BÀI THỰC HÀNH SỐ 4

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Nguyễn Hữu Bảo**

**MSSV: 1811523**

**Phần 1. Mã xác thực thông điệp MAC**

**Câu 1:**

Messenge: Congrats on your tenth purchase! Enjoy a free cup of coffee and one pastry item on us by showing the cashier this text message!

k: NguyenHuuBao

Hash function: MD5 (dài 128 bit)

HMAC variant: H(k, m)

HMAC: D7 CB 57 D4 86 B6 B0 0D 34 B0 67 CD 2B 6B FF DA

HMAC variant: H(m, k)

HMAC: 81 36 25 C8 1E 11 C4 55 53 52 20 1D C1 29 1A 83

HMAC variant: H(k, m, k)

HMAC: 79 C1 A9 E1 7B E3 61 F2 5B AD 2B E0 60 34 1A D0

HMAC variant: H(k, m, k’)

k’: 1811523

HMAC: 62 3C 46 99 65 6E 97 D8 89 D7 D4 2E C2 FF 2A 0A

HMAC variant: H(k, H(k, m))

HMAC: 8F DF 4F FF DD 42 41 A8 FE AD F6 7B 78 DD 46 54

Hash function: SHA-1 (dài 160 bit)

HMAC variant: H(k, m)

HMAC: 10 D7 01 BB 8E 2A 40 C6 AA 00 50 D3 B5 42 88 61 7B DB BF 73

HMAC variant: H(m, k)

HMAC: 60 44 DD F9 8E 7F FE B4 66 31 D9 A8 CE 9C 5E 4A 62 23 8D 3D

HMAC variant: H(k, m, k)

HMAC: 3A BC BB 33 F9 94 92 62 8B 1E 13 09 32 E7 CD 07 55 67 08 C4

HMAC variant: H(k, m, k’)

k’: 1811523

HMAC: 68 09 54 D5 02 22 B3 B1 DD 97 37 B1 DC 86 BE FF B6 97 A0 62

HMAC variant: H(k, H(k, m))

HMAC: F3 09 2B B9 76 EE 1F 6B A3 78 C5 65 DC 41 9B C5 52 E0 68 60

Hash function: SHA-256 (dài 256 bit)

HMAC variant: H(k, m)

HMAC: 87 E0 3B E6 8D 13 0B 8D 37 01 F7 10 FA C5 51 1D 44 7D 97 EF 5B 1E 05 04 9B 82 E5 B1 87 FF 90 43

HMAC variant: H(m, k)

HMAC: 68 DF B0 34 6C 23 C5 BC 89 05 7C 72 BB 83 69 2D 16 43 B1 7A 93 07 38 BD DF 30 10 F5 65 AB 4D 9B

HMAC variant: H(k, m, k)

HMAC: 9A BA C0 FE F2 CA 63 7C F5 04 37 DF 49 2A 15 D0 96 96 43 F6 F3 FF 54 C9 8F 5A D4 22 3F 4C 88 BE

HMAC variant: H(k, m, k’)

k’: 1811523

HMAC: A5 D7 FE 4A E0 44 59 7B 52 FE 02 BB 92 B2 AA 36 80 37 82 20 5D B5 93 D4 EC 28 55 87 4F 5F 69 DA

HMAC variant: H(k, H(k, m))

HMAC: 6C EA 73 8E 70 D3 C1 06 20 03 AA 3C EF D0 B6 97 55 62 1E 05 90 95 0D 65 E1 0C D2 35 2E 92 EC BF

Hash function: SHA-512 (dài 512 bit)

HMAC variant: H(k, m)

HMAC: 6B CF 72 C0 1A 84 B6 43 43 BC 58 5D D7 A5 71 38 D0 8D C4 6B A2 4C 0F 12 B0 F1 96 AD 2C 57 7A 61 D9 13 E4 10 DD D9 D4 08 E4 48 F0 24 12 EF C6 A0 15 43 CE 4C 01 00 65 62 02 28 E8 DD 6D 33 1F 23

HMAC variant: H(m, k)

