TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11495-2:2016
ISO/IEC 9797-2:2011

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - MÃ XÁC THỰC THÔNG ĐIỆP (MAC) - PHẦN 2: CƠ CHẾ SỬ DỤNG HÀM BĂM CHUYÊN DỤNG

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

HÀ NỘI - 2016

Mục lục **Trang**

Lời nói đầu

TCVN 11495-2:2016 hoàn toàn tương đương với ISO/IEC 9797-2:2011.

TCVN 11495-2:2016 do Tiểu ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC1/ SC 27 *Kỹ thuật an ninh* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11495 (ISO/IEC 9797) *Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác thực thông điệp (MAC)* gồm các tiêu chuẩn sau:

- Phần 1: Cơ chế sử dụng mã khối;
- Phần 2: Cơ chế sử dụng hàm băm chuyên dụng;
- Phần 3: Cơ chế sử dụng hàm băm phổ biến;

Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC) - Phần 2: Cơ chế sử hàm băm chuyên dụng

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

1 Phạm vi áp dụng

Tiêu chuẩn này quy định ba thuật toán MAC mà sử dụng một khóa bí mật và một hàm băm (hoặc hàm vòng của nó) cùng với một kết quả *n*-bit để tính ra MAC có *m*-bit. Các cơ chế này có thể được sử dụng như các cơ chế toàn vẹn dữ liệu để xác minh rằng dữ liệu đã không bị thay đổi theo một cách trái phép. Chúng cũng có thể được sử dụng như các cơ chế xác thực thông điệp để đảm bảo rằng một thông điệp đã được khởi tạo bởi một thực thể có nắm giữ khóa bí mật. Độ mạnh của các cơ chế toàn vẹn dữ liệu và xác thực thông điệp phụ thuộc vào entropy và độ bí mật của khóa, vào độ dài (tính theo bit) *n* của mã băm được tạo ra bởi hàm băm, vào độ mạnh của hàm băm, vào độ dài (tính theo bit) *m* của MAC và vào cơ chế cụ thể.

Ba cơ chế được quy định trong tiêu chuẩn này dựa trên các hàm băm chuyên dụng được quy định trong ISO/IEC 10118-3. Cơ chế thứ nhất được biết đến là MDx-MAC. Nó gọi hàm băm một lần, nhưng thực hiện một sửa đổi nhỏ đối với hàm vòng trong hàm băm bằng cách cộng một khóa vào các hằng số cộng tính trong hàm vòng. Cơ chế thứ hai được biết đến là HMAC. Nó gọi hàm băm hai lần. Cơ chế thứ ba là một biến thể của MDx-MAC, nhận đầu vào chỉ là các chuỗi ngắn (nhiều nhất 256 bit). Cơ chế này cho hiệu năng cao hơn đối với các ứng dụng chỉ làm việc với chuỗi dữ liệu đầu vào ngắn.

Tiêu chuẩn này có thể được áp dụng cho các dịch vụ an toàn của kiến trúc, quy trình, ứng dụng an toàn bất kỳ.

CHÚ THÍCH Khung cơ cấu chung để cung cấp các dịch vụ toàn vẹn được chỉ ra trong ISO/IEC 10181-6 [5].

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions (Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng).*

ISO/IEC 10118-3:2004/Amd.1:2006, Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions – *Amendment 1: Dedicated Hash-Function 8 (SHA-224) (Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm – Phần 3: Hàm băm chuyên dụng – Sửa đổi 1: Hàm băm chuyên dụng 8 (SHA-224))*.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau đây.

3.1

khối (block)

chuỗi bit có độ dài L_1, tức là độ dài của đầu vào thứ nhất của hàm vòng.

[ISO/IEC 10118-3]

3.2

hàm băm kháng va chạm (collision-resistant hash-function)

hàm băm thỏa mãn tính chất sau:

- về mặt tính toán không thể tìm được bất kỳ hai đầu vào khác nhau mà ánh xạ đến cùng một đầu ra.

[ISO/IEC 10118-3]

3.3

entropy (entropy)

tổng lượng thông tin được cung cấp bởi một tập các bit, đại diện của nỗ lực công việc cần có cho kẻ thù địch đủ để có thể tái tạo cùng tập các bit đó.

[ISO/IEC 18032]

3.4

chuỗi dữ liệu đầu vào (input data string)

chuỗi các bit làm đầu vào cho hàm băm.

3.5

mã băm (hash-code)

chuỗi các bit là đầu ra của hàm băm.

[ISO/IEC 10118-1]

3.6

hàm băm (hash-function)

hàm ánh xạ các chuỗi bit đầu vào đến các chuỗi bit đầu ra có độ dài cố định, thỏa mãn hai tính chất sau:

- đối với một đầu ra cho trước, về mặt tính toán không thể tìm được một đầu vào ánh xạ tới đầu ra đó;
- đối với một đầu vào cho trước, về mặt tính toán không thể tìm được một đầu vào thứ hai mà ánh xạ tới cùng đầu ra.

[ISO/IEC 10118-1]

3.7

giá trị khởi tạo (initializing value)

giá trị được sử dụng để xác định điểm khởi đầu của hàm băm.

[ISO/IEC 10118-1]

3.8

khóa thuật toán MAC (MAC algorithm key)

khóa dùng để điều khiển hoạt động của một thuật toán MAC.

[TCVN 11495-1(ISO/IEC 9797-1)]

3.9

Mã Xác thực Thông điệp (Message Authentication Code)

MAC

chuỗi các bit là đầu ra của một thuật toán MAC.

CHÚ THÍCH Một mã MAC đôi khi được gọi là một giá trị kiểm tra mật mã (xem ví dụ ISO 7498-2 [1]).

[TCVN 11495-1(ISO/IEC 9797-1)]

3.10

thuật toán Mã Xác thực Thông điệp (Message Authentication Code algorithm)

thuật toán MAC (MAC algorithm)

thuật toán để tính ra một hàm ánh xạ các chuỗi bit và một khóa bí mật thành các chuỗi bit có chiều dài cố định, thỏa mãn hai tính chất sau:

- đối với khóa bất kỳ và chuỗi đầu vào bất kỳ, hàm có thể tính được một cách hiệu quả;
- đối với khóa cố định bất kỳ, khi không cho biết thông tin về khóa trước về mặt tính toán là không thể tính ra giá trị của hàm trên bất kỳ chuỗi đầu vào mới nào, thậm chí khi đã biết thông tin về tập chuỗi đầu vào và các giá trị hàm tương ứng, trong đó giá trị của chuỗi đầu vào thứ i có thể được chọn sau khi quan sát $i-1$ giá trị hàm đầu tiên (đối với số nguyên $i > 1$).

CHÚ THÍCH 1 Thuật toán MAC đôi khi được gọi là hàm kiểm tra mật mã (xem ví dụ trong ISO/IEC 7498-2 [1]).

CHÚ THÍCH 2 Khả năng tính toán phụ thuộc vào các yêu cầu và môi trường an toàn do người dùng quy định.

[TCVN 11495-1(ISO/IEC 9797-1)]

3.11

biến đổi đầu ra (output transformation)

hàm được áp dụng tại điểm cuối thuật toán MAC, trước phép toán cắt ngắn.

[TCVN 11495-1(ISO/IEC 9797-1)]

3.12

đệm (padding)

thêm các bit bổ sung vào một chuỗi dữ liệu.

[ISO/IEC 10118-1]

3.13

hàm vòng (round-function)

hàm biến đổi hai chuỗi nhị phân có độ dài L_1 và L_2 thành một chuỗi nhị phân có độ dài L_2.

CHÚ THÍCH 1 Hàm này được sử dụng lặp như một phần của hàm băm, trong đó kết hợp một chuỗi dữ liệu có độ dài L_1 với đầu ra trước đó có độ dài L_2.

[ISO/IEC 10118-1]

CHÚ THÍCH 2 Hàm này cũng được tham chiếu như hàm nén trong một bản mô tả hàm băm cụ thể.

3.14

độ mạnh an toàn (security strength)

con số tương ứng với lượng công việc (tức là số lượng phép toán) cần có để phá vỡ một thuật toán hoặc hệ thống mật mã.

CHÚ THÍCH Độ mạnh an toàn được quy định theo bit, và là một giá trị cụ thể từ tập {80, 112, 128, 192, 256}. Độ mạnh an toàn bằng b bit có nghĩa là khoảng 2^b phép toán cần có để phá vỡ hệ thống.

3.15

từ (word)

chuỗi có 32 bit được sử dụng trong các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8, hoặc chuỗi có 64 bit được sử dụng trong các Hàm băm Chuyên dụng 5 và 6 của ISO/IEC 10118-3.

[ISO/IEC 10118-3]

4 Ký hiệu và giải thích

Tiêu chuẩn này sử dụng các ký hiệu và giải thích đã định nghĩa trong TCVN 11495-1(ISO/IEC 9797-1) [3]:

D	Chuỗi dữ liệu đầu vào, tức là chuỗi dữ liệu là đầu vào cho thuật toán MAC.
m	Độ dài (theo bit) của MAC.
q	Số các khối trong chuỗi dữ liệu đầu vào D sau quá trình đệm và phân tách
j ~X	Chuỗi nhận được từ chuỗi X bằng cách lấy j bit bên trái nhất của X.
$X \oplus Y$	Phép XOR của các chuỗi bit X và Y.
$X \| \| Y$	Phép ghép nối chuỗi bit X và Y (theo thứ tự này).
:=	Ký hiệu định nghĩa phép toán "đặt bằng với" được sử dụng trong các đặc tả thủ tục của các thuật toán MAC, trong đó chỉ ra giá trị của chuỗi ở bên trái của ký hiệu sẽ được làm bằng với giá trị của biểu thức ở bên phải của ký hiệu

Đối với mục đích của tiêu chuẩn này, các ký hiệu và giải thích sau được áp dụng:

$\overline{D}$	Chuỗi dữ liệu đã được đệm
h	Hàm băm
h'	Hàm băm h có các hằng số đã sửa đổi và giá trị IV đã sửa đổi.
$\overline{h}$	Hàm băm h được đơn giản hóa không có phép đệm và gắn thêm độ dài, không cắt ngắn đầu ra hàm vòng (L_2 bit) về L_H bit bên trái nhất.

CHÚ THÍCH 1 $\bar{h}$ Chỉ được áp dụng cho các chuỗi đầu vào có độ dài là bội nguyên dương của L_1.

CHÚ THÍCH 2 Đầu ra của $\bar{h}$ Phải là L_2 bit thay cho L_H bit; đặc biệt, trong các Hàm băm Chuyên dụng 6 và 8 được định nghĩa trong ISO/IEC 10118-3, L_H luôn nhỏ hơn L_2.

H', H'' Các chuỗi có L_2 bit được sử dụng trong tính toán thuật toán MAC để lưu trữ kết quả trung gian.

IV', IV_1, IV_2 Các giá trị khởi đầu.

k Độ dài (tính theo bit) của khóa của thuật toán MAC.

K Khóa bí mật của thuật toán MAC.

K', k_0, k_1, k_2, $\overline{K}$, $\overline{K}_1$, $\overline{K}_2$ Các khóa bí mật được dẫn xuất của thuật toán mac .

KT Chuỗi đầu vào thứ nhất của hàm ϕ' được sử dụng trong bước biến đổi đầu ra của Thuật toán MAC 1.

$\overline{L}$ Chuỗi bit mã hóa độ dài thông điệp trong Thuật toán MAC 3.

$OPAD$, $IPAD$ Các chuỗi hằng số được sử dụng trong Thuật toán MAC 2.

R, S_0, S_1, S_2 Các chuỗi hằng số được sử dụng trong tính toán các hằng số cho Thuật toán MAC 1 và Thuật toán MAC 3.

T_0, T_1, T_2 Các chuỗi hằng số được sử dụng trong dẫn xuất khóa cho Thuật toán MAC 1 và Thuật toán MAC 3.

U_0, U_1, U_2 Các chuỗi hằng số được sử dụng trong dẫn xuất khóa cho Thuật toán MAC 1 và Thuật toán MAC 3.

ϕ' Hàm vòng cùng với các hằng số được sửa đổi.

$K_1[i]$ Từ thứ i của chuỗi K_1, tức là $K_1 = K_1[0] \,||\, K_1[1] \,||\, K_1[2] \,||\, K_1[3]$

Tiêu chuẩn này sử dụng các ký hiệu và giải thích sau đã được định nghĩa trong ISO/IEC 10118-1.

H Mã băm

IV Giá trị khởi đầu

L_X Độ dài (tính theo bit) của chuỗi bit X

Tiêu chuẩn này sử dụng các ký hiệu và giải thích sau đã được quy định trong ISO/IEC 10118-3.

C_i, C_i' Các từ là hằng số được sử dụng trong các hàm vòng

L_1 Độ dài (tính theo bit) của chuỗi đầu vào thứ nhất trong số hai chuỗi đầu vào cho hàm vòng ϕ

L_2 Độ dài (tính theo bit) của chuỗi đầu vào thứ hai trong số hai chuỗi đầu vào cho hàm vòng ϕ, của chuỗi đầu ra từ hàm vòng ϕ và của IV.

w Độ dài (tính theo bit) của một từ; w là 32 khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8 của ISO/IEC 10118-3, và w bằng 64 khi sử dụng các Hàm băm Chuyên dụng 5 và 6 của ISO/IEC 10118-3.

