Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Bài thi cuối kỳ

Thực hành môn Mật mã học

Tháng 3/2023

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BEE SECURE
INSECLAB

A. TỔNG QUAN

1. Mục tiêu

- Đánh giá lại quá trình thực hành của sinh viên trong 5 lab thực hành

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành ngay sau khi kết thúc buổi học.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Phần mềm visual studio code

2. Hệ điều hành

- Sử dụng cả hệ điều hành linux và window để kiểm tra thuật toán.

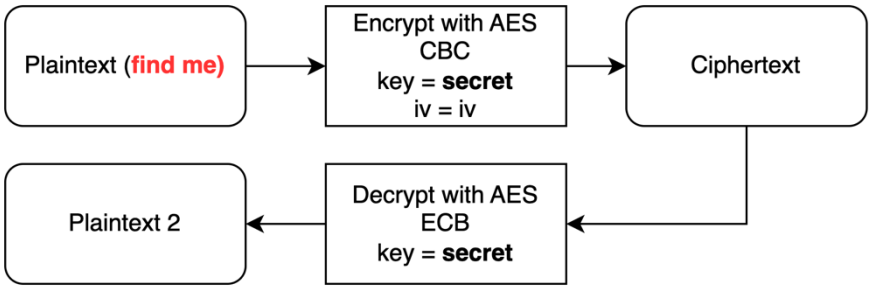
C. CÂU HỎI THỰC HÀNH

1. Thuật toán mã hoá DES

- **Bài tập 1: (1đ)** Hãy tìm ra cặp plaintext-ciphertext để khoá dưới đây trở thành khoá yếu.
- **FE FE 1F 1F FE FE 0E 0E**
- **Bài tập 2: (1đ)** Cho chương trình mã hoá **DES** bên dưới. Kết quả mã hoá được encode base64. Biết **DES** mã hoá **mode ECB** và khoá có liên quan đến khoá yếu và khoá nửa yếu. Hãy tìm ra khoá mà **mã hoá** ciphertext bên dưới ra kết quả là plaintext ban đầu.
- **Plaintext ban đầu**: "*semi weak key des - khoá nửa yếu trong des*"
- **cipher text:**
- 6MupHn98v/yhX3jSCMf+LFOVQc7iRLALzTjd5ow34a5vnoPkSmZ1MHG/wU9Elkva
- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

2. Thuật toán mã hoá AES

- **Bài tập 3: (1đ)** Các trường hợp nào nên sử dụng mode CBC, và trường hợp nào nên sử dụng mode OFB trên AES. Cho ví dụ.
- **Bài tập 4: (1đ)** Cho chương trình mã hoá AES bên dưới. Kết quả mã hoá sử dụng AES mode CBC để mã hoá và sử dụng AES mode ECB để giải mã dựa trên cipher của kết quả mã hoá. Hãy tìm ra đoạn mã rõ ban đầu của chương trình
- Mã hoá sử dụng AES-256 và Block_size = 16



- Cipher text mã hoá bằng **AES_CBC**:

  cipher =

XEkdm4AGP6oQK0OfKhN7a/fTBb+XyUMlKOHAKoPW7wUzrcbuJnj40jaCfVVilHmL
U1V/dXIltUF8dsAhC8LDBIIBhvKzDucvYRwg1HwX9zAwxmeRIq9qFs6+ei80sAzensd
BiyF36TpxPefsJRJTRJfqaO7FV6LLT20GkZrqolaKEXEzuWAB+SuWqaoB+ruVH9VPm
CH6I8PvfdDA+0bEt1XC4otSHMSDc9X5fDoUs796oPpHuJeANALNr1s9V2E+VFreZkn
225Zcldc+XeueBjyg4uy0SwJlteoYvF/tV3U=

  iv = yIwZn0RUXvlw9lxtVhCuOg==

- Mã rõ giải mã bằng **AES_ECB** (cùng key): decrypt(cipher)

  plaintext 2 =

hU+6vyyX7ZhQtxk+dtQ//OyopjjjJkvC8ZDy/Ap7EopMVGuf46GAkUaG4Fv2t88wE86uD
53Rm/JYRv47BbQa45D4ER1SSXbhXDekRVmttmrmSuOLny60WgNeWaAZZNsQY64
O91b9BWG9klpiXchPsfKyLOVSV5/50R2siVxXKzT2hBuHqjmM6wGphfy6icq3MbgSE
9ekgpdMtsdpoYObUY4T/3maWUDjnJxqb4tmvFbvfZKrlo0lOPD1jRTbrwLcWsiTpgMQ
7hRgrI85++eAhc85/gWPV/v0vS90UHPonQU=

- *Lưu ý: plaintext là dạng encode utf8. tiếng việt có dấu.*
- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

3. Thuật toán mã hoá RSA

- **Bài tập 5: (1đ)** Các tham số của public key rsa lần lượt là
- **e = 65537**
- **n =**
- 19432641663970228602454613256929114093476416053442925475633254245656442084676980241826420384564272629134502497370061822076575747111463173201148542655045316278398090385068205171950436581955137869549446126341817834795747752514975275682979945848335808044820464090400072255846712957548213211431401971264889339784897955377737194300284006994191233787440876463420303629452274099577492 8

