TCVN **TIÊU CHUẨN VIỆT NAM**

TCVN 11816-2:2017
ISO/IEC 10118-2:2010

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HÀM BĂM - PHẦN 2: HÀM BĂM SỬ DỤNG MÃ KHỐI N-BIT

Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher

HÀ NỘI - 2017

Mục Lục

Lời nói đầu

TCVN 11816-2:2017 hoàn toàn tương đương với ISO/IEC 10118-2:2010 và đính chính kỹ thuật 1:2011.

TCVN 11816-2:2016 do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã biên soạn, Ban Cơ yếu Chính phủ đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11816 (ISO/IEC 10118) *Công nghệ thông tin – Các kỹ thuật an toàn – Hàm băm* gồm các tiêu chuẩn sau:

- TCVN 11816-1:2017 (ISO/IEC 10118-1:2016), Phần 1: Tổng quan.

- TCVN 11816-2:2017 (ISO/IEC 10118-2:2010), Phần 2: Hàm băm sử dụng mã khối n-bit.

- TCVN 11816-3:2017 (ISO/IEC 10118-3:2004), Phần 3: Hàm băm chuyên dụng.

- TCVN 11816-4:2017 (ISO/IEC 10118-4:1998), Phần 4: Hàm băm sử dụng số học đồng dư.

TIÊU CHUẨN QUỐC GIA **TCVN 11816-2 : 2017**

Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 2: Hàm băm sử dụng mã khối n-bit

Information technology - Security techniques - Hash-functions - Part 2: Hash-function using an n-bit block cipher

1 Phạm vi áp dụng

TCVN 11816-2 đặc tả các hàm băm sử dụng thuật toán mã khối *n*-bit. Vì vậy tiêu chuẩn được áp dụng thích hợp cho các môi trường trong đó một thuật toán đã được cài đặt.

Có bốn hàm băm được đặc tả trong tiêu chuẩn này. Hàm băm thứ nhất cung cấp mã băm có độ dài nhỏ hơn hoặc bằng n, với n là độ dài của khối dữ liệu được sử dụng trong thuật toán mã khối. Hàm băm thứ 2 cung cấp mã băm có độ dài nhỏ hơn hoặc bằng $2n$; hàm băm thứ 3 cung cấp mã băm có độ dài bằng $2n$; và hàm băm thứ 4 cung cấp mã băm có độ dài $3n$. Tất cả 4 hàm băm được đặc tả trong TCVN 11816-2 đều tuân theo mô hình tổng quát được đặc tả trong TCVN 11816-1.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là không thể thiếu cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu có ghi năm công bố thì chỉ áp dụng các phiên bản tài liệu được trích dẫn. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm tất cả các sửa đổi bổ sung).

TCVN 11816-1: 2017 (ISO/IEC 10118-1:2016), Công nghệ thông tin – Các kỹ thuật an toàn –Hàm băm - Phần 1: Tổng quan.

3 Thuật ngữ và định nghĩa

Các thuật ngữ và định nghĩa được đưa ra trong TCVN 11816-1 và các thuật ngữ sau đây được sử dụng.

3.1 Khối (block)

Một xâu bit có độ dài xác định.

3.2 Mã khối *n*-bit (*n*-bit block cipher)

Mã khối với tính chất là khối bản rõ và khối bản mã có độ dài n bit.

[ISO/IEC 18033-3:2005].

3.3 Hàm vòng (round function)

Hàm $\phi(.,.)$ biến đổi 2 xâu nhị phân có độ dài L_1 và L_2 thành một xâu nhị phân có độ dài L_2

CHÚ THÍCH: Hàm vòng được sử dụng trong vòng lặp.

4 Ký hiệu và thuật ngữ viết tắt

Với mục đích của tiêu chuẩn này, các ký hiệu và thuật ngữ viết tắt trong TCVN 11816-1 và các ký hiệu sau được áp dụng.

B^L	Khi n chẵn, xâu bit chứa $n/2$ bit trái nhất của khối B. Khi n lẻ, xâu bit chứa $(n+1)/2$ bit trái nhất của khối B
B^R	Khi n chẵn, xâu bit chứa $n/2$ bit phải nhất của khối B. Khi n lẻ, xâu bit chứa $(n-1)/2$ bit phải nhất của khối B
B_x	Khi B là một dãy các khối m bit thì $B_x(x \geq 0)$ đại diện cho khối thứ x của B.
$E_K(P)$	Thuật toán mã khối n bit với đầu vào là khóa K và khối bản rõ. Các thuật toán mã khối được đặc tả trong tiêu chuẩn TCVN 11367-3:2016 (ISO/IEC 18033-3) được khuyến cáo sử dụng trong các hàm băm.
K	Khóa cho thuật toán E
u hoặc u'	Hàm nhận đầu vào là một khối n bit và đầu ra là một khóa cho thuật toán E.

5 Sử dụng mô hình tổng quát

Các hàm băm được đặc tả trong 4 mục tiếp theo cung cấp mã băm H có độ dài L_H. Các hàm băm đều tuân thủ theo mô hình tổng quát được đặc tả trong TCVN 11816-1. Với mỗi một hàm băm chỉ cần thiết xác định các tham số dưới đây.

- Tham số L_1, L_2 , L_H;
- Phương pháp đệm;
- Giá trị khởi tạo IV;
- Hàm vòng ϕ;
- Phép biến đổi đầu ra T.

6 Hàm băm 1

6.1 Tổng quan

Hàm băm 1 được đặc tả trong TCVN 11816-2 cung cấp mã băm có độ dài L_1 và L_2 trong đó L_1 và L_2 bằng nhau và bằng n. Một số định nghĩa riêng được yêu cầu cho hàm băm 1 được trình bày dưới đây.

CHÚ THÍCH: Hàm băm 1 được mô tả trong [5].