ϕ Hàm vòng, tức là, nếu X và Y là các chuỗi bit có các độ dài tương ứng L_1 và L_2, thì $\phi(X, Y)$ là chuỗi nhận được bằng cách áp dụng ϕ vào X và Y.

Ψ Phép toán cộng modulo 2^w, trong đó w là số các bit trong một từ. Cho nên, nếu A và B là các từ, thì $A \Psi B$ là từ nhận được bằng cách xử lý A và B như các biểu diễn nhị phân

của các số nguyên và tính tổng của chúng theo modulo 2^w, và kết quả được ràng buộc nằm giữa 0 và 2^w - 1 bao gồm các đầu mút. Giá trị của w là 32 trong các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8 và bằng 64 trong các Hàm băm Chuyên dụng 5 và 6.

5 Các yêu cầu

Người dùng muốn áp dụng một thuật toán MAC trong tiêu chuẩn này phải lựa chọn:

- Một thuật toán MAC trong số các thuật toán đã được quy định trong các Điều 6, 7 và 8;
- Một hàm băm chuyên dụng từ các hàm đã được chỉ ra trong ISO/IEC 10118-3;
- Độ dài (tính theo bit) m của MAC.

CHÚ THÍCH 1 Việc sử dụng của các Thuật toán MAC 1 và 3 cùng với Hàm băm Chuyên dụng 7 của ISO/IEC 10118-3 không được chỉ ra trong tiêu chuẩn này.

Thỏa thuận trên các lựa chọn này trong số những người dùng là cần thiết cho việc sử dụng cơ chế toàn vẹn dữ liệu.

Khóa K được sử dụng trong thuật toán MAC phải có entropy thỏa mãn hoặc vượt quá độ mạnh an toàn được cung cấp bởi thuật toán MAC.

CHÚ THÍCH 2 Trong mọi trường hợp, khóa K của thuật toán MAC phải được chọn sao cho mọi khóa có thể là khóa được chọn một cách xấp xỉ bằng nhau.

Đối với các Thuật toán MAC 1 và 2, độ dài m của MAC phải là một số nguyên dương nhỏ hơn hoặc bằng với độ dài của mã băm L_H. Đối với Thuật toán MAC 3, độ dài m của MAC sẽ là một số nguyên dương nhỏ hơn hoặc bằng với một nửa độ dài của mã băm, tức là, $m \leq L_H/2$.

Đối với các Thuật toán MAC 1 và 2, độ dài tính theo bit của chuỗi dữ liệu đầu vào D nhiều nhất là $2^{64} - 1$ khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8, và nhiều nhất là $2^{128} - 1$ khi sử dụng các Hàm băm Chuyên dụng 5 và 6. Đối với Thuật toán MAC 2, nó nhiều nhất bằng $2^{256} - 1$ khi sử dụng Hàm băm Chuyên dụng 7. Đối với Thuật toán MAC 3, nó nhiều nhất là 256.

Việc lựa chọn một thuật toán MAC cụ thể, hàm băm chuyên dụng và giá trị cho m là nằm ngoài phạm vi của tiêu chuẩn này.

CHÚ THÍCH 3 Các lựa chọn này ảnh hưởng mức an toàn của thuật toán MAC. Xem thêm thông tin chi tiết tại Phụ lục C.

Khóa được sử dụng để tính và xác minh MAC cần phải giống nhau. Nếu chuỗi dữ liệu đầu vào cũng được mã hóa, thì khóa được sử dụng để tính MAC phải khác với khóa đã được sử dụng để mã hóa.

CHÚ THÍCH 4 Được coi là thực hành mật mã tốt phải có các khóa độc lập cho tính bảo mật và tính toàn vẹn dữ liệu.

6 Thuật toán MAC 1

CHÚ THÍCH 1 Điều này mô tả về MDx-MAC [9] cùng với các Hàm băm Chuyên dụng 1-6 và 8. Bảng 1 chỉ ra các tên thường được biết đến của MDx-MAC cùng với từng hàm băm chuyên dụng riêng rẽ.

Bảng 1 – Thuật toán MDx-MAC cùng với các Hàm băm Chuyên dụng khác nhau.

Hàm băm Chuyên dụng	Thuật toán MDx-MAC cũng được biết đến như
Hàm băm Chuyên dụng 1	RIPEMD-160-MAC
Hàm băm Chuyên dụng 2	RIPEMD-128-MAC
Hàm băm Chuyên dụng 3	SHA-1-MAC
Hàm băm Chuyên dụng 4	SHA-256-MAC
Hàm băm Chuyên dụng 5	SHA-512-MAC
Hàm băm Chuyên dụng 6	SHA-384-MAC
Hàm băm Chuyên dụng 8	SHA-224-MAC

CHÚ THÍCH 2 Việc sử dụng Thuật toán MAC 1 cùng Hàm băm Chuyên dụng 7 của ISO/IEC 10118-3 không được quy định trong tiêu chuẩn này.

Thuật toán MAC 1 đòi hỏi một lần áp dụng của hàm băm để tính giá trị MAC, nhưng yêu cầu các hằng số trong hàm vòng tương ứng được sửa đổi.

Hàm băm phải được chọn từ các Hàm băm Chuyên dụng 1 - 6 trong ISO/IEC 10118-3:2004, và Hàm băm Chuyên dụng 8 trong ISO/IEC 10118-3:2004/Amd.1:2006.

Độ dài theo bit của khóa k nhiều nhất là 128 bit.

6.1 Mô tả của Thuật toán MAC 1

Thuật toán MAC 1 bao gồm 5 bước sau: mở rộng khóa, sửa đổi các hằng số và *IV*, phép băm, biến đổi đầu ra và cắt ngắn.

6.1.1 Bước 1 (mở rộng khóa)

Nếu K ngắn hơn 128 bit, nối K vào chính nó $\lceil 128/k \rceil$ lần và chọn 128 bit bên trái nhất của kết quả để tạo thành khóa 128-bit K' (nếu độ dài (tính theo bit) của K bằng 128 thì $K' := K$):

$$K' := 128 \sim (K \| K \| \ldots \| K).$$

Tính các khóa con K_0, K_1 và K_2 như sau:

$$K_0 := \bar{h}(K' \| U_0 \| K');$$

$K_1 := 128 \sim \bar{h}(K' \| U_1 \| K')$, khi sử dụng các Hàm băm Chuyên dụng 1, 2 và 3;

$K_1 := 256 \sim \bar{h}(K' \| U_1 \| K')$, khi sử dụng các Hàm băm Chuyên dụng 4, 5, 6 và 8;

$$K_2 := 128 \sim \bar{h}(K' \| U_2 \| K').$$

Tại đây U_0, U_1, và U_2 là các hằng số 768 bit mà được định nghĩa trong Điều 6.3, và $\bar{h}$ ký hiệu hàm băm h đã đơn giản hóa, tức là không có phép đệm và gắn thêm độ dài và không cắt ngắn đầu ra của hàm vòng (L_2 bit) về L_H bit bên trái nhất.

CHÚ THÍCH 1 Bước đệm và gắn thêm độ dài được bỏ qua bởi vì trong trường hợp này độ dài của chuỗi đầu vào hoặc là L_1 bit hoặc là $2L_1$ bit.

CHÚ THÍCH 2 Việc cắt ngắn được bỏ qua vì trong trường hợp này độ dài của K_0 luôn là L_2 bit, ít nhất nó bằng L_H.

Khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 5 và 6, khóa dẫn xuất K_1 được phân tách thành 4 từ được ký hiệu bởi $K_1[i]$ ($0 \le i \le 3$), tức là:

$K_1 = K_1[0] \| K_1[1] \| K_1[2] \| K_1[3]$.

Khi sử dụng các Hàm băm Chuyên dụng 4 và 8, khóa dẫn xuất K_1 được tách thành 8 từ được ký hiệu bởi $K_1[i]$ $(0 \le i \le 7)$, tức là:

$K_1 = K_1[0] \| K_1[1] \| K_1[2] \| K_1[3] \| K_1[4] \| K_1[5] \| K_1[6] \| K_1[7]$.

Để chuyển đổi một chuỗi thành các từ cần có một quy ước thứ tự byte. Quy ước thứ tự byte cho việc chuyển đổi này được định nghĩa cho hàm băm chuyên dụng đã chọn có trong ISO/IEC 10118-3.

6.1.2 Bước 2 (sửa đổi các hằng số và IV)

Khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 4, 5 và 8, các hằng số cộng tính đã sử dụng trong hàm vòng được sửa đổi bằng cách cộng mod 2^w với một từ của K_1, ví dụ:

$C_0 := C_0 \boxplus K_1[0]$.

Điều 6.3 chỉ ra từ nào của K_1 được cộng vào từng hằng số.

Giá trị khởi đầu IV của hàm băm được thay thế bởi $IV' := K_0$. Hàm thu được từ các thay đổi trong bước này được ký hiệu bởi h', và hàm vòng của nó được ký hiệu bởi ϕ'.

6.1.3 Bước 3 (phép băm)

Chuỗi đầu vào cho hàm hăm đã sửa đổi h' là bằng với chuỗi dữ liệu đầu vào D, tức là:

$H' := h'(D)$.

6.1.4 Bước 4 (biến đổi đầu ra)

Hàm vòng đã sửa đổi ϕ' được áp dụng thêm một lần nữa, với đầu vào thứ nhất là chuỗi KT (được định nghĩa dưới đây) và đầu vào thứ hai là chuỗi H' (kết quả của Bước 3), tức là:

$H' := \phi'(KT, H')$.

Đối với các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8,

$KT = K_2 \| (K_2 \oplus T_0) \| (K_2 \oplus T_1) \| (K_2 \oplus T_2)$.

Đối với các Hàm băm Chuyên dụng 5 và 6,

$KT = K_2 \| (K_2 \oplus T_0) \| (K_2 \oplus T_1) \| (K_2 \oplus T_2) \| K_2 \| (K_2 \oplus T_0) \| (K_2 \oplus T_1) \| (K_2 \oplus T_2)$.

Ở đây T_0, T_1 và T_2 là các chuỗi 128-bit được định nghĩa trong Điều 6.3 cho mỗi hàm băm chuyên dụng.

CHÚ THÍCH Biến đổi đầu ra tương ứng với việc xử lý khối dữ liệu thêm được dẫn xuất từ K_2 sau khi đệm và gắn thêm trường độ dài.

6.1.5 Bước 5 (cắt ngắn)

MAC gồm m bit được nhận được bằng cách lấy m bit bên trái nhất của chuỗi H', tức là

$MAC := m \sim H'$.

6.2 Hiệu suất

Nếu chuỗi dữ liệu đã được đệm (trong đó thuật toán đệm phụ thuộc vào hàm băm đã chọn) chứa q khối, thì Thuật toán MAC 1 yêu cầu $q + 7$ lần áp dụng hàm vòng.

Việc này có thể được rút gọn về $q + 1$ lần áp dụng hàm vòng bằng cách tính trước các giá trị K_0, K_1 và K_2, và bằng cách thay thế giá trị khởi đầu IV bằng giá trị IV' trong khi áp dụng hàm vòng. Khuyến cáo thực hiện sửa đổi này với mã lệnh của hàm băm cùng với sửa đổi bắt buộc được yêu cầu cho Bước 2. Đối với các chuỗi đầu vào dài, Thuật toán MAC 1 có hiệu suất là so sánh được với hiệu năng của hàm băm đã được sử dụng.

6.3 Tính toán hằng số

Các hằng số mô tả trong mục này được sử dụng trong các Thuật toán MAC 1 và 3. Thuật toán MAC 3 được chỉ ra trong Điều 8.

Các chuỗi T_i và U_i ($0 \le i \le 2$) là các phần tử cố định trong mô tả của thuật toán MAC. Chúng được tính (chỉ một lần) khi dùng hàm băm; chúng khác nhau cho mỗi một trong số bảy hàm băm.

Các hằng số 128-bit T_i và các hằng số 768-bit U_i được định nghĩa như sau. Định nghĩa của T_i bao gồm hằng số 496-bit R = 'ab...yzAB...YZ1...89" và các hằng số 16-bit S_0, S_1, S_2 trong đó S_i là chuỗi 16-bit được tạo nên bằng cách lặp lại 2 lần biểu diễn 8-bit của i (ví dụ biểu diễn hexa của S_1 là 3131). Trong cả hai trường hợp mã ghi dạng ASCII được sử dụng; tương đương với mã ghi khi sử dụng ISO/IEC 646:1991.

For i:= 0 *to* 2

$T_i := 128 \sim \bar{h}\ (S_i \| R)$ cho Hàm băm Chuyên dụng 1, 2, 3, 4 và 8.

$T_i := 128 \sim \bar{h}\ (S_i \| R \| 0^{512})$ cho Hàm băm Chuyên dụng 5 và 6, trong đó 0^{512} là 512 bit '0'.

For *i*:= 0 *to* 2.

$U_i := T_i \| T_{i+1} \| T_{i+2} \| T_i \| T_{i+1} \| T_{i+2}$

trong đó chỉ số dưới trong T_i được lấy theo modulo 3.

Trong các Hàm băm Chuyên dụng 1, 2, 3, 4, 5, 6 và 8, đối với tất cả các hằng số C_i, C_i' và tất cả các từ $K_1[i]$, bit có nghĩa lớn nhất tương ứng với bit bên trái nhất. Các hằng số C_i và C_i' được trình bày bằng biểu diễn hexa.