HMAC: 35 0A FA AA 92 28 A7 79 BD F7 E9 DB 40 42 A0 5A 77 01 5C 9C 9E 09 90 7D 78 27 69 D9 3F BE BA D5 8D 3B 9C 89 57 92 8B 26 A1 5A 77 C9 E5 7C 91 18 18 4B E5 6F FD 56 88 60 7C 39 0E A2 61 FC D0 E5

HMAC variant: H(k, m, k)

HMAC: 1F 00 F3 D4 7E 7A BD 32 B3 57 AC 67 7D 0D 67 DD B4 9E 6C D8 04 41 34 C4 DF 76 4B 31 2F 4C 84 18 E1 0C 60 E0 1C 79 93 12 D8 FC 2A 0E 5F AD BA A0 3A 69 A0 F8 5F F0 AC A0 70 E2 B7 20 A5 03 3C 60

HMAC variant: H(k, m, k’)

k’: 1811523

HMAC: BD FC 9D 95 C0 78 84 D0 CD FE 73 36 14 94 7C E7 41 61 D9 9C C6 C1 42 65 13 F5 FA AA A2 89 37 43 16 23 DC BC 50 9C 7D 0D 8A E7 67 B2 9C 27 97 C6 F6 CA B9 9B EF 15 E9 E1 F3 1A CA A5 64 46 C9 F1

HMAC variant: H(k, H(k, m))

HMAC: 54 70 EF 7A 23 7B 48 9B C0 FB C4 38 65 78 1A AD 45 B7 84 47 98 74 83 C9 F4 29 70 AE 6D FD 2A 3E 79 C9 6A 5F 16 F9 8E 5E 37 B9 F0 AA D3 F5 81 97 1F 88 FC ED A1 77 0F 71 EA 78 AD F6 63 33 B8 20

3^2086 = 81\*729^347 /440

81\* 289^347

81\*289 \* 83521^173

81\*289\*361^173

81\*289\*361\*130321^86

81\*289\*361\*401^43

81\*289\*361\*401\*201\*81\*401^2

**Câu 2:**

Tấn công ngày sinh nhật

Tấn công brute-force

Tấn công phân tích mã

**Câu 3:**

MAC:

Được sử dụng để đảm bảo tính xác thực và toàn vẹn.

Cách tạo: MAC = CK(M)

Cô đọng một thông điệp M có chiều dài thay đổi dùng một khóa bí mật K thành một mã xác thực có chiều dài cố định.

Là một hàm một chiều (nhiều – một): Nhiều thông điệp có cùng MAC nhưng tìm kiếm chúng rất khó khăn

Hash:

Được sử dụng để đảm bảo

tính toàn vẹn.

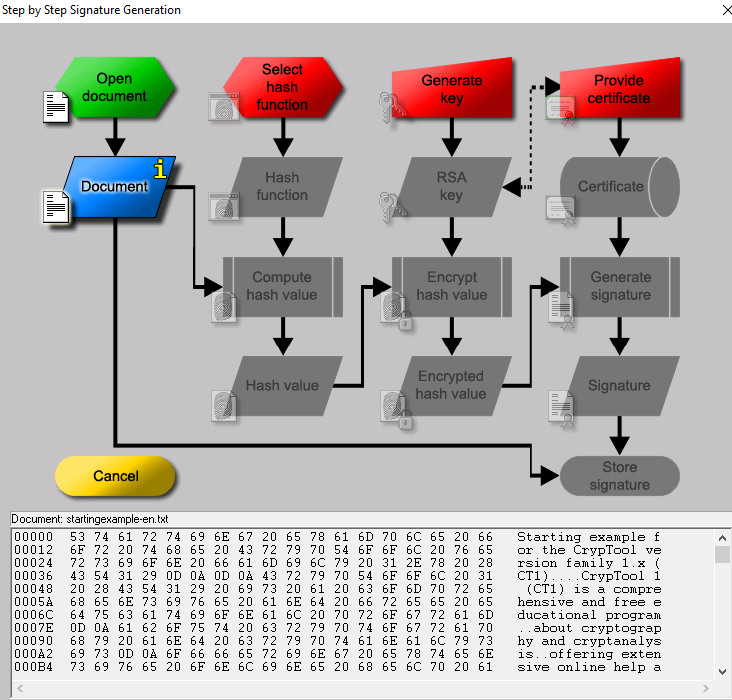
Cách tạo: h = H(M)