6.2 Lựa chọn tham số

Các tham số L_1, L_2 và L_H của hàm băm 1 được đặc tả trong phần này thỏa mãn $L_1 = L_2 = n$ và L_H nhỏ hơn hoặc bằng n.

6.3 Phương pháp đệm

Việc lựa chọn phương pháp đệm sử dụng cho hàm băm 1 không thuộc phạm vi của TCVN 11816-2. Cũng như các yêu cầu tối thiểu, phương pháp đệm đưa ra một tập gồm q khối $D_1, D_2, \ldots, D_q$, trong đó mỗi khối D_j có độ dài n và có thể làm đầu vào cho các đầu ra khác nhau. Các ví dụ về các phương pháp đệm được trình bày trong Phụ lục A TCVN 11816-1.

6.4 Giá trị khởi tạo

Việc lựa chọn IV dùng cho hàm băm 1 không thuộc phạm vi TCVN 11816-2. IV là một xâu bit có độ dài n và giá trị của IV có thể được thống nhất và cố định bởi người sử dụng hàm băm.

6.5 Hàm vòng

Phép biến đổi u:

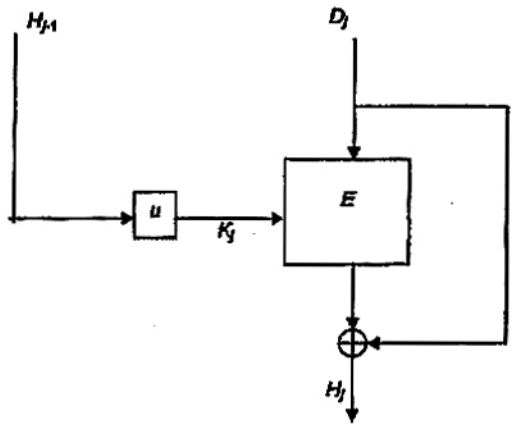
Định nghĩa một ánh xạ u từ không gian mã.

Hàm vòng ϕ kết hợp khối dữ liệu đệm D_j ($L_1 = n$ bit) với H_{j-1} và đầu ra trước đó của hàm vòng ($L_2 = n$ bit) tạo thành H_j . Cần lựa chọn hàm u như một phần của hàm vòng để biến đổi một khối n bit thành một khóa để sử dụng cho thuật toán mã khối E. Việc lựa chọn hàm u để sử dụng cho hàm băm 1 nằm ngoài phạm vi TCVN 11816-2.

Hàm vòng được xác định như sau:

Đặt $H_0 = IV$

$\phi(D_j, H_{j-1}) = E_{Kj}(D_j) \oplus D_j$ trong đó $K_j = u(H_{j-1})$. Hàm vòng được mô tả trong Hình 1.



Hình 1: Hàm vòng của hàm băm 1

6.6 Phép biến đổi đầu ra

Phép biến đổi đầu ra T đơn giản là phép cắt, ví dụ mã băm H nhận được bằng cách lấy các bit L_H trái nhất của khối đầu ra cuối cùng H_q.

7 Hàm băm 2

7.1 Tổng quan

Hàm băm 2 được đặc tả trong phần này cung cấp mã băm có độ dài L_1 và L_2 trong đó L_1 bằng n và L_2 bằng $2n$. Một số định nghĩa riêng được yêu cầu cho hàm băm 2 được trình bày dưới đây.

CHÚ THÍCH 1: Hàm băm 2 được mô tả trong [4].

CHÚ THÍCH 2: Trong [6] tấn công về mặt lý thuyết lên hàm băm 2 đã được ghi nhận: một tấn công va chạm với n =128 có độ phức tạp $2^{124,5}$, một tấn công tiền ảnh yêu cầu độ phức tạp và không gian đầu vào xấp xỉ 2^n.

Lý do duy nhất để giữ hàm băm 2 trong TCVN 11816-2 là vì đảm bảo tính tương thích với các ứng dụng đã có.

7.2 Lựa chọn tham số

Các tham số L_1, L_2 và L_H của hàm băm 2 được đặc tả trong phần này thỏa mãn $L_1 = n$, $L_2 = 2n$, và L_H nhỏ hơn hoặc bằng $2n$.

7.3 Phương pháp đệm

Việc lựa chọn phương pháp đệm sử dụng cho hàm băm 2 không thuộc phạm vi của TCVN 11816-2. Cũng như các yêu cầu tối thiểu, phương pháp đệm đưa ra một tập gồm q khối $D_1, D_2, \ldots, D_q$, trong đó mỗi khối D_j có độ dài n và có thể làm đầu vào cho các đầu ra khác nhau. Các ví dụ về các phương pháp đệm được trình bày trong Phụ lục A TCVN 11816-1.

7.4 Giá trị khởi tạo

Việc lựa chọn IV (độ dài $2n$) dùng cho hàm băm 2 không thuộc phạm vi TCVN 11816-2. IV là một xâu bit có độ dài $2n$ và giá trị của IV có thể được thống nhất và cố định bởi người sử dụng hàm băm. Tuy nhiên, IV được chọn sao cho $u(IV^L)$ và $u'(IV^R)$ là khác nhau.

7.5 Hàm vòng

Hàm vòng ϕ kết hợp khối dữ liệu đệm D_j ($L_1 = n$ bit) với H_{j-1} và đầu ra trước đó của hàm vòng ($L_2 = 2n$ bit) tạo thành H_j. Cần lựa chọn phép biến đổi u và u' như một phần của hàm vòng. Các biến đổi này biến đổi một khối đầu ra thành 2 khối thích hợp độ dài L_K bit làm khóa cho thuật toán E. Đặc tả của u và u' nằm ngoài phạm vi TCVN 11816-2. Tuy nhiên, việc lựa chọn u và u' cũng cần được xem xét vì sự quan trọng của nó đối với sự an toàn của hàm băm.