6.3.1 Hàm băm Chuyên dụng 1 (RIPEMD-160)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 1 được định nghĩa như sau (trong biểu diễn hexa):

T_0 = 1CC7086A046AFA22353AE88F3D3DACEB

T_1 = E3FA02710E491D851151CC34E4718D41

T_2 = 93987557C07B8102BA592949EB638F37

Hai dãy các từ là hằng số $C_0, C_1, ..., C_{79}$ và $C_0', C_1', ..., C_{79}'$ được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 1. Chúng được định nghĩa như sau:

$C_i = K_1[0]\ \Psi$ 00000000, ($0 \le i \le 15$),

$C_i = K_1[1]\ \Psi$ 5A827999, ($16 \le i \le 31$),

$C_i = K_1[2]\ \Psi$ 6ED9EBA1, ($32 \le i \le 47$),

$C_i = K_1[3]\ \Psi$ 8F1BBCDC, ($48 \le i \le 63$),

$C_i = K_1[0]\ \Psi$ A953FD4E, ($64 \le i \le 79$),

$C_i' = K_1[1]\ \Psi$ 50A28BE6, ($0 \le i \le 15$),

$C_i' = K_1[2]\ \Psi$ 5C4DD124, ($16 \le i \le 31$),

$C_i' = K_1[3]\ \Psi$ 6D703EF3, ($32 \le i \le 47$),

$C_i' = K_1[0]\ \Psi$ 7A6D76E9, ($48 \le i \le 63$),

$C'_i = K_1[1] \Psi$ 00000000, $(64 \le i \le 79)$.

6.3.2 Hàm băm Chuyên dụng 2 (RIPEMD- 128)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 2 được định nghĩa như sau (trong biểu diễn hexa):

T_0 = FD7EC18964C36D53FC18C31B72112AAC

T_1 = 2538B78EC0E273949EE4C4457A77525C

T_2 = F5C93ED85BD65F609A7EB182A85BA181

Hai dãy các từ là hằng số $C_0, C_1, ..., C_{63}$ và $C'_0, C'_1, ..., C'_{63}$ được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 2. Chúng được định nghĩa như sau:

$C_i = K_1[0] \Psi$ 00000000, $(0 \le i \le 15)$,

$C_i = K_1[1] \Psi$ 5A827999, $(16 \le i \le 31)$,

$C_i = K_1[2] \Psi$ 6ED9EBA1, $(32 \le i \le 47)$,

$C_i = K_1[3] \Psi$ 8F1BBCDC, $(48 \le i \le 63)$,

$C'_i = K_1[0] \Psi$ 50A28BE6, $(0 \le i \le 15)$,

$C'_i = K_1[1] \Psi$ 5C4DD124, $(16 \le i \le 31)$,

$C'_i = K_1[2] \Psi$ 6D703EF3, $(32 \le i \le 47)$,

$C'_i = K_1[3] \Psi$ 00000000, $(48 \le i \le 63)$.

6.3.3 Hàm băm Chuyên dụng 3 (SHA-1)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 3 được định nghĩa như sau (trong biểu diễn hexa):

T_0 = 1D4CA39FA40417E2AE5A77B49067BBCC

T_1 = 9318AFEF5D5A5B46EFCA6BEC0E138940

T_2 = 4544209656E14F97005DAC76868E97A3

Hai dãy các từ là hằng số $C_0, C_1, ..., C_{79}$ được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 3. Chúng được định nghĩa như sau:

$C_i = K_1[0] \Psi$ 5A827999, $(0 \le i \le 19)$,

$C_i = K_1[1] \Psi$ 6ED9EBA1, $(20 \le i \le 39)$,

$C_i = K_1[2] \Psi$ 8F1BBCDC, $(40 \le i \le 59)$,

$C_i = K_1[3] \Psi$ CA62C1D6, $(60 \le i \le 79)$.

6.3.4 Hàm băm Chuyên dụng 4 (SHA-256)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 4 được tính như sau (trong đó $\bar{h}$ là phiên bản được đơn giản hóa của Hàm băm Chuyên dụng 4 được định nghĩa trong Điều 6.1.1):

$T_0 = 128 \sim \bar{h}(S_0 \| R)$,

$T_1 = 128 \sim \bar{h}(S_1 \| R)$,

$T_2 = 128 \sim \bar{h}(S_2 \| R)$.

Dãy các từ là hằng số C_0, C_1, ..., C_{63} được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 4. Chúng được định nghĩa như sau:

$$C_i = K_1[i \bmod 8] \Psi C_i^{''} \quad (0 \le i \le 63),$$

trong đó dãy $C_0^{''}$, $C_1^{''}$, ..., $C_{63}^{''}$ ở biểu diễn hexa (bit có nghĩa lớn nhất tương ứng với bit bên trái nhất) được định nghĩa như sau, các từ được liệt kê theo thứ tự $C_0^{''}$, $C_1^{''}$, ..., $C_{63}^{''}$.

428a2f98	71374491	b5c0fbcf	e9b5dba5	3956c25b	59f111f1	923f82a4	ab1c5ed5
d807aa98	12835b01	243185be	550c7dc3	72be5d74	80deb1fe	9bdc06a7	c19bf174
e49b69c1	efbe4786	0fc19dc6	240calcc	2de92c6f	4a7484aa	5cb0a9dc	76f988da
983e5152	a831c66d	b00327c8	bf597fc7	c6e00bf3	d5a79147	06ca6351	14292967
27b70a85	2e1b2138	4d2c6dfc	53380d13	650a7354	766a0abb	81c2c92e	92722c85
a2bfe8a1	a81a664b	c24b8b70	c76c51a3	d192e819	d6990624	f40e3585	106aa070
19a4c116	1e376c08	2748774c	34b0bcb5	391c0cb3	4ed8aa4a	5b9cca4f	682e6ff3
748f82ee	78a5636f	84c87814	8cc70208	90befffa	a4506ceb	bef9a3f7	c67178f2

CHÚ THÍCH Các giá trị này là 32 bit đầu tiên của phần thập phân của các căn bậc 3 của 64 số nguyên tố đầu tiên. Chúng là dãy hằng số được sử dụng trong SHA-256.

6.3.5 Hàm băm Chuyên dụng 5 (SHA-512)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 5 được tính như sau (trong đó $\bar{h}$ là phiên bản được đơn giản hóa của Hàm băm Chuyên dụng 5 được định nghĩa trong Điều 6.1.1):

- T_0 = 85f6e8b28ba014ed11d076ead90412a5
- T_1 = 33a6da6c7aaaf2149104fe4183152828
- T_2 = 7682094a7e45cf6bf27d19c2c7d6cf77

Dãy các từ là hằng số C_0, C_1, ..., C_{79} được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 5. Nó được định nghĩa như sau:

$$C_i = K_1[i \bmod 4] \Psi C_i^{''} \quad (0 \le i \le 79),$$

trong đó dãy $C_0^{''}$, $C_1^{''}$, ..., $C_{79}^{''}$ ở biểu diễn hexa (bit có nghĩa lớn nhất tương ứng với bit bên trái nhất) được định nghĩa như sau, các từ được liệt kê theo thứ tự $C_0^{''}$, $C_1^{''}$, ..., $C_{79}^{''}$.

428a2f98d728ae22	7137449123ef65cd	b5c0fbcfec4d3b2f	e9b5dba58189dbbc
3956c25bf348b538	59f111f1b605d019	923f82a4af194f9b	ab1c5ed5da6d8118
d807aa98a3030242	12835b0145706fbe	243185be4ee4b28c	550c7dc3d5ffb4e2
72be5d74f27b896f	80deb1fe3b1696b1	9bdc06a725c71235	c19bf174cf692694
e49b69c19ef14ad2	efbe4786384f25e3	0fc19dc68b8cd5b5	240calcc77ac9c65
2de92c6f592b0275	4a7484aa6ea6e483	5cb0a9dcbd41fbd4	76f988da831153b5
983e5152ee66dfab	a831c66d2db43210	b00327c898fb213f	bf597fc7beef0ee4
c6e00bf33da88fc2	d5a79147930aa725	06ca6351e003826f	142929670a0e6e70
27b70a8546d22ffc	2e1b21385c26c926	4d2c6dfc5ac42aed	53380d139d95b3df
650a73548baf63de	766a0abb3c77b2a8	81c2c92e47edaee6	92722c851482353b
a2bfe8a14cf10364	a81a664bbc423001	c24b8b70d0f89791	c76c51a30654be30
d192e819d6ef5218	d69906245565a910	f40e35855771202a	106aa07032bbd1b8
19a4c116b8d2d0c8	1e376c085141ab53	2748774cdf8eeb99	34b0bcb5e19b48a8
391c0cb3c5c95a63	4ed8aa4ae3418acb	5b9cca4f7763e373	682e6ff3d6b2b8a3

748f82ee5defb2fc	78a5636f43172f60	84c87814a1f0ab72	8cc702081a6439ec
90befffa23631e28	a4506cebde82bde9	bef9a3f7b2c67915	c67178f2e372532b
ca273eceea26619c	d186b8c721c0c207	eada7dd6cde0eb1e	f57d4f7fee6ed178
06f067aa72176fba	0a637dc5a2c898a6	113f9804bef90dae	1b710b35131c471b
28db77f523047d84	32caab7b40c72493	3c9ebe0a15c9bebc	431d67c49c100d4c
4cc5d4becb3e42b6	597f299cfc657e2a	5fcb6fab3ad6faec	6c44198c4a475817

CHÚ THÍCH Các giá trị này là 64 bit đầu tiên của phần thập phân của các căn bậc 3 của 80 số nguyên tố đầu tiên. Chúng là dãy hằng số được sử dụng trong SHA-512.

6.3.6 Hàm băm Chuyên dụng 6 (SHA-384)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 6 được tính như sau (trong đó $\bar{h}$ là phiên bản được đơn giản hóa của Hàm băm Chuyên dụng 6 được định nghĩa trong Điều 6.1.1):

T_0 = 33bfc7a7db2d833c1fa120f248ea0c68

T_1 = 0f53e26170ddedf90aa666a58accf8c4

T_2 = f9371fddd155caefbd989e1270066c7c

Dãy các từ là hằng số $C_0, C_1, ..., C_{79}$ được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 6. Chúng được định nghĩa như sau:

$$C_i = K_1[i \bmod 4] \Psi C_i^{"} \ (0 \le i \le 79).$$

trong đó dãy $C_0^{"}, C_1^{"}, ..., C_{79}^{"}$ chính là dãy cho Hàm băm Chuyên dụng 6 của Điều 6.3.5.

6.3.7 Hàm băm Chuyên dụng 8 (SHA-224)

Các chuỗi hằng số 128-bit T_i cho Hàm băm Chuyên dụng 8 được tính như sau (trong đó $\bar{h}$ là phiên bản được đơn giản hóa của Hàm băm Chuyên dụng 8 được định nghĩa trong Điều 6.1.1):

$T_0 = 128 \sim \bar{h}\ (S_0 || R)$;

$T_1 = 128 \sim \bar{h}\ (S_1 || R)$;

$T_2 = 128 \sim \bar{h}\ (S_2 || R)$.

Dãy các từ là hằng số $C_0, C_1, ..., C_{63}$ được sử dụng trong hàm vòng của Hàm băm Chuyên dụng 8. Chúng được định nghĩa như sau:

$$C_i = K_1[i \bmod 8] \Psi C_i^{"} \ (0 \le i \le 63).$$

trong đó dãy $C_0^{"}, C_1^{"}, ..., C_{63}^{"}$ chính là dãy cho Hàm băm Chuyên dụng 4 của Điều 6.3.4.

7 Thuật toán MAC 2

CHÚ THÍCH 1 Mục này chứa mô tả của HMAC [7].

Thuật toán MAC 2 yêu cầu hai lần áp dụng của một hàm băm để tính một giá trị MAC.

Hàm băm được chọn từ ISO/IEC 10118-3, với yêu cầu rằng L_1 là bội số dương của 8 và $L_2 \le L_1$.

CHÚ THÍCH 2 Các Hàm băm Chuyên dụng 1 – 7 trong ISO/IEC 10118-3:2004 và Hàm băm Chuyên dụng 8 trong ISO/IEC 10118-3/Amd1:2006 thỏa mãn các điều kiện này.

Kích thước khóa k tính theo bit cần ít nhất bằng L_2, trong đó L_2 là kích thước của mã băm tính theo bit, và nhiều nhất là L_1 bit, trong đó L_1 là kích thước của đầu vào dữ liệu của hàm vòng tính theo bit, tức là, $L_2 \le k \le L_1$.

7.1 Mô tả của Thuật toán MAC 2

Thuật toán MAC 2 yêu cầu 4 bước sau: mở rộng khóa, phép toán băm, biến đổi đầu ra và cắt ngắn.

7.1.1 Bước 1 (mở rộng khóa)

Gắn thêm ($L_1 - k$) bit 0 vào bên phải của khóa K; chuỗi thu được có độ dài L_1 được ký hiệu bởi $\overline{K}$.

Khóa $\overline{K}$ được mở rộng để tạo ra hai khóa con $\overline{K}_1$ và $\overline{K}_2$:

- Định nghĩa chuỗi *IPAD* như ghép nối của $L_1/8$ bản sao của giá trị hexa '36' (hay giá trị nhị phân '00110110'). Sau đó tính giá trị $\overline{K}_1$ như XOR của $\overline{K}$ và chuỗi *IPAD*, tức là:

  $\overline{K}_1 := \overline{K} \oplus IPAD$.

