TRƯỜNG ĐẠI HỌC BÁCH KHOA TP.HỒ CHÍ MINH  
KHOA KHOA HỌC KỸ THUẬT VÀ MÁY TÍNH

──────────────────────── \* ───────────────────────



BÁO CÁO LAB-3

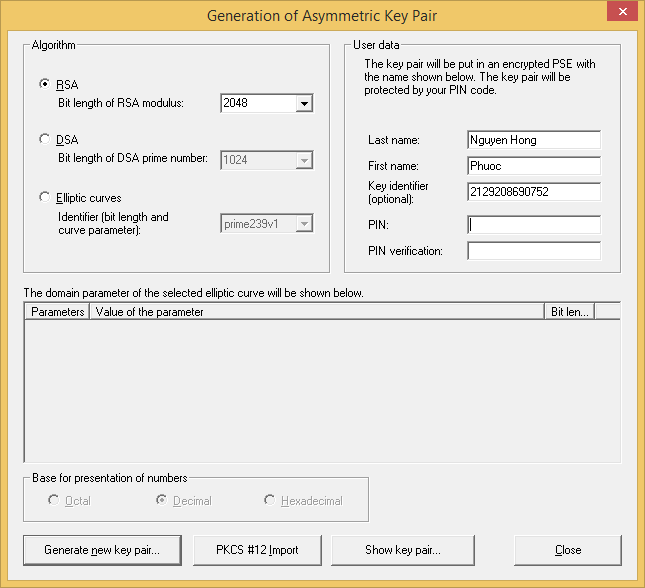
MÔN HỌC : MẬT MÃ VÀ AN NINH MẠNG

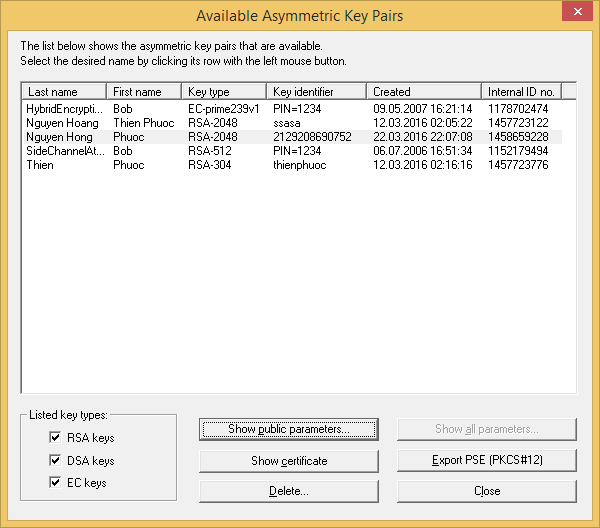
SINH VIÊN THỰC HIỆN : NGUYỄN HỒNG PHƯỚC.  
 MSSV : 51202890.  
 NHÓM : A02.  
 GIÁO VIÊN HƯỚNG DẪN : NGUYỄN NHẬT NAM.

*TP.HỒ CHÍ MINH, tháng 3 năm 2016.*

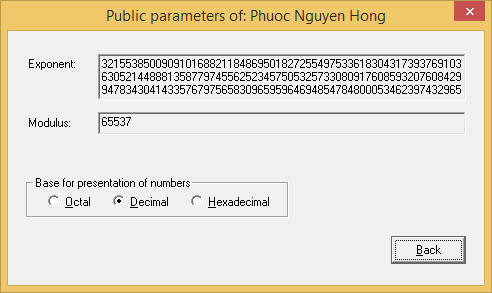
PART 1. GENERATION AND CERTIFICATION OF RSA KEYS

1.Generate a pair of RSA keys:



2.Show key pair:  


3.Show public parameters:



4.Show certificate:

Version: 2 (X.509v3-1996)

SubjectName: CN=Phuoc Nguyen Hong [1458659228], DC=cryptool, DC=org

IssuerName: CN=CrypTool CA 2, DC=cryptool, DC=org

SerialNumber: 8D:9C:53:5A:42:FB:EE:5A

Validity - NotBefore: Tue Mar 22 22:07:19 2016 (160322150719Z)

NotAfter: Wed Mar 22 22:07:19 2017 (170322150719Z)