Đặt H_0^L và H_0^R tương ứng bằng IV^L và IV^R. Hàm vòng được xác định như sau, với $j = 1$ đến q.

$$H_j = \phi(D_j, H_{j-1})$$

$$X = u(H_{j-1}^L) \text{ và } Y = u'(H_{j-1}^R)$$

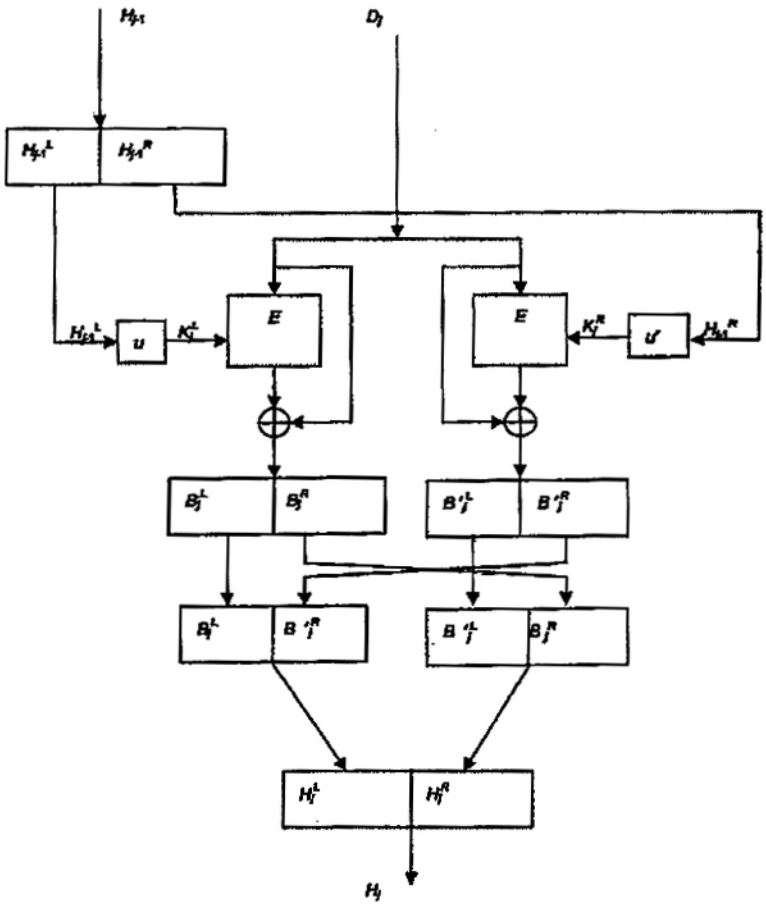
$$B_j = E_X(D_j) \oplus D_j \text{ và } B'_j = E_Y(D_j) \oplus D_j$$

$$H_j^L = B_j^L \parallel B'^R_j \text{ và } H_j^R = B'^L_j \parallel B_j^R$$

Hàm vòng được mô tả trong Hình 2, trong đó X và Y được thay thế tương ứng với K_j^L và K_j^R.

7.6 Phép biến đổi đầu ra

Nếu L_H chẵn thì mã băm sẽ là ghép của $L_H/2$ bit trái nhất của H_q^L và $L_H/2$ bit trái nhất của H_q^R. Nếu L_H lẻ mã băm sẽ là ghép của $(L_H + 1)/2$ bit trái nhất của H_q^L và $(L_H - 1)/2$ bit trái nhất của H_q^R.



Hình 2: Hàm vòng của hàm băm 2

8 Hàm băm 3

8.1 Tổng quan

Hàm băm 3 được đặc tả trong phần này cung cấp mã băm có độ dài L_H, trong đó L_H bằng $2n$, với giá trị n chẵn. Một số định nghĩa riêng được yêu cầu cho hàm băm 2 được trình bày dưới đây.

CHÚ THÍCH: Hàm băm 3 được mô tả trong [1].

8.2 Lựa chọn tham số

Các tham số L_1, L_2 và L_H của hàm băm 3 được đặc tả trong phần này thỏa mãn $L_1 = 4n$, $L_2 = 8n$, và $L_H = 2n$.

8.3 Phương pháp đệm

Phương pháp đệm sử dụng cho hàm băm 3 được đặc tả trong mục A.3 TCVN 11816-1 sao cho $r = n$.

8.4 Giá trị khởi tạo

Việc lựa chọn IV dùng cho hàm băm 3 không thuộc phạm vi TCVN 11816-2. IV là một xâu bit có độ dài $8n$ và giá trị của IV có thể được thống nhất và cố định bởi người sử dụng hàm băm.

8.5 Hàm vòng

Phép biến đổi u:

Định nghĩa 8 ánh xạ $u_1, u_2, \ldots, u_8$ từ không gian mã tới không gian khóa, sao cho:

$u_i(C) \neq u_j(C)$ với tất cả i, j từ tập {1, 2,..., 8}, $j \neq i$ đối với tất cả giá trị của C.

Điều trên có thể đạt được bằng cách cố định các bit khóa ví dụ, có thể cố định 3 bit khóa tới các giá trị 000, 001, ..., 111. Các điều kiện khác có thể áp dụng dựa vào các ánh xạ u_i, ví dụ để tránh các vấn đề liên quan đến khóa yếu hoặc các thuộc tính bù của mã khối. Đặt $u_{j,i} = u_j(X_{j,i})$.

Hàm f_i:

Định nghĩa 8 hàm f_i như sau:

$f_i(X, Y) = E_{ui(X)}(Y) \oplus Y, 1 \leq i \leq 8.$

Ánh xạ tuyến tính β:

Định nghĩa ánh xạ tuyến tính β nhận đầu vào là một xâu $2n$ bit $X = x_0 \| x_1 \| x_2 \| x_3$ và ánh xạ sang một xâu $2n$ bit $Y = y_0 \| y_1 \| y_2 \| y_3$ như sau:

$$y_0 := x_0 \oplus x_3$$

$$y_1 := x_0 \oplus x_1 \oplus x_3$$

$$y_2 := x_1 \oplus x_2$$

$$y_3 := x_2 \oplus x_3$$

Trong đó x_i và y_i là các xâu $n/2$ bit.