- Định nghĩa chuỗi *OPAD* như ghép nối của $L_1/8$ bản sao của giá trị hexa '5C' (hay giá trị nhị phân '01011100'). Sau đó tính giá trị $\overline{K}_2$ như XOR của $\overline{K}$ và chuỗi *OPAD*, tức là:

  $\overline{K}_2 := \overline{K} \oplus OPAD$.

7.1.2 Bước 2 (phép toán băm)

Chuỗi đầu vào của hàm băm bằng với ghép nối của $\overline{K}_1$ và D, tức là:

$H' := h(\overline{K}_1 \| D)$.

7.1.3 Bước 3 (biến đổi đầu ra)

Chuỗi đầu vào của hàm băm bằng với ghép nối của $\overline{K}_2$ và H', tức là:

$H'' := h(\overline{K}_2 \| H')$.

7.1.4 Bước 4 (cắt ngắn)

MAC có m bit được rút ra bằng cách lấy m bit trái nhất của chuỗi H'', tức là:

MAC := $m \sim H''$.

7.2 Hiệu suất

Nếu chuỗi dữ liệu đã được đệm (trong đó thuật toán đệm là đặc thù đối với hàm băm được chọn) chứa q khối, thì Thuật toán MAC 2 yêu cầu $q + 3$ lần áp dụng hàm vòng.

Nó có thể được rút gọn về $q + 1$ lần áp dụng hàm vòng bằng cách sửa đổi mã lệnh của hàm vòng. Người ta có thể tính trước các giá trị $IV_1 := \phi(\overline{K}_1, IV)$ và $IV_2 := \phi(\overline{K}_2, IV)$ và thay thế giá trị khởi đầu IV bởi IV_1 trong lần áp dụng thứ nhất của hàm băm, và bởi IV_2 trong biến đổi đầu ra (lần áp dụng thứ hai của hàm băm). Nó cũng yêu cầu một sửa đổi của phương pháp đệm: thực ra, đầu vào thực sự của hàm băm bây giờ là L_1 bit ngắn hơn; điều đó có nghĩa rằng giá trị L_1 phải được thêm vào giá trị L_D.

Đối với các chuỗi đầu vào dài, Thuật toán MAC 2 có hiệu năng so sánh được với hiệu năng của hàm băm được sử dụng.

8 Thuật toán MAC 3

CHÚ THÍCH Điều này chứa một biến thể của Thuật toán MAC 1, nó được tối ưu hóa cho các đầu vào ngắn (nhiều nhất 256 bit).

Thuật toán MAC 3 yêu cầu bảy lần áp dụng cho hàm vòng đơn giản hóa để tính toán một giá trị MAC, nhưng việc này có thể được giảm về một lần áp dụng của hàm vòng này bằng cách thực hiện các tính toán trước nhất định.

Hàm băm phải được lựa chọn từ các Hàm băm chuyên dụng 1 – 6 từ ISO/IEC 10118-3:2004 và Hàm băm Chuyên dụng 8 từ ISO/IEC 10118-3/Amd1:2006.

Kích cỡ khóa k tính bằng bit lớn nhất bằng 128 bit và độ dài MAC theo bit là m lớn nhất bằng $L_H/2$.

8.1 Mô tả của Thuật toán MAC 3

Thuật toán MAC 3 yêu cầu năm bước sau: mở rộng khóa, sửa đổi các hằng số của hàm vòng, đệm, áp dụng hàm vòng và cắt ngắn.

8.1.1 Bước 1 (mở rộng khóa)

Nếu K ngắn hơn 128 bit, ghép nối K vào chính nó một số đủ lần và chọn 128 bit bên trái nhất để tạo ra khóa 128-bit K' (nếu độ dài (tính theo bit) của K bằng với 128 thì $K' := K$):

$$K' := 128 \sim (K \| K \| \ldots \| K).$$

Tính các khóa con K_0, K_1, và K_2 như sau:

$$K_0 := \bar{h}\,(K' \| U_0 \| K');$$

$$K_1 := 128 \sim \bar{h}\,(K' \| U_1 \| K'), \text{ khi sử dụng các Hàm băm Chuyên dụng 1, 2 và 3;}$$

$$K_1 := 256 \sim \bar{h}\,(K' \| U_1 \| K'), \text{ khi sử dụng các Hàm băm Chuyên dụng 4, 5, 6 và 8;}$$

$$K_2 := 128 \sim \bar{h}\,(K' \| U_2 \| K').$$

Ở đây U_0, U_1 và U_2 là các hằng số 768-bit mà được định nghĩa trong Điều 6.3, và $\bar{h}$ ký hiệu hàm băm h mà không có phép đệm và gắn thêm độ dài, và không cắt ngắn đầu ra hàm vòng (L_2 bit) thành L_H bit bên trái nhất.

CHÚ THÍCH 1 Phép đệm và gắn thêm độ dài được bỏ qua bởi vì trong trường hợp này độ dài của chuỗi đầu vào hoặc là L_1 bit hoặc là $2L_1$ bit.

CHÚ THÍCH 2 Phép cắt ngắn được bỏ qua bởi vì trong trường hợp này độ dài của K_0 luôn là L_2 bit, nó là $\geq L_H$.

Khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 5 và 6, khóa dẫn xuất K_1 được phân tách thành 4 từ được ký hiệu bởi $K_1[i]$ ($0 \leq i \leq 3$), tức là:

$$K_1 = K_1[0] \| K_1[1] \| K_1[2] \| K_1[3].$$

Khi sử dụng các Hàm băm Chuyên dụng 4 và 8, khóa dẫn xuất K_1 được phân tách thành 8 từ được ký hiệu:

$$K_1 = K_1[0] \| K_1[1] \| K_1[2] \| K_1[3] \| K_1[4] \| K_1[5] \| K_1[6] \| K_1[7].$$

Để chuyển đổi một chuỗi bit thành các từ, một quy ước thứ tự byte được yêu cầu. Quy ước thứ tự byte cho chuyển đổi là quy ước mà được định nghĩa cho mỗi hàm băm chuyên dụng trong ISO/IEC 10118-3.

8.1.2 Bước 2 (sửa đổi các hằng số và IV)

Khi sử dụng các Hàm băm Chuyên dụng 1, 2, 3, 4, 5, 6 và 8, các hằng số dùng để cộng được sử dụng trong hàm vòng được sửa đổi bởi phép cộng mod 2^w với một từ của K_1, ví dụ:

$$C_0 := C_0 \boxplus K_1[0].$$

Điều 6.3 chỉ ra từ nào của K_1 được cộng vào từng hằng số.

Giá trị khởi đầu IV của hàm băm được thay thế bởi $IV' := K_0$. Hàm vòng kết quả được ký hiệu bởi ϕ.

8.1.3 Bước 3 (đệm)

Các bit đệm được thêm vào chuỗi dữ liệu ban đầu chỉ được sử dụng để tính MAC. Do vậy, các bit đệm này (nếu có) không cần phải lưu trữ hoặc truyền đi cùng với dữ liệu. Người kiểm tra phải biết dù các bit đệm có được lưu trữ hoặc truyền đi hay không.

Chuỗi dữ liệu D là đầu vào cho thuật toán MAC cần phải được đệm về phía bên phải cùng với số ít nhất các bit '0' (có thể không có) như cần thiết để nhận được chuỗi dữ liệu $\overline{D}$ có độ dài 256 bit.

CHÚ THÍCH Nếu chuỗi dữ liệu đầu vào là trống, thì chuỗi dữ liệu đã được đệm $\overline{D}$ chứa 256 bit '0'.

8.1.4 Bước 4 (áp dụng hàm vòng)

Chuỗi bit $\tilde{L}$ được tính như biểu diễn nhị phân của độ dài (tính theo bit) L_D của chuỗi dữ liệu D, nó được đệm về phía bên trái bởi số ít nhất các bit '0' như cần thiết để nhận được một chuỗi 128-bit. Bit bên phải nhất của chuỗi bit $\tilde{L}$ tương ứng với bit có nghĩa nhỏ nhất của biểu diễn nhị phân của L_D.

Chuỗi đầu vào của hàm vòng ϕ' (cùng với các hằng số được sửa đổi) bằng với ghép nối của K_2, $\overline{D}$ và kết quả XOR của K_2 và $\tilde{L}$.

Đối với các Hàm băm Chuyên dụng 1, 2, 3, 4 và 8:

$$H' := \phi'(K_2 \,||\, \overline{D} \,||\, (K_2 \oplus \tilde{L}), IV).$$

Đối với các Hàm băm Chuyên dụng 5 và 6:

$$H' := \phi'(K_2 \,||\, \overline{D} \,||\, (K_2 \oplus \tilde{L}) \,||\, K_2 \,||\, \overline{D} \,||\, (K_2 \oplus \tilde{L}),\ IV).$$

8.1.5 Bước 5 (cắt ngắn)

MAC có m bit được rút ra bằng cách lấy m bit trái nhất của chuỗi H', tức là:

$$\text{MAC} := m \sim H'.$$

8.2 Hiệu suất

Thuật toán MAC 3 yêu cầu 7 lần áp dụng hàm vòng.

Thuật toán có thể được rút gọn về một lần áp dụng duy nhất của hàm vòng bằng cách tính trước các giá trị K_0, K_1 và K_2.

Phụ lục A

(quy định)

Mô đun ASN.1

Phụ lục này chỉ ra module ASN.1 có liên quan tới các cơ chế MAC đã quy định trong tiêu chuẩn này.

```
MechanismsUsingADedicatedHashFunction {
  iso(1) standard(0) message-authentication-codes(9797)
  part(2)asn1-module(0) mechanisms-using-a-dedicated-hash-function(0)
version2(2)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ALL;
IMPORTS
    OID, ALGORITHM, HashFunction, HashFunctionAlgs
        FROM DedicatedHashFunction {iso(1) standard(0)
          hash-functions(10118) part(3)
          asn1-module(1) dedicated-hash-functions(0)};
-- gán OID
-- ===============
is9797-2 OID ::= {iso standard message-authentication-
        codes(9797) part(2)}

id-mac-1 OID ::= {is9797-2 macAlgorithm-1(1)}
id-mac-2 OID ::= {is9797-2 macAlgorithm-2(2)}
id-mac-1 OID ::= {is9797-2 macAlgorithm-3(3)}

-- kiểu định danh thuật toán MAC và tập các thuật tóan MAC đã nhận diện
-- ========================================================
AlgorithmIdentifier {ALGORITHM:IOSet} ::= SEQUENCE {
   Algorithm ALGORITHM.&id({IOSet}),
   Parameters ALGORITHM.&Type({IOSer}{@algorithm}) OPTIONAL
}
MessageAuthenticationCode ::=
         AlgorithmIdentifier{{MacAlgorithms}}

MacAlgorithms ALGORITHM ::= {
{ OID id-mac-1 PARMS MacParameters} |
{ OID id-mac-2 PARMS MacParameters} |
{ OID id-mac-3 PARMS MacParameters} ,
... - các thuật toán bổ sung mong đợi --
}

-- định nghĩa các kiểu tham số MAC
-- ==============================
-- Các tham số tùy chọn có thể được thỏa thuận theo các cách khác

MacParameters ::= SEQUENCE {
   dhfAlgo HashFunctions OPTIONAL
   m INTEGER (1..MAX)
}

END -- MechanismsUsingADedicatedHashFunction --
```

Phụ lục B
(tham khảo)
Các ví dụ

B.1 Tổng quan

Phụ lục này đưa ra các ví dụ cho việc tính các Thuật toán MAC 1, 2, và 3. Các ví dụ của Thuật toán MAC 1 và 3 sử dụng các Hàm băm Chuyên dụng 1-6 và 8. Các ví dụ của Thuật toán MAC 2 sử dụng các Hàm băm Chuyên dụng 1-8. Các Hàm băm Chuyên dụng 1-7 được chỉ ra trong ISO/IEC 10118-3:2004 và Hàm băm Chuyên dụng 8 được chỉ ra trong ISO/IEC 10118-3/Amd1:2006. Chín ví dụ của việc tính mã băm được đưa ra cho các Thuật toán MAC 1 và 2. Các chuỗi đầu vào được đánh số từ 1 tới 9 được chứa trong Bảng B.1. Chỉ có 5 ví dụ đầu trong bảng được áp dụng cho Thuật toán MAC 3.

Trong toàn bộ phụ lục này chúng ta đề cập tới mã ASCII của các chuỗi dữ liệu; nó là tương đương với mã khi sử dụng ISO/IEC 646.

Bảng B.1- Các chuỗi đầu vào cho các giá trị kiểm tra

TT	Chuỗi đầu vào
1	"" (chuỗi rỗng)
2	"a"
3	"abc"
4	"message digest"
5	"abcdefghijklmnopqrstuvwxyz"
6	"abcdbcdecdefdefgefghfghighijhijkijkljklmklmnnlmnomnopnopq"
7	"ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvw xyz0123456789"
8	"1234567890" được lặp lại 8 lần để đưa ra 80 ký tự
9	"a" được lặp lại 1,000,000 lần để đưa ra 1 triệu ký tự

Hai giá trị khóa được sử dụng là các chuỗi 128-bit sau:

key 1 = `00112233445566778899AABBCCDDEEFF` và

key 2 = `0123456789ABCDEFFEDCBA9876543210`

B.2 Thuật toán MAC 1

Đối với các ví dụ trong mục này, giá trị $m = L_2/2$ được chọn, tức là, m = 80 cho Hàm băm Chuyên dụng 1 và 3, và m = 64 cho Hàm băm Chuyên dụng 2.