Public Key Fingerprint: ADDD EA28 C4B8 4FE5 EEDB 027C 57D7 35C8

SubjectKey: Algorithm rsa (OID 2.5.8.1.1), Keysize = 2048

Public modulus (no. of bits = 2048):

0 FEB83F36 D808DFB8 9F0196BD C9257D8E

10 11464463 C4B62CB2 4CADB7B5 29E6ABC0

20 0DF82059 359B52B9 79D78B1B 0CE50D92

30 04550C1E 3B36007F A852262E FD6B7282

40 BFA0E679 B02E5695 AECC15AD 18549F13

50 92D7B3D6 27925F95 7A00947A 4D2B519B

60 A1400321 D11D2FF7 A512D9A7 15A9AB06

70 B9B6EB1D 601AD57E B07E5B86 51A493D8

80 381BA61C AD4CB6ED 9559969D BEC44F1D

90 B4E8530A B8AC6740 0415BB56 46123497

A0 11187ECD 26B67593 DDB1F12B 8EF6EE81

B0 F2D00C2B 8828885C CA156CC6 CA132462

C0 7C6A63C4 4AA613DF 9CD7F132 E7903C53

D0 665C7D5A 4FBE7002 9E96BDED 002D4D00

E0 66EBC596 D29F44BF A91A9036 1B381EFE

F0 AA90AD0A 7DF04AB8 734E5769 F2E8F1A3

Public exponent (no. of bits = 17):

0 010001

Certificate extensions:

Private extensions:

OID 2.206.5.4.3.2:

PrintableString:

|[Nguyen Hong][Phuoc][RSA-2048][1|

|458659228][2129208690752] |

SHA1 digest of DER code of ToBeSigned:

0 30D8B7B2 0668B1CD 265496DE 51C01C24

10 DA4BDC48

Signature: Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL

0 56080DB3 E6FC79DC 1F215758 B1B2D27C

10 C5D645A7 DBFCFC17 6F3943B2 C6400B53

20 FCB3F186 B1566D8C F92950B9 54361B3D

30 7A9EC57A B19CC10A 7977E7C1 CF5055EF

40 A741FA30 0C4FF950 5EC77E37 F56E0110

50 AA0E5245 2D6687EA 28E7DAF7 90FB5601

60 7604F8ED F5A4DFA1 A1C303B5 4B66346E

70 4DB0A0B1 CBA0BD0D 727EDBA3 81AF73F9

80 959B4923 9AA9E624 0431C035 B5692A5A

90 40FB72FE D8E8327E 8DC0DF5E AD9DBB55

A0 7145248F 6E17BCDE E7D03612 4A4760E4

B0 07B45219 B61A2FAF 46BE2D92 4445BF52

C0 373D1AFB 460000EB 159B1DE1 A0A78D39

D0 3EBB7E16 A7E2CB54 BBCF24D4 6A633BD5

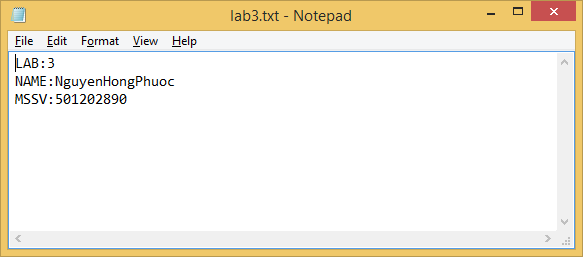
E0 D85E68F7 32797DED F334C42C B133A15C

F0 A1228FC0 295B6B7D 138DDF47 5EBD5AED

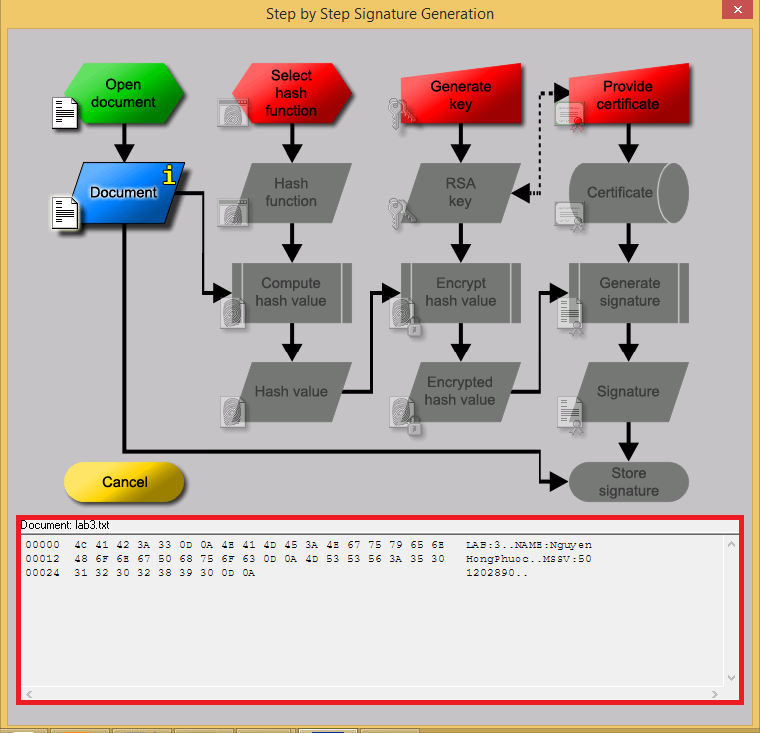
Certificate Fingerprint (MD5): AD:CF:92:88:61:F7:C6:7A:67:9B:B6:E3:59:86:B8:68

Certificate Fingerprint (SHA-1): C2B8 2CDC 08E8 CD20 F00D 4DF0 CB64 609D 5E36 01FA

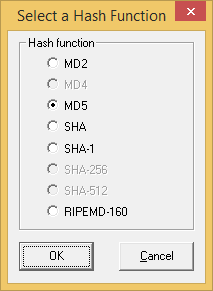
Part2. SIGNATURE DEMONSTRATION  
+ Open document : <lab3.txt>



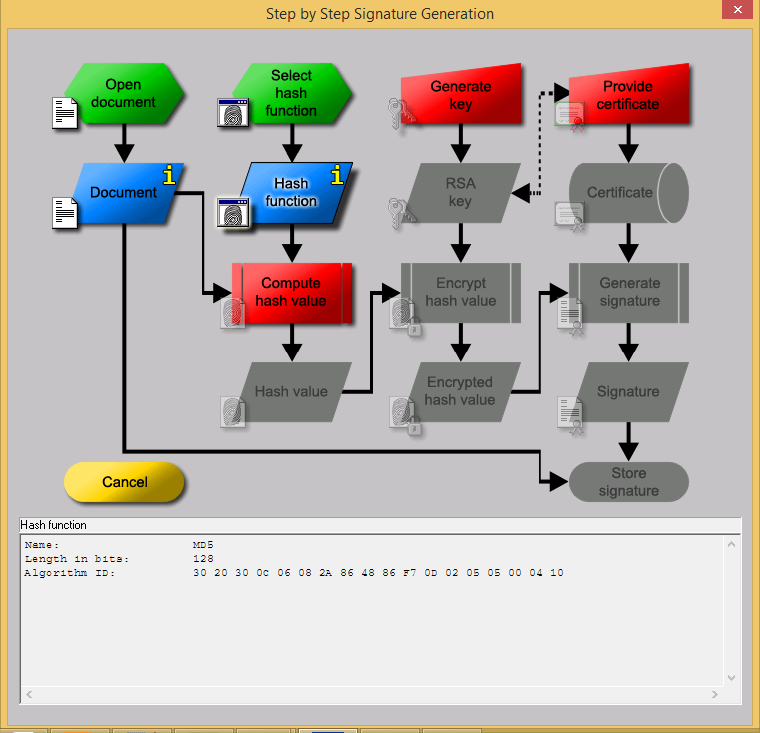
+ Document :