Hàm vòng ϕ có 8 khối mã song song, và 8 dãy biến có độ dài n bit $H_{j,1}, H_{j,2}, \ldots, H_{j,8}$.

Trong mỗi vòng lặp, 4 khối dữ liệu độ dài n bit $D_{j,1}, D_{j,2}, D_{j,3}, D_{j,4}$ (độ dài $L_1 = 4n$ bit) được kết hợp với đầu ra vòng trước đó của hàm vòng $H_{j-1,1}, H_{j-1,2}, \ldots, H_{j-1,8}$ (độ dài $L_2 = 8n$ bit) để tạo thành $H_{j,1}, H_{j,2}, \ldots, H_{j,8}$ (độ dài $L_2 = 8n$ bit).

Hàm vòng dựa vào một ánh xạ tuyến tính γ_1 nhận đầu vào là 12 xâu độ dài n bit $l_1, l_2, \ldots, l_{12}$ và ánh xạ sang 8 xâu độ dài n bit $X_1, X_2, \ldots, X_8$ và 8 xâu độ dài n bit $Y_1, Y_2, \ldots, Y_8$. Ánh xạ của tám xâu phụ có độ dài $2n$ bit $R_0, R_1, M_0, M_1, \ldots, M_5$. Ánh xạ γ_1 được xác định theo các bước sau đây:

i) Đặt $H_{0,1}, H_{0,2}, \ldots, H_{0,8}$ theo cách sao cho $H_{0,1} \| \cdots \| H_{0,8} = IV$

ii) For $i = 0$ to 5 do $\{M_i^L := l_{2i+1};\ M_i^R := l_{2i+2}\}$
$R_0 := 0;\ R_1 := 0;$

iii) for $i = 1$ to 5 do{
$B := R_1 \oplus M_i;$
$R_1 := R_0 \oplus \beta(B);$
$R_0 := B;\}$

iv) for $i = 1$ to 8 do$\{ X_i := l_i;\}$

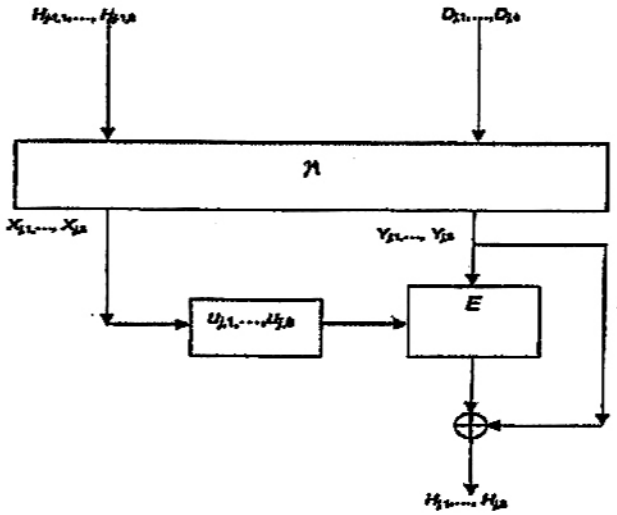
$Y_1 := R_0^L$;
$Y_2 := R_0^R$;
$Y_3 := R_1^L$;
$Y_4 := R_1^R$;
for $i = 1$ to 4 do{ $Y_{4+t} := l_{8+t}$;}

Hàm vòng có dạng sau ($1 \leq j \leq q$)

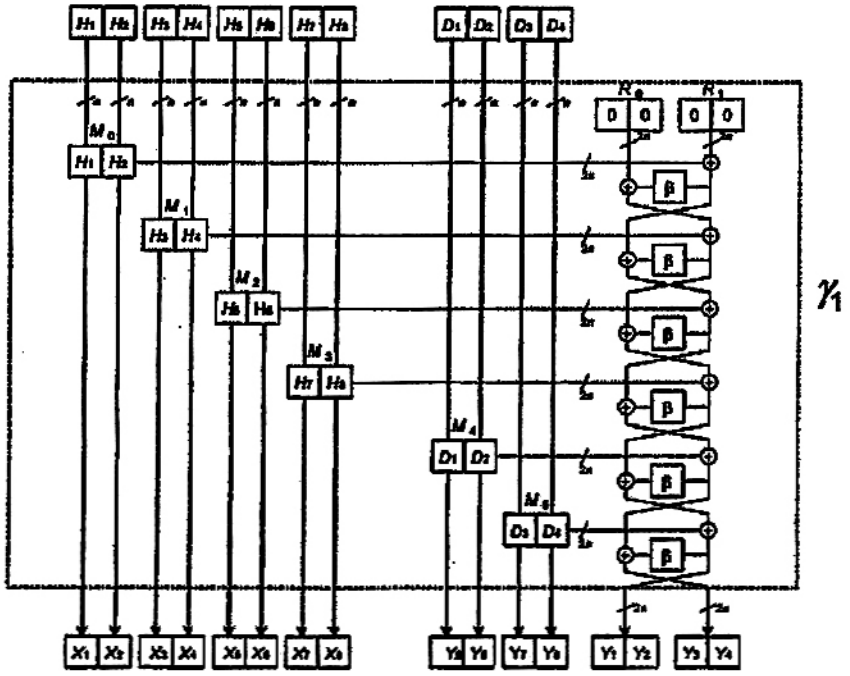
$$\left(X_{j,1}, X_{j,2}, \ldots, X_{j,8}, Y_{j,1}, Y_{j,2}, \ldots, Y_{j,8}\right) := \gamma_1\left(H_{j-1,1}, H_{j-1,2}, \ldots, H_{j-1,8}, D_{j,1}, D_{j,2}, D_{j,3}, D_{j,4}\right);$$

for i = 1 to 8 do $\{H_{j,i} := f_i(X_{j,i}, Y_{j,i});\}$

Hàm vòng được mô tả trong Hình 3 và ánh xạ γ_1 được mô tả trong Hình 4 dưới đây:



Hình 3: Hàm vòng của hàm băm 3



Hình 4: Ánh xạ tuyến tính γ_1 của hàm băm 3

8.6 Phép biến đổi đầu ra

Sau quá trình xử lý thông báo đệm, chuỗi các biến có giá trị $H_{q,1}, H_{q,2}, ..., H_{q,8}$. Thực hiện 4 vòng lặp bổ sung với đầu vào:

$$D_{q+1,i} = H_{q,i}, 1 \le i \le 4$$

$$D_{q+2,i} = H_{q,i+4}, 1 \le i \le 4$$

$$D_{q+3,i} = H_{q,i}, 1 \le i \le 4$$

$$D_{q+4,i} = H_{q,i+4}, 1 \le i \le 4$$

Đầu ra của hàm băm có độ dài L_H là ghép của $H_{q+4,1} \parallel H_{q+4,2}$. Phép biến đổi đầu ra yêu cầu 26 lần mã (trong vòng lặp cuối chỉ 2 lần mã được thực hiện).

9. Hàm băm 4

9.1 Tổng quan

Hàm băm 4 được đặc tả trong phần này cung cấp mã băm có độ dài L_H, trong đó L_H bằng $3n$, với giá trị n chẵn.

CHÚ THÍCH: Hàm băm 4 được mô tả trong [2].

9.2 Lựa chọn tham số

Các tham số L_1, L_2 và L_H của hàm băm 4 được đặc tả trong phần này thỏa mãn $L_1 = 3n$, $L_2 = 9n$, và $L_H = 3n$.

9.3 Phương pháp đệm

Phương pháp đệm sử dụng cho hàm băm 4 được đặc tả trong mục A.3 TCVN 11816-1, trường hợp $r = n$.

9.4 Giá trị khởi tạo

Việc lựa chọn IV dùng cho hàm băm 4 không thuộc phạm vi TCVN 11816-2. IV là một xâu bit có độ dài $9n$ và giá trị của IV có thể được thống nhất và cố định bởi người sử dụng hàm băm.

9.5 Hàm vòng

Phép biến đổi u:

Định nghĩa 9 ánh xạ $u_1, u_2, ..., u_9$ từ không gian mã tới không gian khóa, sao cho:

với tất cả i, j thuộc tập $\{1, 2, ..., 9\}$, $j \ne i$, $u_i(C) \ne u_j(C)$, đối với tất cả giá trị của C

Điều trên có thể đạt được bằng cách cố định các bit khóa ví dụ, có thể cố định 4 bit của khóa tới các giá trị 0000, 0001,..., 1000. Các điều kiện khác có thể áp dụng dựa vào các ánh xạ u_i, ví dụ để tránh các vấn đề liên quan đến khóa yếu hoặc các thuộc tính bù của mã khối.

Hàm f_i

Định nghĩa 9 hàm f_i như sau:

$$f_i(X, Y) = E_{ui(X)}(Y), 1 \le i \le 9.$$

Ánh xạ tuyến tính β:

Xem 8.1 để biết thêm các định nghĩa liên quan đến hàm băm này.

Hàm vòng ϕ có 9 khối mã song song, và 9 dãy biến có độ dài n-bit $H_{j,1}, H_{j,2}, ..., H_{j,9}$

Trong mỗi vòng lặp, 3 khối dữ liệu độ dài n bit $D_{j,1}, D_{j,2}, D_{j,3}$ (độ dài $L_1 = 3n$ bit được kết hợp với đầu ra vòng trước đó của hàm vòng $H_{j-1,1}, H_{j-1,2}, ..., H_{j-1,9}$ (độ dài $L_2 = 9n$ bit) để tạo thành $H_{j,1}, H_{j,2}, ..., H_{j,9}$ (độ dài $L_2 = 9n$ bit).

Hàm vòng dựa vào một ánh xạ tuyến tính γ_2 nhận đầu vào là 12 xâu dài n-bit $I_1, I_2, ..., I_{12}$ và ánh xạ sang 9 xâu độ dài n bit $X_1, X_2, ..., X_9$ và 9 xâu độ dài n bit $Y_1, Y_2, ..., Y_9$. Ánh xạ sử dụng chín xâu phụ có độ dài $2n$ bit $R_0, R_1, R_2, M_0, M_1, ..., M_5$. Ánh xạ γ_2 được xác định theo các bước sau đây:

i) Đặt $H_{0,1}, ..., H_{0,9}$ theo cách sao cho $H_{0,1} \| ... \| H_{0,9} = IV$

ii) for $i = 0$ to 5 do $\{ M_i^L := I_{2i+1}$; $M_i^R := I_{2i+2}$;$\}$

$R_0 := 0$; $R_1 := 0$; $R_2 := 0$;

iii) for $i = 0$ to 5 do {

$B := R_2 \oplus M_i$;

$U := \beta(B)$;

$R_2 := R_1 \oplus U$;

$R_1 := R_0 \oplus U$;

$R_0 := B$; }

iv) for $i = 1$ to 9 do $\{ X_i := I_i$;$\}$

$Y_1 := R_0^L$;

$Y_2 := R_0^R$;

$Y_3 := R_1^L$;

$Y_4 := R_1^R$;

$Y_5 := R_2^L$;

$Y_6 := R_2^R$;