B.2.1 Hàm băm Chuyên dụng 1 (RIPEMD-160)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	B7F4508111EB8C3B5229C6AED406DE9ECA640133
2	BC78F55933BCEB1EE85A906F9E18374F23E310F9
3	6300DC20E97A5AA29DB9C7D607D23D126FA36863
4	3A2AC89B78EEAB8759F5112BCAD4CD405EEB5D35
5	16DC174925BBC27E0C93D426C346846F97F8BC69
6	E062210BA5C9C94737BF3A6E85B3B5664FBD1D4E
7	9B462D5CBDAE1485FFE10BC001EF9E3AF6D128B5
8	88E73A01A1DE36C92D6F9E41F7278D407B4A4CCD
9	E7B128E4A1842B750F1E61A486C867C4887A4B21

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	B45D6CA84CFB9020E0D5ABA2A7609D3D81F3F57F
2	8844375992037D1BCD0D118EE548D70C3F19CBBB
3	917C59B8AC7FC19DC25BEF82766412FA16BBC6A7
4	E0737CC7976D8F424390CB8798D623D751AFE15A
5	D57FAE836870718EFA4BD4A5F2F322A179A8735E
6	42B20D4C8FD5E8672760CF83C0478D7BF8021404
7	42B20D4C8FD5E8672760CF83C0478D7BF8021404
8	10441DF4F68CE8815818DC0FB370ABF87BCA4464
9	E06AD21D2AF04DD4217AB03B1A578F036997D01A

B.2.2 Hàm băm Chuyên dụng 2 (RIPEMD-128)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 64-bit: 64 bit bên trái nhất của
1	A47A64E9EDE0741B3FDDE33E5C1C6D78
2	51355051852FDC79FB228EAC905633AD
3	D83940DAFFBD4CBBE6BA30A6F9E63F5F
4	1A7CFE2BB26E973E213C1CB96FA4C2EF
5	798AEAC6046B31907C197BD68E59D376
6	0B8E1D4A571F32657189E22A1F2F4A53
7	B814730F482300C6E474FD255A66D680
8	9060A30758EBE3368D939AC168F1A9FD
9	20763FDEDF01E56FF5756954302C7DE0

key 2: 0123456789ABCDEFEDCBA9876543210	
tt	Kết quả MAC 64-bit: 64 bit bên trái nhất của
1	35FA3AC39F50F2A4E3FFC7AF5776B4EB
2	A89E25E6796747B630A2A00B802EA53E
3	66339027A36608EBD932DD551616E7B2
4	1F8779BAD84B50373931211A2761EAD3
5	31BF5B5B7ABAC2567DC0E02F1C3A25D7
6	B5B8BA3B8EA895FBC83CB7588FBD2656
7	8D27BBEC257C848D5CF375EB5EDA4CC7
8	B40B5BF6727DE90B26F770850F059C89
9	76C7BC831B0BCE593DFD44E8E054A373

B.2.3 Hàm băm Chuyên dụng 3 (SHA-1)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	C8A8B3C75E6CE7C6C4F79CC19853CCD54ABCB079
2	8DD9AE643BF10BBB7B978EF13EE6C0F480618FB0
3	A738B26A8BD318184E76707A99CAE14C670B9711
4	1EBFE413E55D6B288A2BD01D294A21FD8D4B20BF
5	0CE7BF40A73D977AB4999CF3A9BD1C5BEDC442E9
6	12A6823CC181294F95109073A6AA0C8961B14386
7	9369EE4A043AF1CA6E078D0B8A9CE5C1545440BA
8	B00D37D70A84B762FC0A8A9BC1B15F0E517B5EDF
9	DDDF44613E8559D12C150D022D5FE33F9E0FBACE

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	C3A5ECD1E715C7272CFE78BC278086587B040422
2	D5D50FFA7EFDF1B17E96E2EC14DBC4412F7B771F
3	01BFDD568008D412158F5B0C90AE2730DCFB77FB
4	9982E0EE91DB89AE7E7618AD1D649BA43406DBDD
5	ACD04E1004FCE53DECA9EE7AB95DAF97B7C44AA8
6	FADF62DCE789E86E60756AA819EF62C3E5C25E94
7	46DB9A49FB4976D007B14B1574843D019CA99445
8	4EF5BED3E816C530B23F491583C038596BB76FDB
9	BAC6BE6BE6153FECE2891F9DA03824D D4D535D19

B.2.4 Hàm băm Chuyên dụng 4 (SHA-256)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	76D91CA2337FF25EF66DF2AE7172626C5544428822B9E1B9C94121D384489C09
2	479DA7965233CB2133C6B949AD82CBC5B29F528DB90FF04A1496323D77D15FFD
3	BE6E923798F594BC529C87DF5A42333EE18BE88FED984B0EFE092BF31D570FAE
4	664AA91CFF68C786E943FEB0E6BB465213FFC57AF5C8F973827DF67956FC21D6
5	D7A7A1D1007CB2D3DC578BB4FDA4A5B1B2EBF7B27C9CC43BDF7A382851DF91AB
6	BC9853B4E7AE574B3DCF4728BF44FC27A3C04C5AB90EA189DD175B6F5ECB4335
7	66F3238A2C2B6A3AB86089B9DF33BA6420F7E66F5DE6856D79CCA908DFE57BFE
8	B1A59E0905F8EE9ACF5C77E67883C8C3CA10DA965BE31F75A47AD85015CD478B
9	15FC09FABB62AADEE831B9988E2DE2F41A3C685D28E4C06720ED6E8493CD060A

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	F0400A79DD136B4E83EB507E23F98C1A54E7DCA33A38C75902008F90B003C37A
2	407FA9A8170113C1C0B06B8FDC32AB5914343D0CBEBEE5B1C84008182794CD8C
3	7E02C2AB8B8115B446E80C70CE4A0126E83E0208420E39965272D6497EE16B86
4	BEFC08E950BF7CD6B6BA0026A910328ACF45551DB93180099D0893C8415314F1
5	00019D3C8D5D563A9A24462029171C6D4CF29BCF8CC6D60BF76584A6B4F696ED
6	383F7B8050D7B08DEAEEB3B5B04496669815277968D5A2ACDEF04D37C596E2E7
7	FFEE6E137909EF2140A87619B51CF6C7FBAFC6EF5B8388C8ACF0F7DE5AA8E7BB
8	511855ADB1B5FE79C1C04B565CD40359B5DFA474AC52BE7F4CB2753285B90D0C
9	8F6D5B1C7CC360DC4E4320755684B24726B8C4312A12B329ADC8C2550C3FEB08

B.2.5 Hàm băm Chuyên dụng 5 (SHA-512)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	A4D628912D3CDA87D92F4597B7385E9BEB6161A2C12D412E3EAA7B4FD1003ABE D6EBE9C7418D60905267A84F0A2B22865D8E21F1E48D4E105F6C3A653D5C63E2
2	DBBD9316AAE10399C742C212365A529B7EE5F9BBDB96BA9A14A078010AF81806 AF4635AADA77595FE21B7B5C552038AAE38CF32C4D4E480855560E98AC25297F
3	C9598B319F5DA537044289553FB7B0FAC95B51569BD08DB4A45995CB75A344FE 88ABF5001694497ED71B5CAB3C5D4212E937E50712CCFAFF5C8B3D4C23EABDF5
4	B22A1CD30D3AF351931E746542BEFAD2985BD6838831BDBCFEE3B9DA48AA8996 76C4ADF4278D79D45A6C6E4AEA613B5F3FDE4E6F4FE06854B9736B9355EE0A6B
5	EC807431CE07B43F95E001B562525B0F49EC6BD5B91055C030D79D5E462008A8 B9D862ABD3E8517D59FE3F3E60424EFC1327D67D53A04F4871076999619D4327
6	176422D10271BD8A22AFA4164F62439DEFAF0B4901AF4F8FD366C79055280635 175B8D920574AC85B493FBA1EFFDD46233C54BAEC783FF3030BADF6FB37413AD
7	22E8A8624F3982CA3A7B18635E4029FB6CD3B771EAFF7BAD5A00C064C1099B99 7BCF7FA529D5864BEA94DA7EB5367D8C27763B7303FAD4F517D598AC7453A60A
8	17A2D95A4935C88234EEBFBA29140B57ACECA329E513AA7BD7110283759FA6E6 D9457D4B58C7DE765A495703B04AA476E5412DDE52E799C841EAF37925A37CB3
9	F807A843A14B94B977259556B656A7A401C3D026B5FDC993BC1E6A2E0E5AC7EC 7CAA611C9EB3F4609E7699F43A305BDC4818B823B219BE7AB5C54A4AC01F5E4B

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	14D4BDDF705DEFA756AE8154FA09792D1D86EF52A88E8552CA4DB56420F6BD08 0D3114F626B90B59EA1D0C7E4187678E22C263FE94D074D70477252CDDA86C04
2	C340C2B6F8C606AD499747EC6239DF94D5365047061EB4A26789EB83177B002A 2F8C1F5B866A23389CAE742A057C4ECBDC7F7C20266BC99625A974DC345B0EE0
3	AE0343C78F41BB04026B8BC36C7D09BDB7E6C8450FE340A7223274C5F61DBA14 5C776D694C3B05E8BEBB1A494607A00E363E21B3BCC7ADB5FAE52F20D4F2B210
4	F98F58C4C7498F17A70FB5A86CA0D2AE86DA99E318CF0B8A801639A6DC7B3DB7 C57B975EA6347B55D68C6E8B34C185CB06972370B15EADBB4F35C8277AFB7D79
5	7B073E2F13EB203BF937567D6A42F4F80A7BBD47E120226B2B1171C8F62BCC53 CC0DA4F0DD78C5534C1370E3DAEA81DD2EA6DF7EDD7BEE7334065A6A2B0A0FB8
6	641BBAA2591C17B1D73435DE640A22FAC1A2C38D11BC025F6991ACF667096011 D6E48F27826F06BB006425DC4EBBE9EE7CDE3CF1C3A9592C674CCEEDA0F10BE4
7	B0025F9B04BDD64D15AA61D0A5CF8CE5C1FC0A55830CF81FEAB1A3854D5D3E41 F111918913E9638292B9BF752C6B6F0626A322FC89C28E03C80816F5115C7753
8	5E9A6219308123921A527502526DA57957E0C2C00601CA5224769DD925FC43F4 7FEAC4163B0D62CBCC7E4537859792DF8E4CCFEA4E8E3D387014A514F42B6CA3
9	CDB9961A62447DAAEA3046E59517DFBAA8C7E51C7B45A4561918B8B5CFD3EF89 96B36921490049A70AA19CFAF88F017BDC03FC1CE419BAB718642186C17502FC

B.2.6 Hàm băm Chuyên dụng 6 (SHA-384)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	3148BD96B4CAB64EE95C6444EAE0053E783AC28949FE05D0 52A1FCCE7DB8A619A1D0BC858FAF013E53BD2A24AAEA03E8
2	735E4ED128DDF2EEC1FDF0370BF32517DF63E836FC0CBBB9 A1C5CEFEC32CFB5586E2AA3A85ABD08FC6EB8EB9E777CB52
3	15B7AF6E28E6AC436DB405B706078ED88F0F9D292C4C1A4A 5EF1FAF0BA315683439D0DFE325283C1C83DE846C23DA890
4	F49C22A8E48D0B4C145EEFDDE51027248A2BCD341FE43504 4DC980C38333D5F197CE08BF26354C545690C805D6AB1E9F
5	9DB498C5971A668857AD56C724F82104C2CC78D90701A29A E97D9D269180FC64E35E058CE8898927001D20BBFF3B472A
6	3D782A279E1D683623EE34D9935D43D9627CF5D045DBEB7D FFF8C29CB3916A4F0FF00C012CE125956655873A3D883812
7	3A9AFFFEBF68E5660606797A5BAFDBC2B47DE1DEDA40AC48 0F535583D9544A63210ACE4DA24F997786C2F80367FA5284
8	0309E1B60798568E00522AC145ABB39AA19C5066549E07AA 5D6ADDEED34B4F2F3DF166C9C3915F44F92D79A049E7B753
9	343CC7791B07C4D26E5735224B302C495D9CB2A92EA27BDB 2A96487C9CB3EC09D75C9E0179F73180E24D78000D45D8FD

