HW5

2019/12/19

Github 專案放置

- 此次為分組作業
- 在同一個專案下建立新資料夾 HW5

Programing Language

- C
- Python
- C++

作業繳交

- 程式碼部分 - github
- 說明文件部分 - moodle

Problem

- 實作 DSA 演算法
  - 產生 Key (p:1024 bits q:160 bits)
  - 簽署 (hash function use SHA1)
  - 驗證

請實作 DSA 演算法，簡單來說可以分成三部分，各位可以根據這三個部分去分工，一些要注意的規格我都寫在上面了，其他就照講義即可，SHA1 可以 call library

操作範例 (不用照範例 可自行設計)

Key Generation

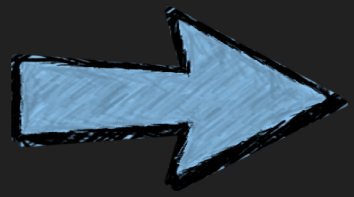
python ./DSA.py -keygen 160

Put two keys in the files

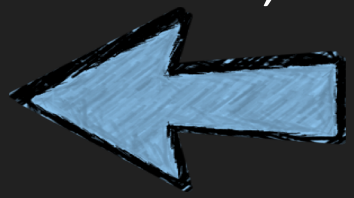
Priv Key	Pub Key
d	p q α β

Signing

python ./DSA.py -sign {message}



Return r, s



Priv Key

d

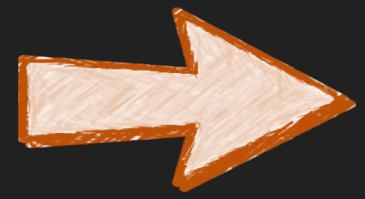
Pub Key

p q

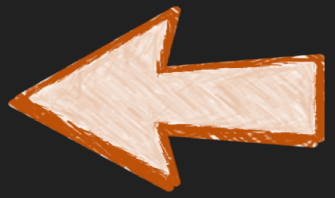
α β

Verifying a signature

python ./DSA.py -verify { message }



Return valid or invalid



Pub Key

p q

α β

Input & Output

- 如上面範例所說 可自行設計
- 測試的 Plaintext 接為可見字元 (ascii 0x21 ~ 0x7A)

說明文件部分

- 請在文件中說明
  - 分工
  - 建置環境
  - 操作方式
  - 執行過程截圖
  - 程式碼解說
  - 遇到困難與心得

注意事項

- 請寫 c 或 c++ 的同學要記得編譯出可執行檔
- 如果想再補交請寄信通知我
- 上傳說明文件時請把檔名改成 [Student ID]_HW5_report.pdf

評分標準

- 說明文件 (40%)
- 程式 (60%)