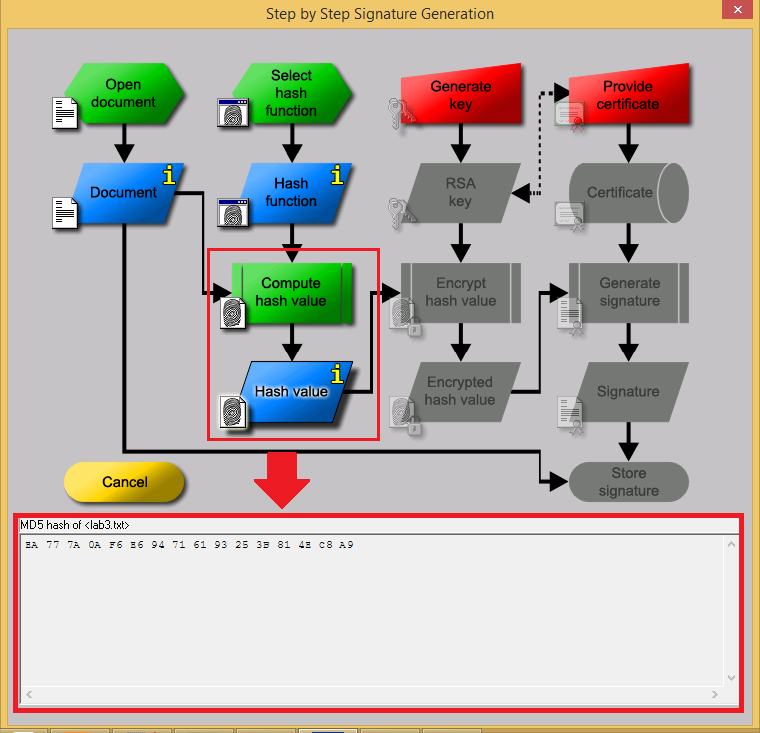
+ Select has function:



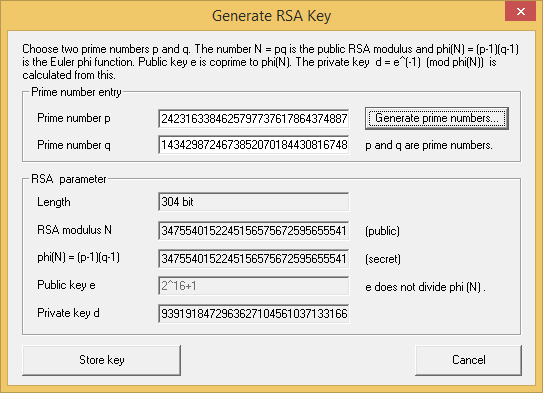
+ Hash function:

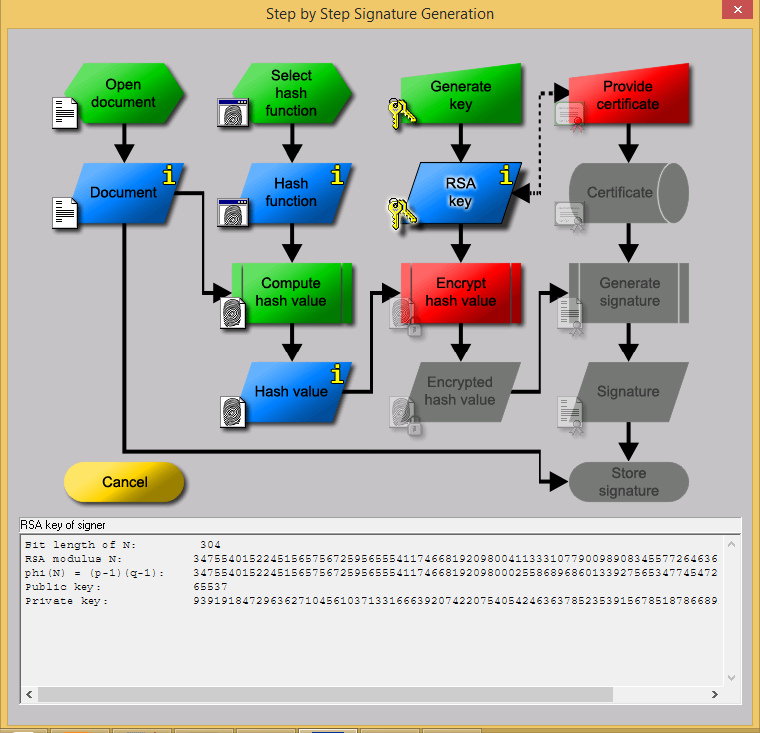


+Compute hashvalue and Hash Value:

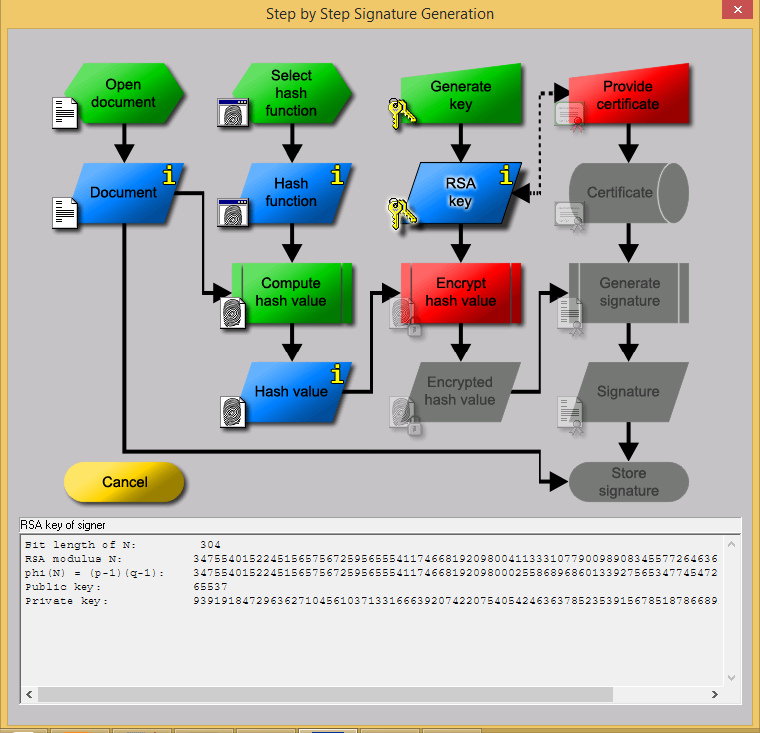


+ Generate key:

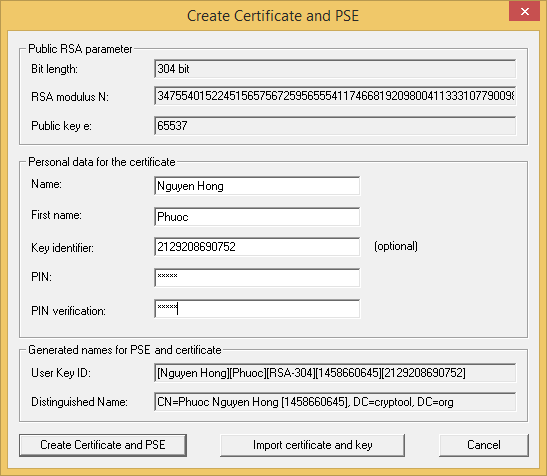
  
+ RSA Key:



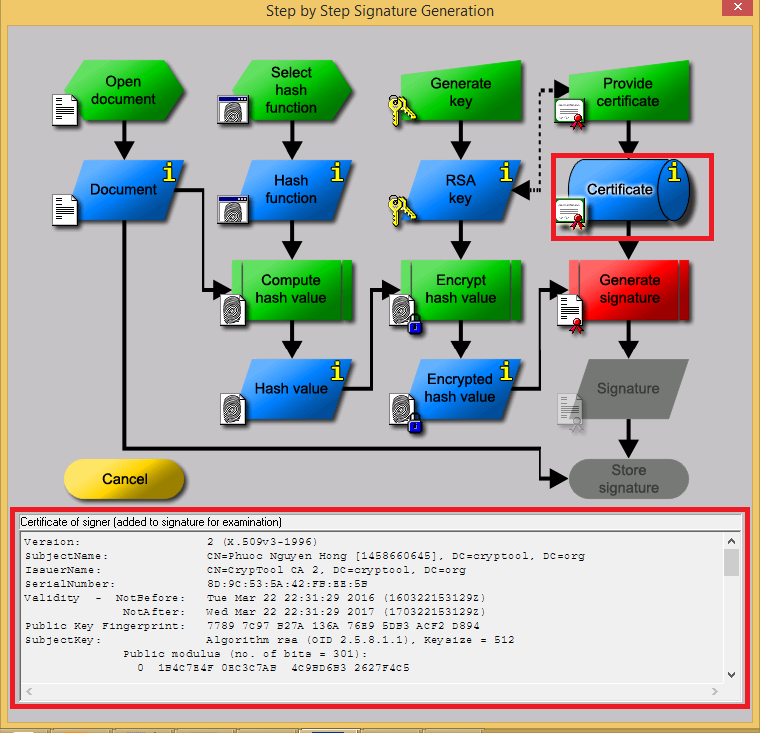
+Encrypt hash value and Encrypted has value :