359350793610756535979599054763670020913479914224493181176117375
077425641188006017981734325511332998105838358491786509679417739
097282284112315123568770467663376955215760444696892551143067709
099918922517643203289309445735094671434909088037 61

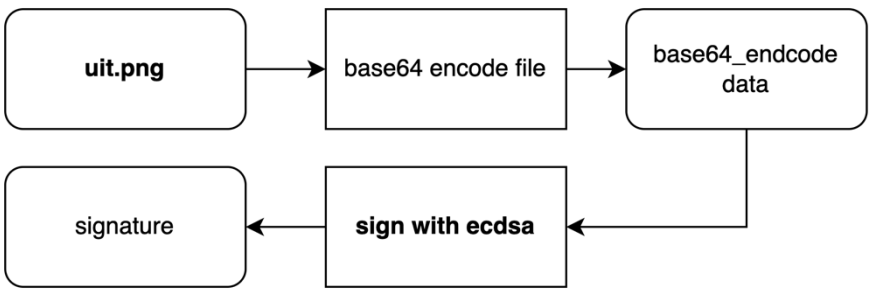
- và ciphertext là
855170488574088974430975503298702010186351242562518088813862740
360716130495382273899339168052034526559264504306866252070816936
692978169116991838127336217048867739226341396910883292327848223
658682742972787562894905848727060265815810169422220948937093367
388625828062022515347678541096638536893106420441094541551906163
528110226903722244634683086789109616809890122371823675206906129
120347833372851603600611649241830844379800492872829723685394001
060700097508405960942046873646269753641742245602862931302228779
149091138431649442359046234269522834405279144780425770698113288
270766337624238742520225606529197495296139490351 2.
- *ciphertext ở dạng long interger*
- Hãy tìm lại plaintext ban đầu (ascii).
- Biết được sau khi mã hoá thêm **2^1025-2** lần thì trả lại về ciphertext.
- **Bài tập 6: (1đ)** Luyện tập sử dụng RSA với các thông số sau.
- **Cho n =**
435227995514595233481777875128553267789518490019706910041264522
576167370450264035329257425687482934218288024104078760071937867
729665165419232294862039037539532541018791091866554026890772575
542500150368974003244421620283419245914341287587224850385960568
423695648149349495978867307820806527640140691505076087374609353
298143855991989318319669872124242201980703435385615498797284322
677624835318103731393994098910886917562724347695067095669231136
720031684292021310133061079843385444572080810544948629628974181
777140491860399469644232450319213975427311559751291837603257905
925943747171923743698060317530792349350565355167829754335569445
464792889281199869050951650062752207270084432084886661576814628
312460127436112433665026888094684183767029613461887272581286948
495000989351862729355214783631666092155446521437980264068221581
550496355873858463013338063976581480921483114034017598115462382
106048201140451953055975911628100841560325826387331926991422032

779045330472217987711669298126827082999696913345514967480677833
463901712977749379374425621167007520596686819348591909364154970
947609912147460887228457333276376257510336977082403345074258916
164127134850307837982021563565563407259490768379096274939487599
712954658915228217488835923905955229

- **e =** 13
- **cipher text =**
  476571097361060712805283430610657498271936961456822634648857175
  380529608803901802760993465949620967958626141563851005820592167
  730085060290419632039841105730979318019479078715201753887446756
  062404554684911770626043180714027744617745344458698435421380020
  840817358604995463436341736272836579615685301783159150858520879
  420080221905331503395347356296036476615978362646961605585534974
  049093004914633532819880643142080759567584600177170720817851983
  702541917483916363432538052549112656589320428839171031224774297
  390078158400291697438394384804913953729256484171251651400462750
  974928602074326662338107961433661604958026091208405652573460412
  991510712318847973519565492089103801447814243199399268480111326
  239199768353505214373833199829061482165511195427258610736723328
  680398665930829404240490185093722845938558671289607841
- Tìm plaintext ban đầu của chương trình
- Kết quả chương trình 50%
- Giải thích chi tiết: 50%

4. Thuật toán mã hoá Elliptic Curve

- **Bài tập 7:(2đ)** Cho chương trình mã hoá chữ ký bằng ECC. Hãy viết một chương trình xác thực chữ ký với các tập tin hình ảnh được cung cấp. Kiểm tra signature đính kèm nào là đúng với tập tin ban đầu.(có 10 signature cần kiểm tra)
- ECDSA<ECP, SHA1>



- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

5. Hàm băm

- **Bài tập 8:**(2đ) Luyện tập về hàm băm.
- Tìm giá trị xung đột băm (hash collision) của chương trình trong **baitap_8.py**
- *Kết quả chương trình 50%*
- *Giải thích chi tiết: 50%*

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm Code, CSDL được export và chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1.
  - Ví dụ: [NT219.K11.ANTN.1]-Lab1_1852xxxx-.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!