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	FE10F454AD0EAA717123E77AF83760DA2B5F27AAB2BBE4D3 5C4AE1352D54CA36554EA206475F1BC5D24060CAF17E7432
2	BCE4739807A7BD64F709605DBE1A2B572D963CFF5CAF557F 194F18CB924A6B90B2A54E3844701A77D459A64AB3142A1C
3	86CD24861B303510FA374D2AA5E2CA78F329138D5B9C2E04 3C0FFC5E0AB37342B7859AE8B7CD8D6F3B1833F81628CA9E
4	B03FC36C1FA2C72EF1EC1C9B8E9E322EA23C1A0F6C5AC5E9 AB2BA60D560D7156385D8D2DB0B117C71340E053DE4A08EA
5	3B923573C9598E5F78EED06EADFCD6DAE2F8C762A8BBDFDE 8F0986934F5DD4A212B3493DD190E723A17B51D4F4F351AA
6	0188E2DDA587AD67E91DD38C247051E1446CEDA39EDF33B0 DD9BFC4310BAFE41887638216955F6E31E683420D858D16B
7	269010C8844FECCF00F3EC33E600DD6F1BA56DA91F1F1257 575BD5C5EBE6931F212CC8FDF81EA70C0CDCFBF20D06E84C
8	92CF0571CD8AD78C1CD43E847837A849EC8B92CEAAEED5E7 541E23B14C4FF713A40C94D6A34E731543E1D3EC52B69BEA
9	95FA93E72585717CA74701D46EF9E25A9E2FD10FE015CD8F 04427323315A60B074E1A1134F18B2154644658C24EB3D36

B.2.7 Hàm băm Chuyên dụng 8 (SHA-224)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	065B86EDEE58E12C4D83C7AD1500EB4CD313DC3AA2147A12F39B7AFE
2	73D5627C9DBDE736841766FE543B7954D59AEE1F5C6823BCE7E77351
3	A4F4EA69DF69D9705D71305817B38AFE1EF6ECF724C3F6743B26A9D2
4	E8E14D49D6C2A88D4A717A276693FF3D03444AC43FE02C99B6919A23
5	38CB47CB00B57B858A0ABB864F05B8E83EE4A250A5794740796FAA05
6	64ACE1CD852195AC765764DBA813749BDECB15498C30FB6CA73E0F71
7	570E89F76E8435B945CF47AF5B054262C654636AEB955FD951076B91
8	CCC8BDEED3869F5D8E2013EDFCE22A36185C5403103F04E586F987C5
9	E0BEA67230DA03039540FA70CB0FBD69464E9DEE3C3FF80CD5D76646

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	FD5B8A7CD44B62730BF4DE82D7E2D70135E29FAEB1E66933D54BFF68
2	E70AB63A4D92C3B2A6975BB24B9380B5320D7E510107D27CC97F0086
3	36C19C58F5F13B43544424A085EB5E822AF4BD7F32B7AD190B5CA3BB
4	DC53898B38F96269AAF0890A3A4D7E00B03B931C3AF7C80C8BBCF6EC
5	446B9988D8C5B35A20DD6B71B5F1E3E048144CD082C801449B5497EA
6	48E72C0EDC3E52370EF2DAE859A5462D60C735DA3F0B7494AFB0D5AB
7	3E048D2F615BC681D1B2FD59A37F7D8972AE7C8096603B859F771223
8	E2CC9DFD0A2945F8F2C3003ADD8AAA493BB0C72BFAA82B7CA8B1F289
9	552A67693AB02EC7D0AF18075DA9875B8B5D1DB89F6CFC73EA7151DE

B.3 Thuật toán MAC 2

Đối với các ví dụ trong điều này, giá trị m = 80 được lựa chọn.

B.3.1 Hàm băm Chuyên dụng 1 (RIPEMD-160)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	9EBEA41FBC24CD80BF2ECFD5B8C8CC8181D3FCAE
2	75CB722C50024C0E8A7A0DBA7D5C36B86D9D1DD5
3	5B48C1749DDED71EDFE0ADE2B944E808E4A65820
4	F9033064567F541235C3944EE95CB476055985D1
5	B37885405B71E025AF0CB574021A562A62733628
6	5C6429B982C8054B5B3348A0D7D2CE24D7032BC1
7	B0A4A451D0926855E52428E16D1FEAA241C4DD9B
8	1CCEEC5122F08A76EBCD8E3DE88610D942D8A5F6
9	45D61908BFF6039E6DE3C037FDCE6191F19F6410

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	2FDE5DAF7050D14E6D7ACD2254D17FA3A8CBFCDD
2	239C4020610429A8662BF81A2CAAEA47F8EA0A44
3	89EFFB9F5A6BCEAE3C65D0C9803F3464E5E9E349
4	F5FC87FD5702F5D4E7BB634DA4CB4B41CD505B6C
5	5686C00F69E6C868732C67402AA107CEAB513439
6	525EC4893A221EFD9B6DD351059B40C05B4CE2D3
7	B975ED3893FC8D535376EF49211E2E6B1BB30B90
8	BC201FFA581357C271DAE25104167F3DCC97BADC
9	95A875A1D64D55E677D8E4455E1445E7E940F758

B.3.2 Hàm băm Chuyên dụng 2 (RIPEMD-128)

Key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	AD9DB2C1E22AF9AB5CA9DBE5A86F67DC
2	3BF448C762DE00BCFA0310B11C0BDE4C
3	F34EC0945F02B70B8603F89E1CE4C78C
4	E8503A8AEC2289D82AA0D8D445A06BDD
5	EE880B735CE3126065DE1699CC136199
6	794DAF2E3BDEEA2538638A5CED154434
7	3A06EEF165B23625247800BE23E232B6
8	9A4F0159C0952DA43A8D466D46B0AF58
9	19B1B3AF333B894DD86D09427116D0AD

Key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	8931EEEE56A6B257FD1AB5418183D826
2	DBBCF169EA7419D5BA7BD8EB3673FF2D
3	2C4CD07D3162D6A0E338004D6B6FBC9A
4	75BFB25888F4BB77C77AE83AD0817447
5	B1B5DC0FCB7258758855DD1840FCDCE4
6	670D0F7A697B18F1A8AB7D2A2A00DBC1
7	54E315FDB34A61C0475392E5C7852998
8	AD04354D8AA2A623E72E3594EE3535C0
9	6F9B1C0FC06753618D6DB4B007733795

B.3.3 Hàm băm Chuyên dụng 3 (SHA-1)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	86C2962E58B3498A2608935AF7726311F2BFB538
2	0497FF21DAE3251DA0ED2F47F5A3B74ABA6B2560
3	6EE2A25F943E3F3EC05225FBB86BA73E2E5D51D2
4	CD4C0D1328DC4A8DC2801001B129AEFC6E0CF9CE
5	89ECE303FAD1E4313950CC3B008CB239B5B85844
6	9DF741057D075D3C4E1533E38A5FF469647194B4
7	188A58390A6EF9827035B81CDF1B5069211F0EE5
8	98A98D6A81FD361030856D2C19742AD8DBC468E7
9	D2986310BA18A78786534882F9C6BCBF06CCE9E3

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	2739B6BE63F539EB70FE250346F6382A2DFA345F
2	A0C2711A6B1DA4CD8F85EF1E6FF7BF70B412B477
3	18F570E864FF903D2773D53C2E114E1A62152953
4	A80845A89BA15E941A2457084BC431F3E47759E1
5	14143EA1057B02D20C0157216190A006E30F3D41
6	DAB4B41BA639B4715889406FE18E0C037017E063
7	AEAEA5415B4F266CB15CBEB844E56AEC2DABAD6D
8	3DBA11471EB4FCCF21BAEB0BFF7E20150132C6CF
9	3BB917B8BD8560E89FF9054FBE096CBACA109D5F

B.3.4 Hàm băm Chuyên dụng 4 (SHA-256)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	E8A06537F096CCF1A3C425A56CEA054072C4A8DB67BD28CFB02FBEAF84B35F6C
2	DDABFDF46CE93311868B7275E05730AD3E23192A575CC291AE3785289B94A2F3
3	02581EA39A6CF2D752793FD782CFB9CF965BE72B32B322C9551D03510645FB31
4	1F12288F42F42661349E5DB741CE19F3B8C3A8149FD4B8981237FA200FEB104F
5	EA4A04E76EEC57D6906098AFA7AE0264072C09F0DB34269B117C68C3ED989C5E
6	6EB683218305A862A1C1EFBA04A2A62DC4EC27886D3C79AFF7C493C2D6DFB080
7	6DC64AC5C5F197EB5463474AA6B329DA9D5B3C6A3324B147469E06F21EB53C41
8	8F4B417527DA9533408D95951ED6504525C9683B45637B246CE25C99ACC64698
9	5E2E0579A26517B06D2933CF62DEA20347A0A8DF9D7C3D200FA5E894ED9C5EDF

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	DCC3C81236AAD92043D1478DF7926E78205F7BBD0C3001854BF9087261ACCE47
2	AEE154DCF83568248DC228C8C3513E9BEEA268B4979FF17CDE5BE484F4919DDA
3	C3B53B9897D72197B240F08715E5C830886FE2F2EFC2E5A8ACD9D5405098863B
4	60CD78CAED2CC9BD3F5BDA6AAA81596B55556660B19A2DF2FF6C48F89C52CD7E
5	6283D8BA031EE52E2D7EBA96287025F161A5219EF1FB59CEBE6133007B35A146
6	3BB625768D0900710F0EF7E854990BBBA35AA9B7BD4B0133656D290992A9BF79
7	98FF69D0048FF552843CB8D5DC686EB2FEC3600D664A464F7B88F7289CC41A78
8	5893F4AD6CEBB85BB90CD4107BF85EEEBAB621C6EEB4EC487780A45DED09F5B2
9	781BFEC8396C6268E5413D76EDAE0C90E6592B624BB4E0FB6137F4DF33FB91D1

B.3.5 Hàm băm Chuyên dụng 5 (SHA-512)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	EEB2E7DC1EA7C75966552A7F45C9F30E3FB9A7EA1362BA6D7324DD7DEF461F88 B2B5E433CD7CA25A08554605B0B020C3A865434BABFC140DE5D55C8A94C7FDC6
2	8A507C281F9155A086C97E3BDB14B658F6C901B1948674139389853F55B453C4 83DF9AB807269B286AFD6FBDB6A59E3CF190BB61951D8A89BB0F3D611DC012DC
3	F5B41F81B56D9CEF4BFFFBDD659470CA9DE7348A23DAC136790B028986D13E7D 74DC59759FAEA253D5342ABD56CF6F5859145AD54BCA62E0C45245B7E4FA5C53
4	2EEC2E512FFDAC27444A563B40BFE9EAF594D0C83947A374AC82797DA811466E 8DF8380836446B4B392E4E815B8E84695DB8253230635C18CFEB19CBE1CF012B
5	DCD40B28C684428F83D1E7D457A906DFCAB55C2298B7A242C4F208F205E948A1 BA081A39C6DF60E2279DE4C3D6F82A4490ACCD6679AAF7FEA90DE4BAE06F2C32
6	E78F92E31D7410DD16EC830B477FE703B79925811758F0D3A11F3E4F48DA0C26 87A797EB2E3D7E20026936A87E6903F9D8C93EF3E8FECF2CB2A42A720F301821
7	49BCFE57FA600FDF68562B91E686B02DE81DE25CF4466C7072985389808 80BFD 339264B48F2BD712127A1C66D97D1B367DDD8656B996CBD8D5B7EDD561328CD5
8	C4979A98F32B6DCAC7718B6089694DBFC6E6ACDF82724F1EFFB277593B716389 ECEA6F4C40EA524C84A1324C6AFABB78C0FE0AA008C1EA3427AF179540FDFBF3
9	376DD55BA616E59FCD6249267577608563C168CBF82CC6A89B83BC9224641B28 CC944C6DFEEDE8CCF7FC6F61FF0D322B3183449677330B6EBD83BDD7B57FB846

key.2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	42A0B3DC6AF1D40CF4D58E2E35832C5824AA77E6B685B3E3BBBE69A82C726DD8 B46C861BBE0DADFA359207426187A1675A054CE82905F5A2FCE5495D6BBB6957
2	DAED898D6A86AFD1C622C96D33521175690365330EA0CEEEDB85292F8BBADFD8 67A7C1327356DFD75FA0C38B099BD229C39CF7CF07F479308F52A5C29CD284DA
3	41A98A3AD2B5BF46C000DEB754D93C2D41C4EFBE272163346E8D78A1FA222BD8 046551C4FFE81E8BA0A0DBD746A25066DBFAE79B4040D964D8F2DE181E71212D
4	1296CD85141D1D3BAA6C52ED6A1569925112AAB7820883B3369D278A5711C62C F483045B5F4172841BC917BF92D45EAFC448D975FCAF58D95E8E9AFD127BB7A6
5	C0941AAEA51B8539592403C1CCBB98736F470F5F07C2FBB2374CEFDDE6BF0A34 EAA164B430B59E6921422D6E0C5BEA969FB9F6A7381AC9A8E0107D5BBDD11E3A
6	B87B9328C0041DC4492C5F0AA613EBDC9E1D01156E4E0628705A27B3DCB6EEEC 20E862DA7971DC2B999B6C6952ADB7D8615E68384289076C4B752D0DF393F2E3
7	CB102567BDB4AAB8833419ED3BB95F1875488439B5416FDD466B79CC73BD26E0 9690A3E94CF611D7532128224E225C671B50FC2BED4934516A4955931774B30E
8	41B7CD308733F10CCCC0AE5CAD8AF9E0740317A0EE874489872EC640CC0CB16F 101A12E446F555855555E7AB5128B8D370C006FFA151C7FA35EE10144E1FDD16B
9	2FFE4FEF445D76A2A41E5EDB715170D02ACAC44A580144C17ED65434A876CC99 568E39E97CE78E5325EE376B113C6D7C5247D96AA0DC1D91A0932C81B58D956F