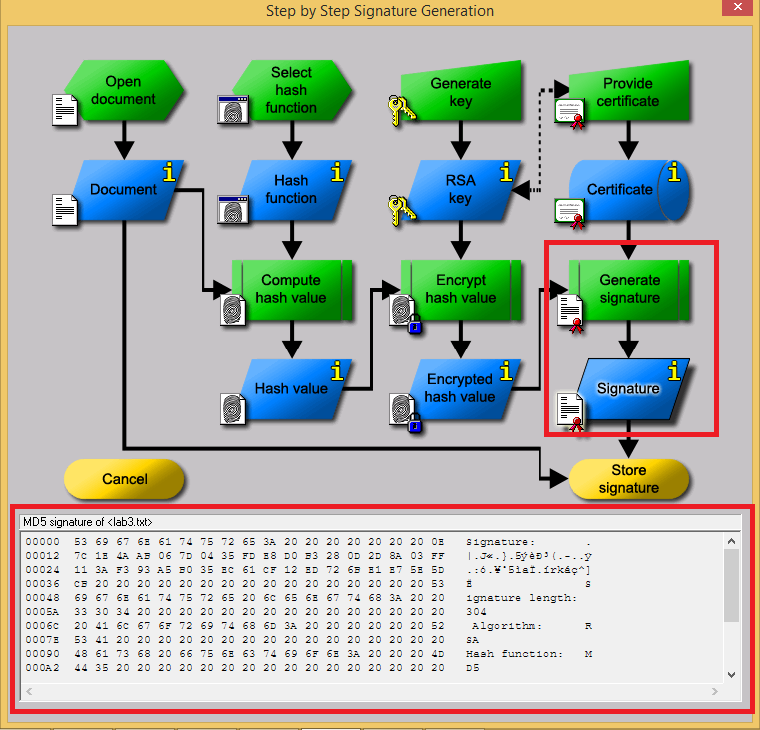
+Provide certificate:



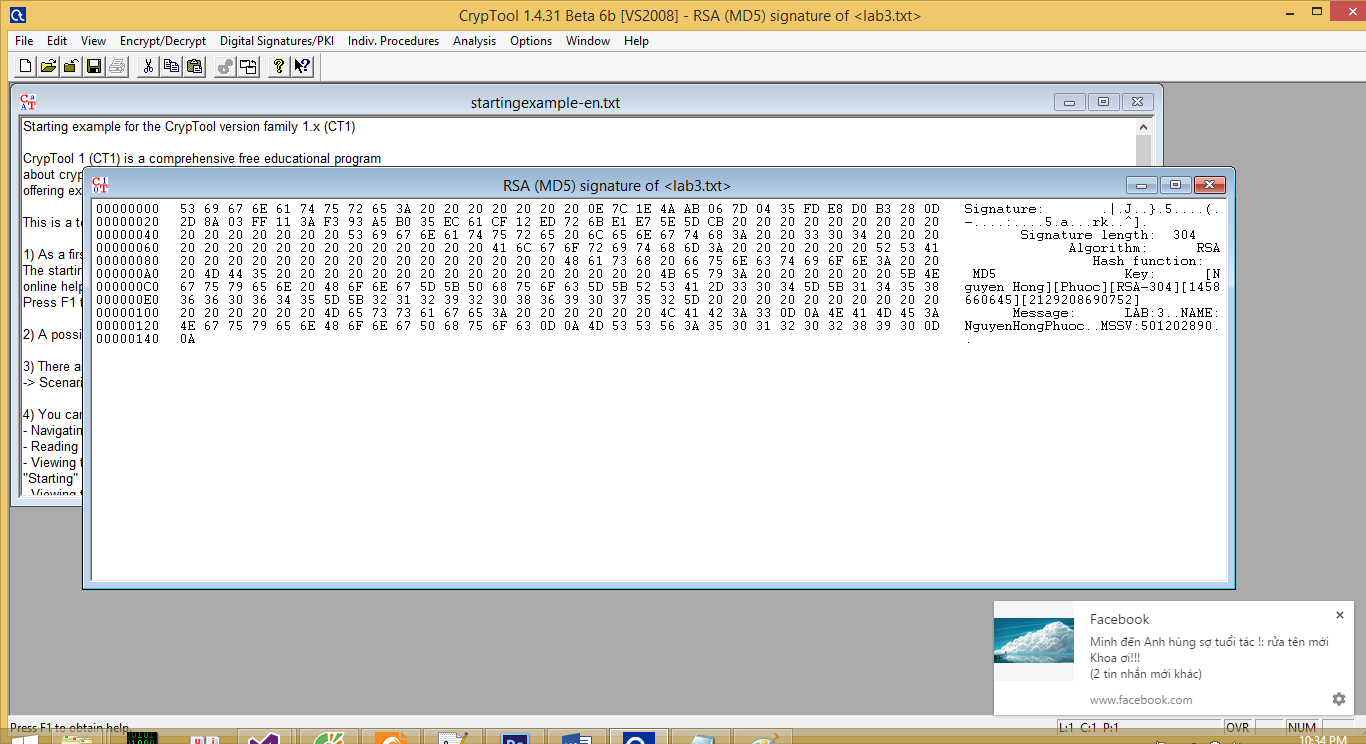
+Certificate:



+Generate signature and Signature:



+Store signature: <Cry-RSA-lab3.hex>

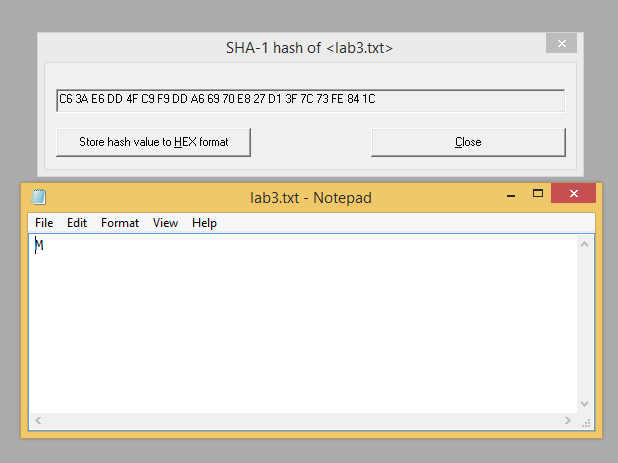


Part3. CRYPTOGRAPHY HASH FUNCTIONS

2. Consider the following hash value obtained by hashing with SHA-1 a single letter of English alphabet: C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C. Find the corresponding letter. Describe your approach. Use CrypTool to accomplish this task.

=> Kết quả : M  
=> Phương pháp : Dùng phép thử.

Indiv. Procedures -> Hash Value of File ->lab3.txt -> SHA-1.



3.Assume that you succeed in the previous task (you recover the hashed

letter). Does you success imply that that SHA-1 hash function does not satisfy oneway property? Explain your answer.

=> SHA-1 vẫn là một one-way function. Bởi vì kích thước dữ liệu ở bài trên quá nhỏ, và có thể dễ dàng suy ra bằng một vài phép thử. Nếu dữ liệu lớn thì điều này là không thể.

4. Create a new document in CrypTool by clicking on the icon “New”. Write

some text in the new document. In the main menu, under “Indiv. Procedures”

submenu select “Hash 7→ Hash Demonstration...” to open “Hash demo” window.

Modify text that appears in “Actual document” window and observe what happens

with the corresponding hash value. Explain your observation.

=> Khi thay đổi giá trị đầu vào, thì giá trị Hash lập tức thay đổi.

Inut : Nothing to write

0.00% of the bits differ (0 of 160).

newInput: Nothing to write1

54.38% of the bits differ (87 of 160) :

=> Chỉ cần thay đổi hoặc thêm 1 ký tự thì giá trị Hash thay đổi tới 54.38%. Cho thấy việc suy ngược ra input là rất khó, có độ an toàn cao