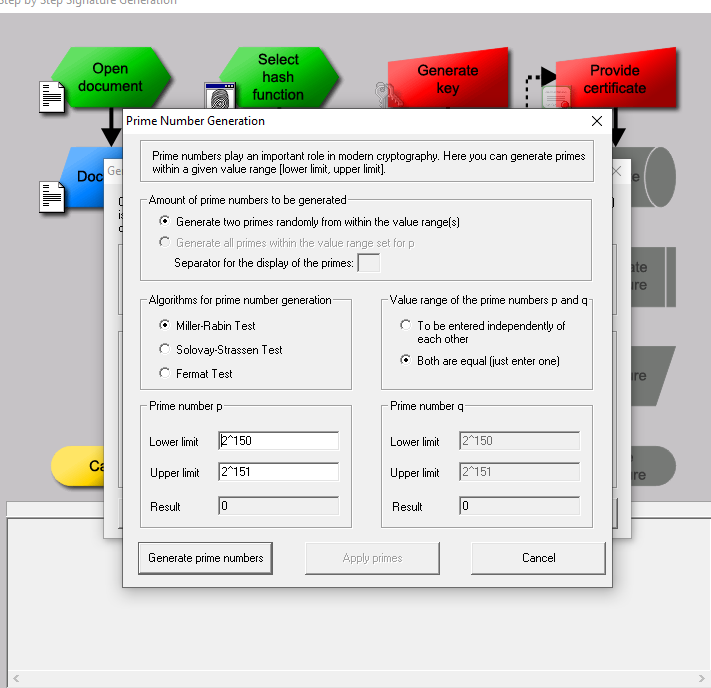
Cô đọng một thông điệp M có chiều dài thay đổi thành một thông điệp có chiều dài cố định.

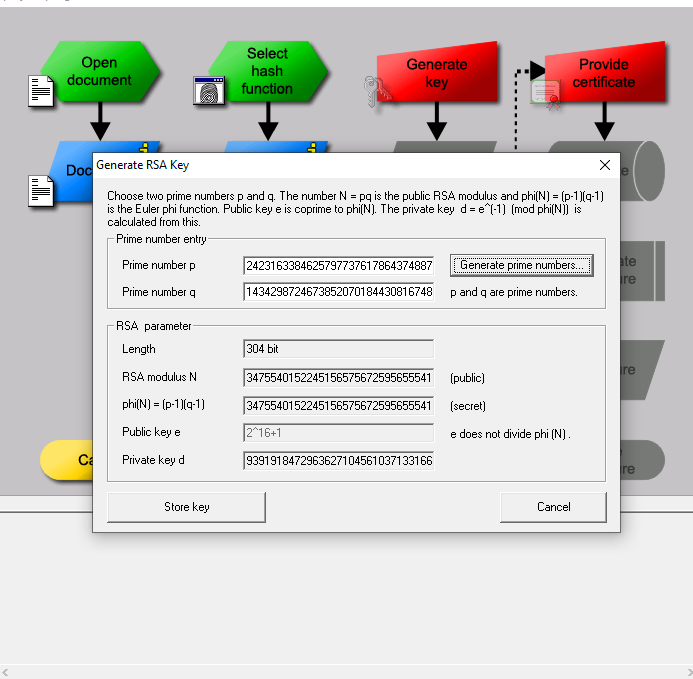
Là một hàm một chiều (nhiều – một): Nhiều thông điệp có cùng H nhưng tìm kiếm chúng rất khó khăn