B.3.6 Hàm băm Chuyên dụng 6 (SHA-384)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	7BEE4557700A1D8ECE045E8A6FC980F456D2FF4F5AA77BEA 3147F54DC77E8F6A2FA016E9BAA4E105D53B4631CE088CBE
2	33B764BFC7E4A95BB432BD7766C3EB0F0AB686CAC8FD40CD A53A0B0D623D48373F36B321412C4D01E4AAF8BA53C77751
3	67BF47CD4B410564245D335985B5DD404D085E2DB88F2A35 B0782C7FA4AEF3407D489D66EA8914E74752CD1913963139
4	1522B5D65022C1CEBF2425EC914320CCDBE198251CFEA79F 499179A2025185B5CE6241E84A6FF0F9C83820FA83597E62
5	98E3EA52031575D96489C7DB7AE3B4A4AE7D80E789958CE7 99350E2E07D7B852FC8BB3EFF3F2954A2C158BC3C70E8ED1
6	34B80B9F2775DABB019819277302ADAEEC0CA6F0963B2979 314A44724B6318D9213DDFFA2E04B175E1E7D6778FC8A8A5
7	5BF44F677E77FBEBE31516D80CED014DC99E7F51AC4CC41F 6401292990E3668319B137C2F1626C67BB92A1CED7BE15AA
8	7A8610621AB18CA0C87AD25A984C333D3B4BE12E85DEB8E3 88E4656133115FD4710DF4B81D0A526E56553C25E6279131
9	63490CBECD7350ACD6D9D5F485D323440A271555CC3C1E51 F245E0FE4D8DFE6340C6146D2EEB46DFF90A0D1970A30C52

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	6760086DFFB66B3AA619569BF567D6ACEFD52E2F3D90CC40 103346CB1EE0A493E159785876F8C310B44BF05B64E6B2FF
2	6575DC9AF2E0A9D32D619465C95FED1FF5B1D3E65A2EAD93 405BD2DA82896EE3F9D336B374E5D015594EC44872EBF8C2
3	A6685B72C7545F84405CF20CF17CB67B246FA914C59F335E 7F95B5B11963072777FA3B635AABF86D0D75B83D6365211D
4	0D52B84209956EFD9F39DE27821D328CB0B3FCDEFCF64B99 ED2B65C4DE7A753BCA2361CBB26043649FDFCD8C757E700C
5	9A50FF272D08AB3AD03911B4FB042E0CB8080C18F5938F0C 93340DA508722DBB799C72EA1274B67AD30EAE22E86213B3
6	21BC7FA9F9E23536084CB65EE28727DDD378A1FD6D316D29 BFC3C8A39851EDE817A392D460A628E79A018989249A0CC0
7	F291C145D2F9A10C76C5E40CD4C4027E2688799C95FE4C45 3042DED3EEE4C4331CDC5F571B8642C615DA2A1A854C6EA4
8	23A9161DE7B21284446B49D5038F0D2823A0F05619B243F3 D0E114E3AA9AC905C506A9546E9EEB41F1DD1ABCE8F43B71
9	D056C9491A84401387A18E6953C7157E86C3AD4D3E2B0971 5E91B486EE89C7FE17CE40A10C78EF819433F006F7779443

B.3.7 Hàm băm Chuyên dụng 7 (WHIRPOOL)

key 1: 00112233445566778899AABBCCDDEEFF				
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của			
1	5A77B599D2DB9B6B 47556A7EC5191745	8C8E5112DD5F0B88 4AAD7C63F5F9A7A9	719D60A4866688C2 439C7887DDD47DBF	DFF624A6EA4ADB62 E45B0A68ABE62A40
2	177B98F9F215046E CCE9FDDCD3853303	640B8EFE3E723C4E B84821F0B070296C	7233C5E745B72DE9 EC039B7C86432B34	381D6A3F47E30F95 90520D5FB2585A19
3	F92ECF9FB82E39EC 61D32FA9C99DCBC9	B2D3EC8CFEF76317 A7FF32E7643F6B00	A8C4E6F835BD4994 8B8D1510FB2A95D9	D4D156B68F640D37 A1AEC1CC15508634
4	078067C14C1E3930 ECB7BA5D3225B39D	11BFE58E1E94F03F EE3B63A616368829	9062DA01378760A6 02EB3B4999CB227B	5F7BE1FF041B8087 60F1613C174DBBD3
5	05411A95D2A5CDA0 C37973E0FE0EFCB1	CB4A7339A70E62FF 5F68EB1E06AA4E3C	790D945F25963F15 F15DEFA7E2A4A129	95E39486BAD88B2F B18F4C5C8B300B63
6	8E2A8C15E9611E57 653C4CA5CD6FC863	5BF67165B38B0425 E6A6E0CFDAD1F5B7	9A30C8C15F9DE729 60E657B5365ADA57	97391B32575D9C78 04BA92ED92277DDF
7	9A7D93D28BA451CD C2528ABA3661909A	E57570C1CC41E943 91044C6C1C8EA914	D288F3FD112C7E32 2F1FCFB07CE394A9	22185F2163AE9328 C0F31862B5A2328B
8	A3676A07D9E79CAB D08E538430F7A050	DAA1DA6EAB3FBAD1 2E3504C51A5B2449	28114F4D7E00050A 2BE90403BA08B1A3	B7167400203585B6 D7C1E9E8B70B50E5
9	521EA57548F1068E B6D4A01127D67966	C0364330ABEEAC85 157DEC38F1D77A35	9E008D976323B1BA 361BACDA62E506C4	13ECFB405E0909EB 59DE28298AEC9CCE

key 2: 0123456789ABCDEFEDCBA9876543210				
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của			
1	FDB6120AFEDAEB87 C29A8B3524BA23F3	A4DDC952FE02C1EC 512765C83734D2A2	B17DDD6647D0FAB6 6D65139B49FE5A0D	7194CAA506EED1DB 8682E868353DA04B
2	8B738011A43BD813 66D15236D52C5FF7	63C38B941E81975B 35CAA40ED5A49561	C2562EC9185B70B5 D57A5FB202386A21	503D34FEA89B0E3B E226335C78928E0D
3	C97109474261CEDB 16D1F15A20C9844E	4FE524CE8319BD1E AEAE04EBA11D6D67	4FAD2DCA54348400 F1405C58A1779C5C	30238EB26812644D 0E4C2D6C42E7252A
4	A320497D440E9452 FCE87CB6215E5ADD	846B80EFD4578628 711D76EF1C0573CD	ACD969D64A6EC42E D5C6E1F133F31472	F350F05BE6F604E8 776D37CE86E9B369
5	E1C734A8E6301FD2 1B29C21F864E60AB	70655F5E6DACCE51 49FA8143BE4CF0F0	15083D3DA974D411 F12622BA4C6E2325	82C219F74F357E48 D09BDA7F634518BB
6	66E060BF156AEC45 236D7C34E465105D	4058E4D4A88A0DA8 5AD7C6D7206801CE	8FAD6D118D5B7310 CC20CB08109486F6	60FA0BB68B673DDB 0E6B48FEAC3D5B77
7	608FB970FD10D1BB DC7313D3D2C5FEC0	CEAEE1FA02E44C06 32A3DCA366CF7FBF	2F1711A214E2594B B0EBE2504F2C749C	E57A71FCC419042F D89E914D87292F11
8	D3B314AD10D07CC4 CBB66497472C2E50	5708D35526B165A8 A91EE7705695D1AC	9B5AE596D24ABEAC 0750F2237CD78E8C	FCD3C0EF2DCCF196 D01C9891429CA501
9	024F0B3B7A403417 1B0F8AFBC605AD78	B8191F8383DFFE55 3F5BE4F1D2B19C51	F23F5B1A29E3FC24 CEA40F91A5239B70	BB29097E294FE798 4A65ABF1DB054FC9

B.3.8 Hàm băm Chuyên dụng 8 (SHA-224)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	B5BC4C46AE5F4E335792CE51304F986D3DD6EAB862933AB3EE7DB5D7
2	63C3DB8305A361388FC52CF4567521303ADA68C31A6FA0638113D594
3	B176AB2549522FD0B93EE32B99BD43C00388DF17FE2B827CE91FD603
4	CD676B859E48A06EC59AE4BF8F341997D9E9FDBA4922ABC983D787A1
5	4CA41164F2AC8F994CA036C8FF516142EED491D82FA6A9C51B44F817
6	3BC5924DA588B993389429D0146FCCD64320CB69E1057C16CDA57AE1
7	184AD4D6C9B1C5BC8FE7D4184C20F724E66C4F158DB41E3025B022D2
8	39FC2867E4979919B1EE5A03D1B15571D69BABA4FED9891D9F97FBF1
9	63859486E22F8C2E90E5F5BF510E732543414F6FB731B0A8E9807249

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	13247FB84F20471BEC77D777E9648D2C2C4C7B7E132782FC3D1262A4
2	F07713FCB295F3C9997E823B63D0C0B2170D7A6EF533E0F93076D235
3	6F072241CED9E423F04B10F89D656CE36AC7AA6027CB22A6E1216A42
4	9582A2C75DECBCD7E5378D583559B33F74AC61A4A3CF5AA25CD6E3A0
5	47CA643A560DD0A7D06E86218A7E80256CA87FE6A29CCD2081F40EC4
6	02358052E6DF1510771267593C2682814A8E4362E6DF0BDEB59D4DDD
7	B08BCB38E974C3972451DA9805C977DF001CEA225FE3D8EA105938AE
8	EB50337CE04D4131ABF837780BBBD9674473EA029A08E774F1DC6876
9	6774049ADA46BCC6AD6BCAE615404A22704885B0627F1BDD74D2F8DA

B.4 Thuật toán MAC 3

Đối với các ví dụ trong mục này, giá trị $m = L_2/2$ được chọn, tức là, m = 80 cho Hàm băm Chuyên dụng 1 và 3, và m = 64 cho Hàm băm Chuyên dụng 2.

B.4.1 Hàm băm Chuyên dụng 1 (RIPEMD-160)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	6606EF2D3BBD010F516C65372C3CF0ACF111B3F7
2	F0BC0C81307E17A71F4C40AE0B2AC39FCB23CE12
3	7720FD23925B854F963E8812573CD86EBA61EB66
4	2683D6CE053BA0420E76130EAE2367734B7D2D53
5	DE532D156CBE12464BB6147E99470C471D91F1C6

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	4BD390E9EC460AD4866CCB32D091AFBF73E5B6DA
2	CD2847BAB4636C9BCEADCF3D187122A9199DA670
3	15C3910C42638E5EE6DEBD506BD8C4DB94713A3A
4	04148DCB47728E3E57B836A66043D5145879796E
5	829A24010704DBD0EE34A6D607F7B34829E04E95

B.4.2 Hàm băm Chuyên dụng 2 (RIPEMD-128)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 64-bit: 64 bit bên trái nhất của
1	aeb2c45f13c0c6f5f10be2f1e3e9c322
2	16874d0e17e4f1c290dd749cceff7834
3	a289aa06aeb8fc99b989c377baadd9d4
4	0d80db68bbf99442dc3d6b83d038def3
5	11dc4a6bd375c64f78bb78ad265ed7cd

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 64-bit: 64 bit bên trái nhất của
1	7248481816b8d3af29f5c002ff769ea5
2	dfe1e36ce9792476e0889f1becef18a9
3	9b4f1d21320f4a327f023947554bfc3b
4	3d2d658d0196e4339f42ada50dfcfa6f
5	0a34452d9da70c70183dffddb8eec056

B.4.3 Hàm băm Chuyên dụng 3 (SHA-1)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	708F4A226CDE708820643CBEEFDCBE6CB36FB269
2	EAB87BE709D1E5CB62C7489C2B1407130B772760
3	C1BD6F9C908132FEF5187CBE681B42A8C785FBF6
4	F34DEB241D46C6448D67ACE6B8CD4DF00DA23EBC
5	669DED2BD6A1AE0BCFF7D3B74494C1D8161FA0D8

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	EAF6F9DDBAFD299320FF0FC8E02E2BE62879F341
2	2AAE9DE0A555E7CD7383C27506A467B8DF4E3A33
3	FE6031710329D12090F73F55CFFCC6215F9BEAE9
4	0CCDD9DAB6B0126800EC1CC7A02656E12EDEA42C
5	ABDBC8AAAE4A8CE734432188740A149BDF2D215F

B.4.4 Hàm băm Chuyên dụng 4 (SHA-256)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	B5FA90A26AC41FF4260BC38142032D5745C2635AEE274846DDAAAAB27ED9E77D
2	3859B97FEF3B4FFF77813AA8E9310BFBB5A015D03564557EFAF3AAFA2888E830
3	8800151E003F4956B4F351862587FCC40DF84D3EC691459DA9E6A8E55E8C3F60
4	5708BD75C1B763B6ACE40E91E1B165C33ECB3EEA3D63B95FD31D895FBF6D46E9
5	3865F84EE189730BB4FC387D42F8A86281DBE3687341C83BB7A5ED362D8094FE

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	5977BDB720997D17297835A553017D478A7F514990215A73A661089A9C5ABC7D
2	E5C2A8C6328E749FAB5E983FCC9D213CB968B2CBFC8634A28DE38C17336DE017
3	CBE66212BD2BF930C303399B2836C8A246FAFF28D34C2B389C6A16DD7F101A48
4	6F7C08BA9AB6BFC73C157B55EEB892F11819B09915818F5B515E1486CB0167E0
5	F519F962E848583855E2FAEFC5D89238B53126719CD62792FE1BA0039C51B3D3