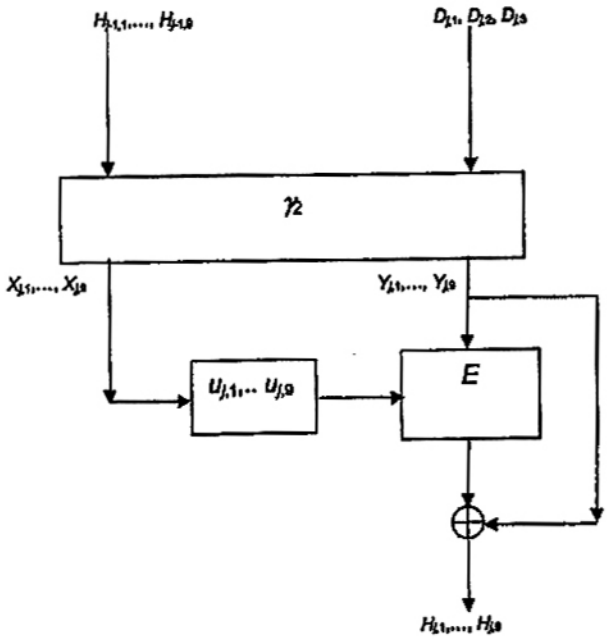
for $i = 1$ to 3 do $\{ Y_{6+i} := I_{9+i}$;$\}$

Hàm vòng có dạng sau ($1 \le j \le q$)

$(X_{j,1}, X_{j,2}, ..., X_{j,9}, Y_{j,1}, Y_{j,2}, ..., Y_{j,9}) := \gamma_2(H_{j-1,1}, H_{j-1,2}, ..., H_{j-1,9}, D_{j,1}, D_{j,2}, D_{j,3})$;

for $i = 1$ to 9 do $\{ H_{j,i} := f_i(X_{j,i}, Y_{j,i})$;$\}$

Hàm vòng được mô tả trong Hình 5 và ánh xạ γ_2 được mô tả trong Hình 6 dưới đây:



Hình 5: Hàm vòng của hàm băm 4

9.6 Phép biến đổi đầu ra

Sau quá trình xử lý bản thông báo đệm, chuỗi các biến có giá trị $H_{q,1}, H_{q,2}, ..., H_{q,9}$ Thực hiện 4 vòng lặp bổ sung với đầu vào

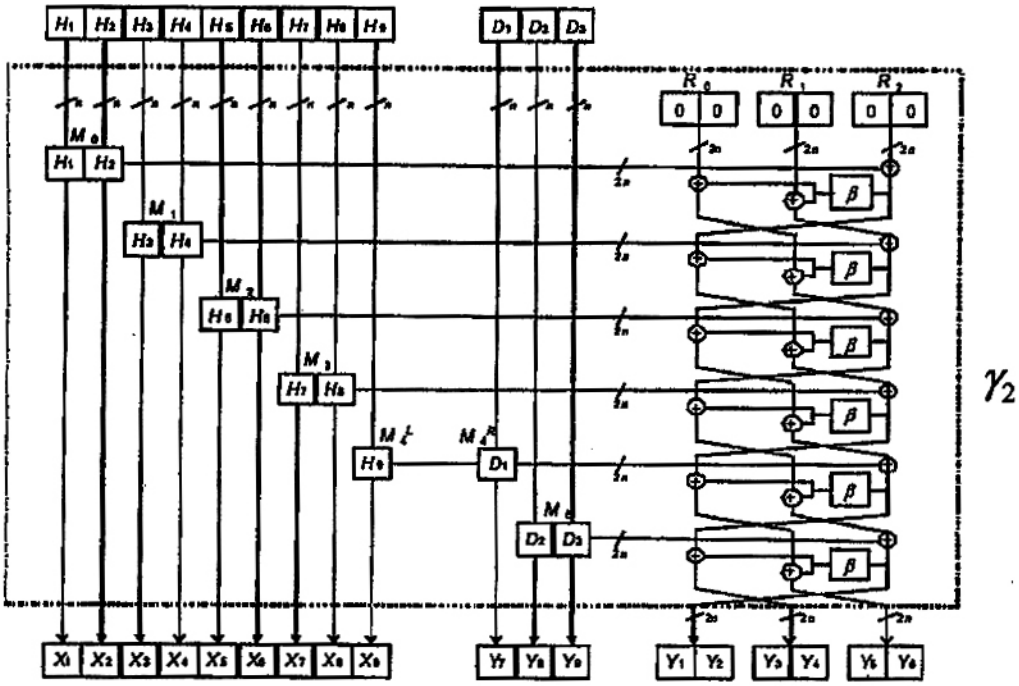
$$D_{q+1,i} = H_{q,i}, 1 \leq i \leq 3$$

$$D_{q+2,i} = H_{q,i+3}, 1 \leq i \leq 3$$

$$D_{q+3,i} = H_{q,i+6}, 1 \leq i \leq 3$$

$$D_{q+4,i} = H_{q,i}, 1 \leq i \leq 3$$

Đầu ra của hàm băm có độ dài L_H là ghép của $H_{q+4,1} \parallel H_{q+4,2} \parallel H_{q+4,3}$. Phép biến đổi đầu ra yêu cầu 30 lần mã (trong vòng lặp cuối chỉ 3 lần mã được thực hiện).



Hình 6: Ánh xạ tuyến tính γ_2 của hàm băm 4

Phụ lục A
(tham khảo)

Sử dụng AES

A.1 Tổng quan

Phụ lục này trình bày một cách sử dụng thuật toán mã khối AES (TCVN11367-3:2016 (ISO/IEC 18033-3)) kết hợp với các hoạt động của hàm băm được đặc tả trong TCVN 11816-2. Các tham số cho AES là n = 128. Độ dài K là 128 bit.

A.2 Hàm băm 1

IV = '52525252525252525252525252525252' (dạng mã thập lục phân)

Phép biến đổi u được chọn theo cách sau: gọi X là biểu diễn nhị phân của xâu 128-bit khi đó $Y = u(X) = X$.

CHÚ THÍCH: Người ta tin rằng việc tìm được va chạm cho hàm vòng và hàm băm cần tới 2^{64} lần mã AES.

