES-256-ECB, AES-256-CBC, AES-256-CTR, RSA-2048, SHA-512 這 5 個 algorithm. 這樣的話, 學弟妹們將可以站在你們的經驗上, 做更多且更具難

度的作業.

- ✧ 當然他們下學期的作業就不會只有用 2 個 packages 實作出 AES-256-ECB, AES-256-CBC, AES-256-CTR, RSA-2048, SHA-512 而已, 既然已經站在你們的肩膀上了, 就會請他們往更細節更艱深的地方來探討.

該怎麼繳交 (若不符合規定則恕不接受)?

- ✧ 每一份 code 請用功能與 package 來命名. 譬如 PyCrypto +AES-256-ECB.py 就是用 PyCrypto 來實現 AES-256-ECB 的 code.
- ✧ 在 Google Drive 內新增一個資料夾, 名稱叫做「assignment1」. 所有作業上傳至 Google Drive 上, 並且將所有 code, report 都放置在「assignment1」裡面.
- ✧ 繳交截止日 2017 年 10 月 26 日 23:59:59. 可以遲交一個禮拜, 但扣 20%分數.