B.4.5 Hàm băm Chuyên dụng 5 (SHA-512)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	CE19A0FCC29F1AB31C204973AC0BCF4AB1A044E187423DC5774C1EBA4D87450A 62FABB4ADC2F6FA8C37B1AF79D249967E89CDF9328312F3B077B9E408481DD06
2	BB06A4991397163DC273F94F871BF4B61E1001ED9BEDD6E6282484464F7F60A6 FEAD67F105FFEC40AB367DB98DA8AB72E3EFF4CDE8ED61B64B2CAAB8278D32A3
3	0FEA25FBC2C95D3D73EF4972FC2EE17D51F0CB354D3677BBBE41DBA70B78DB32 F11BAAB1C9A6BDFD22A60615929600C5594CC58798F979EEED931F21F4F6765D
4	B38B47605771DC1F34DF203239C111BC44BFCC182A338259BBD89D6A468458DA AB551BFFC15F3681C3D3C3882669D441371427A1FF6BF25F08093AB399391F32
5	AC2171E8EBC170C7C7556FEA4E4786DE7DCD8FF80A3C8C701E752ACA0BFDF478 C6A8F90C4D57275D97CF8E23F2F7BBC15847EB49666A63FD4F52B3EB9014F0AD

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	286800D1661857CE3DE713777E0302303A04C6DB6CA5D8D880DBA5328B498CBC 2A0F3353AADA7AD6DF456DF5FB08C067819BB0A29C46EEF7BB91E86DD85217F0
2	758512264E54DD20394B5E90228FDD8BDC159D4F4F04B4AECC1CD51DCA88DD62 4F364B98B031A4175E2D896D883E1F280A6A27E005A6F7CB764A37676C231A62
3	ADCC88C406F7118E6BC673FE38D7D16E42A7373892050044676BEDFAFA4CD23F 11B4253C6B4A1965EB8044E277962FE38A848CDE27C8AA84E2583A6F6A6C8EFB
4	A18E3AF76F7D24AE7220A3DC9616675301025C007753BBFB7E6785D107DE656B 62DDEA8D58B03AF290C82E9C8429FB1DB45FE684D114E5D4FF1560B0495005B8
5	988DF21325F32F1F4BB9C9F4DABDF9989CA976D5626C67FFEA7820060FFB3AE2 233A91F0E9AA99D82A41434CAB5A2B662D97353D22A12164A21A5492CCBD1C3A

B.4.6 Hàm băm Chuyên dụng 6 (SHA-384)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	20425431D9A664F039928CAEF044869B0FA02BD8D19504BE CE96A79318708202A92B4FB3ACF24BD0236EDFB7CE31C8FC
2	75A2FB6690CA619F9A99704A1F94E7737E8FE9C0697AAC22 9DACC85F651CE67324E64E22095ED0A6182D1FB147EDD58E
3	89CDF73409FC87BEE998DDFEE1B87C0903F92313D950BB2C B692CED9DFAE48AA50D8B43454469D84AFCF39EFFFC12669
4	A5BE64C72729F20E8A429BD75002EE2B71769FAF8B114078 D2676002B04A8F04D4A4509A89EFA1D54B38846C23037336
5	9ADE9EA42AD6C130931B1A56C771EA76EEF2D0E8217E413D 26D1E2881C8E20494F48236DB922B500194E164EE7D43376

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	BE7105BE54B7317D28B2F42122B37AC16042AD2EC2154765
2	CA08E95A8FC51CE4623B11CC770AB72CD835D4772DA97B6A
3	CD1E2677F344EABB86D6818BC3F6A2B4D91ED101510E7940
4	058A4434BFD62E7B2D2D44A4CEFC4850850B6E025FC7E224
5	AAA67DFDD03B318FE45C76ACD53DB05DA702CDFFF34B8E86

B.4.7 Hàm băm Chuyên dụng 8 (SHA-224)

key 1: 00112233445566778899AABBCCDDEEFF	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	2E47E46A24AB4E7DF363DCC7A418B27F0DE8D8FB63183AA2CACC34BB
2	BDE7A7F350661ABA5585F0B32C430874D12637E4AE7D2164AA112A6D
3	073B15C8448DF8D65A0BC23546BF02C3A527884297DD2519BA170791
4	18A89EC81098140110E97905BBCC072311929A19DD214118AB636702
5	E7D1F07468AEFE9DC2E5AD9549523213F25043845A3CEA3E9E6A10C6

key 2: 0123456789ABCDEFEDCBA9876543210	
TT	Kết quả MAC 80-bit: 80 bit bên trái nhất của
1	559000BB6220FEF550B35EE119EA561CC4C393F03BB52E9267DE560D
2	3CFF9B831C517828ADDBFAB6228BE80A1346F905BE32D109E34110FA
3	73774106EA714A5CBD6682D83A6832E80C788E209174807F3273D8F5
4	CF69464136119BD6B0E8C0D7037214F1CD61FA1EBBAF4BDFA4BDFAC3
5	9517EEF881B9D989C402836D84AEDCF93037E70B6AEBEC1D4E311B37

Phụ lục C
(tham khảo)
Phân tích độ an toàn của các thuật toán MAC

Phụ lục này đề cập về mức an toàn của các thuật toán MAC trong tiêu chuẩn này. Mục tiêu là để hỗ trợ người sử dụng tiêu chuẩn này trong việc lựa chọn một trong những cơ chế và giá trị các tham số.

Trong phụ lục này, $MAC_K(D)$ ký hiệu MAC cho chuỗi D được tính khi dùng khóa của thuật toán MAC là K.

Để xác định mức an toàn của một thuật toán MAC, hai chiến lược tấn công đã được xem xét:

Tấn công giả mạo: Tấn công này bao gồm việc dự đoán giá trị của $MAC_K(D)$ cho chuỗi dữ liệu D mà không có hiểu biết ban đầu về K. Nếu đối phương có thể làm điều này cho một chuỗi dữ liệu duy nhất, anh ta được gọi là có *khả năng giả mạo*. Các tấn công thực hành được thường yêu cầu rằng một giả mạo là xác minh được, tức là MAC bị giả mạo là tính được chuẩn xác từ trước với xác suất gần bằng 1. Hơn nữa, trong nhiều ứng dụng chuỗi dữ liệu có một khuôn dạng đặc biệt, tại đó áp đặt các ràng buộc thêm lên chuỗi dữ liệu D;

Tấn công khôi phục khóa: Tấn công này bao gồm việc tìm ra bản thân khóa K của thuật toán MAC từ một số các cặp chuỗi dữ liệu/MAC. Một tấn công như vậy là mạnh hơn so với giả mạo, vì nó cho phép các giả mạo tùy ý.

Tính khả thi của một tấn công phụ thuộc vào số các cặp chuỗi dữ liệu/MAC đã biết và số các cặp chuỗi dữ liệu/MAC lựa chọn được yêu cầu, và vào số các lần mã hóa không trực tuyến.

Các tấn công có thể chống lại các thuật toán MAC được mô tả dưới đây; không có đảm bảo rằng danh sách này là đầy đủ toàn bộ. Hai tấn công đầu là tổng quát, tức là, chúng áp dụng được vào thuật toán MAC bất kỳ. Tấn công tiếp theo áp dụng được vào thuật toán MAC lặp bất kỳ (để biết chi tiết hơn hãy xem [9]).

Đoán MAC: Đó là một giả mạo mà không xác minh được, và nó có xác suất thành công bằng $\max(1/2^m, 1/2^k)$. Tấn công này áp dụng được vào tất cả các thuật toán MAC, và chỉ có thể bị ngăn ngừa bằng lựa chọn đúng đắn của m và k.

Khôi phục khóa vét cạn: Tấn công này yêu cầu về trung bình 2^{k-1} lần tính; việc xác minh của một tấn công như vậy yêu cầu khoảng k/m cặp chuỗi dữ liệu/MAC. Một lần nữa tấn công này áp dụng được vào tất cả các thuật toán MAC. Nó có thể bị ngăn chặn bằng lựa chọn đúng của giá trị k. Một cách khác, người ta có thể ngăn cản ai đó nhận được k/m cặp chuỗi dữ liệu/MAC, đó là số cần thiết để nhận dạng khóa một cách duy nhất. Ví dụ, nếu $k = 128$ và $m = 64$, xấp xỉ 2^{64} khóa tương ứng với một cặp chuỗi dữ liệu/MAC đã cho; nếu một khóa khác được sử dụng để tính mỗi giá trị MAC, thì việc khôi phục khóa bằng cách vét cạn sẽ không hiệu quả hơn so với việc đoán giá trị MAC.

Giả mạo ngày sinh [9]: nếu đối phương biết một số đủ các cặp chuỗi dữ liệu/MAC, anh ta hy vọng tìm được hai chuỗi dữ liệu D và D' sao cho $MAC_K(D) = MAC_K(D')$ và các giá trị đầu vào của biến đổi đầu ra trong cả hai tính toán là bằng nhau; nó được gọi là một va chạm trong. Nếu D và D' tạo nên một va chạm trong, thì $MAC_K(D||Y) = MAC_K(D'||Y)$ đối với chuỗi Y bất kỳ. Việc này cho phép một giả mạo sau một

chuỗi dữ liệu đã được chọn, vì kẻ thù địch có thể dự đoán MAC cho $D'||Y$ sau khi đã quan sát MAC tương ứng cho $D||Y$. Giả mạo này là trên các chuỗi dữ liệu có dạng đặc biệt, mà có thể không được quan tâm trong tất cả các ứng dụng, nhưng cần được nhận thấy rằng các mở rộng của tấn công này tồn tại mà cho phép có tính mềm dẻo lớn hơn trong các chuỗi dữ liệu. Tấn công yêu cầu một chuỗi dữ liệu được lựa chọn và xấp xỉ $2^{n/2}$ chuỗi dữ liệu đã biết và 2^{n-m} chuỗi dữ liệu được lựa chọn.

Tấn công giả mạo kiểu ngày sinh có thể bị ngăn ngừa bằng cách thêm một khối vào phía trước chuỗi dữ liệu mà chứa một số seri và làm cho việc tính MAC phụ thuộc trạng thái. Điều này có nghĩa rằng cài đặt phải đảm bảo rằng mỗi số seri chỉ được sử dụng 1 lần để tính MAC trong thời gian sống của khóa. Điều này không sẵn có trong mọi môi trường.

Khôi phục khóa đường tắt: Một số thuật toán MAC tiềm tàng bị tổn thương đối với các tấn công khôi phục khóa dựa trên va chạm trong. Chưa có báo cáo về có tấn công đường tắt đối với các Thuật toán MAC đã được mô tả trong tiêu chuẩn này.

Các chứng minh độ an toàn

Đã chứng minh được rằng Thuật toán MAC 1 là an toàn nếu các giả thiết sau đúng [8]:

- Hàm vòng ϕ được nạp khóa bởi giá trị khởi đầu *IV* và bởi hằng số dùng để cộng là một hàm giả ngẫu nhiên.

CHÚ THÍCH Một hàm giả ngẫu nhiên cùng với khóa bí mật mà có hành vi như một hàm ngẫu nhiên (tức là, khó phân biệt với một hàm ngẫu nhiên) đối với người không biết khóa bí mật.

Đã chứng minh được rằng Thuật toán MAC 2 là an toàn nếu các giả thiết sau đúng [6]:

- Hàm vòng ϕ được nạp khóa bởi giá trị khởi đầu *IV* là một thuật toán MAC mạnh (tức là, đầu ra của nó là khó dự đoán được).

Độ an toàn của Thuật toán MAC 3 là tương tự đối với các giả thiết được làm trên hàm vòng ϕ để chứng minh độ an toàn của các thuật toán MAC 1 và 2.

Thư mục tài liệu tham khảo

[1] ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture;

[2] ISO/IEC 646:1991, Information technology – ISO 7-bit coded character set for information interchange;

[3] TCVN 11495-1 (ISO/IEC 9797-1), *Công nghệ thông tin – Các kỹ thuật an toàn – Các mã xác thực thông điệp (MAC) – Phần 1: Các cơ chế sử dụng mã khối;*

[4] ISO/IEC 10118-1:2000, Information technology – Security techniques – Hash- functions – Part 1:General;

[5] ISO/IEC 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*

[6] BELLARE, M. "New proofs for NMAC and HMAC: Security without Collision- Resistance," Advances in Cryptology, Proceedings Crypto'06, LNCS 4117, C. Dwork, Ed., Springer-Verlag, 2006, pp. 602-619;

[7] BELLARE, M., CANETTI, R., KRAWCZYK, H. "Keying hash functions for message authentication",Advances in Cryptology, Proceedings Crypto'96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 1-15;

[8] BELLARE, M. CANETTI, R., KRAWCZYK, H. "Pseudorandom functions revisited: The cascade construction and its concrete security," Proc. 37th Annual Symposium on the Foundations of Computer Science, IEEE, 1996, pp. 514-523. Full version via http://www-cse.ucsd.edu/users/mihir;

[9] PRENEEL, B. VAN OORSCHOT, P.C. "MDx-MAC and building fast MACs from hash functions," Advances in Cryptology, Proceedings Crypto'95, LNCS 963, D. Coppersmith, Ed., Springer-Verlag, 1995 ,pp. 1-14;

[10] ISO/IEC 18032, Information technology – Security techniques – Prime number generation;