A.3 Hàm băm 2

IV^L = '52525252525252525252525252525252' (dạng mã thập lục phân)

IV^R = '25252525252525252525252525252525' (dạng mã thập lục phân)

Phép biến đổi u được lựa chọn như sau: gọi $X = x_1x_2...x_{128}$ là biểu diễn nhị phân của một xâu X độ dài 128 bit Khi đó $Y = u(X)$ là xâu nhận được sau khi chuyển bit x_1 thành giá trị '0'. Kết quả là: $Y = 0x_2x_3...x_{127}x_{128}$. Phép biến đổi u' được lựa chọn như sau: $Y = u'(X)$ là xâu nhận được sau khi chuyển bit x_1 thành giá trị '1'. Kết quả là: $Y = 1x_2x_3...x_{127}x_{128}$.

A.4 Hàm băm 3

$IV_1, IV_2, ..., IV_8$ cùng bằng '52525252525252525252525252525252' (dạng mã thập lục phân)

Phép biến đổi u_1, u_2,..., u_8 được chọn như sau: $X = x_1x_2...x_{128}$ là biểu diễn nhị phân của xâu X độ dài 128 bit. Khi đó $Y = u_i(X)$ là xâu nhận được sau khi chuyển các bit x_1, x_2, x_3 tới giá trị cho trước trong bảng 1 dưới đây.

Bảng A.1 - Hàm băm 3: Giá trị của các bit khóa số 1, 2, 3 trong 8 hàm con

Hàm con i	Hàm con i
1	000
2	001
3	010
4	011
5	100
6	101
7	110

8	111

A.5 Hàm băm 4

$IV_1, IV_2, ..., IV_9$ cùng bằng '52525252525252525252525252525252' (dạng mã thập lục phân)

Phép biến đổi u_1, u_2,..., u_9 sẽ được chọn như sau: $X = x_1x_2...x_{128}$ là biểu diễn nhị phân của xâu X độ dài 128-bit. Khi đó $Y = u_i(X)$ là xâu nhận được sau khi chuyển các bit x_1, x_2, x_3, x_4 tới giá trị cho trước trong bảng 2 dưới đây.

Bảng A.2 - Hàm băm 4: Giá trị của các bit khóa số 1, 2, 3 và 4 trong 9 hàm con

Hàm con i	Hàm con i
1	0000
2	0001
3	0010
4	0011
5	0100
6	0101
7	0110
8	0111
9	1000

Phụ lục B
(tham khảo)

Các ví dụ

B.1 Tổng quan

Phụ lục B đưa ra ví dụ về việc tính toán mã băm cho tất cả các hàm băm được đặc tả trong các mục từ 6 đến 9 TCVN 11816-2, thuật toán mã khối được đặc tả trong phụ lục A TCVN 11816-2; Việc lựa chọn phương pháp đệm được đặc tả trong phụ lục A TCVN 11816-1.

Xâu dữ liệu là mã ASCII 7-bit được mô tả trong [3] (Không chẵn lẻ) cho "Now_is_the_time_for_all_" khi đó biểu thị "_" chỉ các khoảng trống trong biểu diễn hệ thập lục phân.

'4e6f772069732074686520746696d6520666f7220616c6c20'

B.2 Hàm băm 1

Xem A.2.

Phương pháp đệm 1

J	D_j	H_{j-1}	H_j
1	4e6f772069732074	5252525252525252	113fff9a8dfe98c1
	686520746696d6520	5252525252525252	6ed8932aff2dfd9e
2	666f7220616c6c20	113fff9a8dfe98c1	08851dc2ef0dd720
	0000000000000000	6ed8932aff2dfd9e	b76972c33761b988

Phương pháp đệm 2

J	D_j	H_{j-1}	H_j
1	4e6f772069732074	5252525252525252	113fff9a8dfe98c1
	686520746696d6520	5252525252525252	6ed8932aff2dfd9e
2	666f7220616c6c20	113fff9a8dfe98c1	2bf0f0e63c36e020
	8000000000000000	6ed8932aff2dfd9e	780d4835b98590ea

B.3 Hàm băm 2

Phương pháp đệm 1

J	D_J	H^L_{J-1}	H^R_{J-1}
1	4e6f772069732074	5252525252525252	2525252525252525
	68652074696d6520	5252525252525252	2525252525252525
2	666f7220616c6c20	113fff9a8dfe98c1	f3d9241c9087aba2
	0000000000000000	6b704f1114ce1958	6ed8932aff2dfd9e

J	D_J	H^L_J	H^R_J
1		113fff9a8dfe98c1	f3d9241c9087aba2
		6b704f1114ce1958	6ed8932aff2dfd9e
2		4fd1fe4b9ab6699d	0f6990b902b8d6ed
		22db4af462fad373	3fc8fe860ffcf1bc

Phương pháp đệm 2

J	D_J	H^L_{J-1}	H^R_{J-1}
1	4e6f772069732074	5252525252525252	2525252525252525
	68652074696d6520	5252525252525252	2525252525252525
2	666f7220616c6c20	113fff9a8dfe98c1	f3d9241c9087aba2
	8000000000000000	6b704f1114ce1958	6ed8932aff2dfd9e

J	D_J	H^L_J	H^R_J
1		113fff9a8dfe98c1	f3d9241c9087aba2
		6b704f1114ce1958	6ed8932aff2dfd9e
2		4b0505561be3b0d5	8eabdffdcc6641e6
		27b9d7a11fb3e254	c715d6acb73a1506