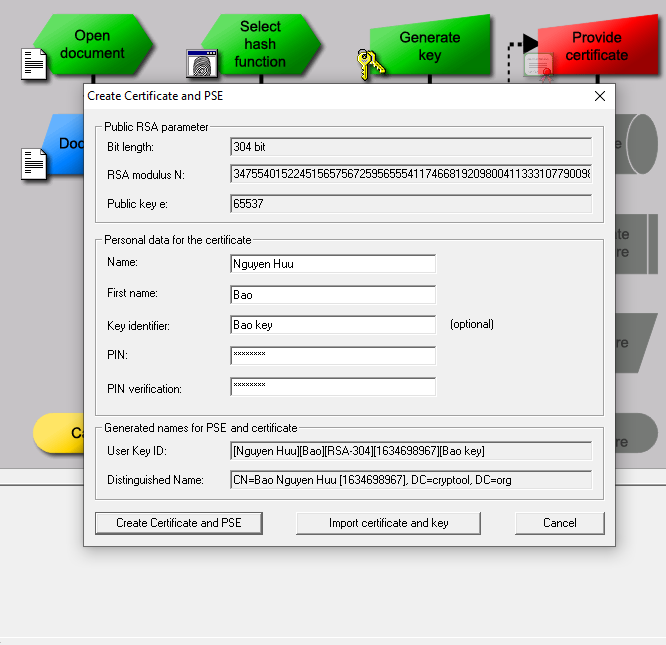
**Phần 2. Chữ ký số**

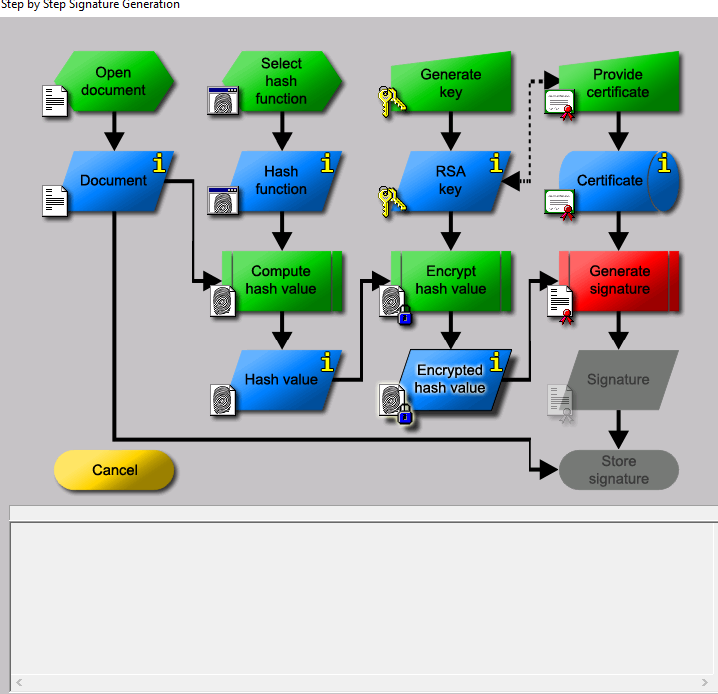
**Câu 1:**

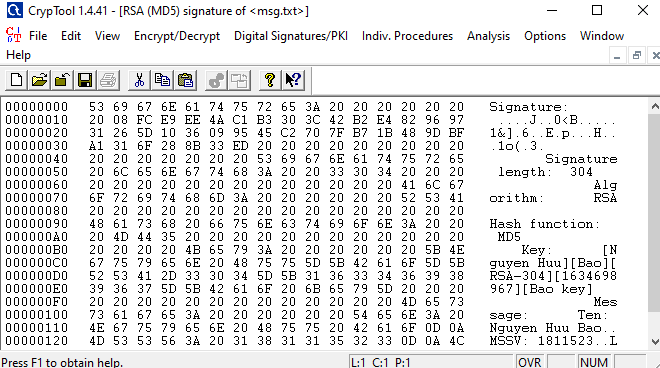












**Câu 2:**

Các yêu cầu của chữ ký số

Phải phụ thuộc trên thông điệp được ký.

Phải sử dụng thông tin duy nhất từ người gửi để tránh giả mạo và từ chối.

Phải tương đối dễ dàng để tạo.

Phải tương đối dễ dàng để nhận biết và xác minh

Không khả thi trong tính toán để giả mạo

Lưu trữ chữ ký số trong thực tế

**Câu 3:**

Nếu một người có thể biết khóa của MAC có thể tạo ra 2 thông điệp cùng MAC

Chữ ký số là một cơ chế xác thực nhằm xác nhận danh tính của người tạo ra thông điệp và chống thoái thác về xuất xứ (giải quyết tranh chấp). Chữ ký số được tính toán trên giá trị băm của thông điệp và mã hóa bằng khóa riêng của người gửi.