B.4 Hàm băm 3

Phương pháp đệm 3

$D_{1,1}, D_{1,2}, D_{1,3}, D_{1,4}$	$H_{0,1}, H_{0,2}, H_{0,3}, H_{0,4}$ $H_{0,5}, H_{0,6}, H_{0,7}, H_{0,8}$	$H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4}$ $H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}$
4e6f772069732074	5252525252525252	218f923b370be9a8
686520746963d6520	5252525252525252	9205626148594f7e
666f7220616c6c20	5252525252525252	8a26575e97be292b
8000000000000000	5252525252525252	4aa47e1e8206a2f7
0000000000000000	5252525252525252	1230f84cffde57fd
0000000000000000	5252525252525252	988b6063b3b2d3cf
0000000000000000	5252525252525252	ed5d056582182065
00000000000000c0	5252525252525252	c4fb4f2966b27058
	5252525252525252	6eb4beb7c1b2141f
	5252525252525252	268ba3326336413b
	5252525252525252	c90a43026a380748
	5252525252525252	dcc2521dd2cf3e0d
	5252525252525252	c9851c64fef13ad7
	5252525252525252	11d1a801e2ac052d
	5252525252525252	1e79a495366b8cd9
	5252525252525252	ca1eca9844dc09e5

$D_{2,1}, D_{2,2}, D_{2,3}, D_{2,4}$	$H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4}$ $H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}$	$H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4}$ $H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}$
218f923b370be9a8	218f923b370be9a8	e05e2407707fa017
920562614859df7e	920562614859df7e	44e1156f9ba14704
8a26575e97be292b	8a26575e97be292b	2d6d30d47c1736d0
4aa47e1e8206a2f7	4aa47e1e8206a2f7	597e1750720f4247
1230f84cffde57fd	1230f84cffde57fd	01af4028b2023819
988b6063b3b2d3cf	988b6063b3b2d3cf	40db2f9056889610
ed5d056582182065	ed5d056582182065	450cebc815285244
c4fb4f2966b27058	c4fb4f2966b27058	343f87f2aba57fe8
	6eb4beb7c1b2141f	ccc71fdf4a500dbe
	268ba3326336413b	6fc9f91932ec9cdd
	c90a43026a380748	7332ba30f8c7fab0
	dcc2521dd2cf3e0d	55f859f7c74d4589
	c9851c64fef13ad7	9c8e431285712ab2
	11d1a801e2ac052d	675dc2734f1bac40
	1e79a495366b8cd9	96c578ed26e38a77
	ca1eca9844dc09e5	d62f10e896523889

$D_{3,1}, D_{3,2}, D_{3,3}, D_{3,4}$	$H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4}$ $H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}$	$H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}$ $H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}$
6eb4beb7c1b2141f	e05e2407707fa017	f9c0dfe1c95010b2
268ba33263364413b	44e1156f9ba14704	8f8bcb23eef6daa2
c90a43026a380748	2d6d30d47c1736d0	ea0ad33cc80231dc
dcc2521dd2cf3e0d	597e175072of4247	9790b34d5ec03c0e
c9851c64fef13ad7	01af4028b2023819	861bafcee007b4cd
11d1a801e2ac052d	40db2f9056889610	6dbf787a2654dcf7
1e79a495366b8cd9	450cebc815285244	977028407cb93345
ca1eca9844dc09e5	343f87f2aba57fe8	b163d9e3a005ff7f
	ccc71fdf4a500dbe	5688331e36f098bc
	6fc9f91932ec9cdd	75d83967830d4086
	7332ba30f8c7fab0	6196b975ab6fee13
	55f859f7c74d4589	fff012673153fd87
	9c8e431285712ab2	7f021bdfc73f846f
	675dc2734f1bac40	8e485a4fe0fa1644
	96c578ed26e38a77	6662de8b03a6b64d
	d62f10e896523889	5fb159f1adf26d5d

$D_{4,1}, D_{4,2}, D_{4,3}, D_{4,4}$	$H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}$ $H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}$	$H_{4,1}, H_{4,2}, H_{4,3}, H_{4,4}$ $H_{4,5}, H_{4,6}, H_{4,7}, H_{4,8}$
218f923b370be9a8	f9c0dfe1c95010b2	5a3824dd343c1c91
9205626148 59df7e	8f8bcb23eef6daa2	cd5ddb98d4c0da49
8a26575e97be292b	ea0ad33cc80231dc	f929439b08ccf36b
4aa47e1e8206a2f7	9790b34d5ec03c0e	14ae2fce0d7e2c76
1230f84cffde57fd	861bafcee007b4cd	ff001505ccb8b3a6
988b6063b3b2d3cf	6dbf787a2654dcf7	0a3f4674496b91f1
ed5d056582182065	977028407cb93345	baa3b2b7746c548e
c4fb4f2966b27058	b163d9e3a005ff7f	0676aff6595c6e11
	5688331e36f098bc	3be7c5a7d47b7bbb
	75d83967830d4086	f3f8df583e5633d1
	6196b975ab6fee13	4a87df6f5892eece
	fff012673153fd87	73bf2cd832bfc181
	7f021bdfc73f846f	fead044cd64757ed
	8e485a4fe0fa1644	74477d02b1ecfff2
	6662de8b03a6b64d	a836d76f2117e1f1
	5fb159f1adf26d5d	faa55af85c67f5b2

$D_{5,1}, D_{5,2}, D_{5,3}, D_{5,4}$	$H_{4,1}, H_{4,2}, H_{4,3}, H_{4,4},$ $H_{4,5}, H_{4,6}, H_{4,7}, H_{4,8}$	$H_{5,1}, H_{5,2}, H_{5,3}, H_{5,4}$ $H_{5,5}, H_{5,6}, H_{5,7}, H_{5,8}$
218f923b370be9a8	5a3824dd343c1c91	35af124f4845eb47
9205626148559df7e	cd5ddb98d4c0da49	256a959eb84554e0
8a26575e97be292b	f929439b08ccf36b	3b78dd0c4a1d9bf3
4aa47e1e8206a2f7	14ae2fce0d7e2c76	6c4a4010aa41d8c5
1230f84cffde57fd	ff001505ccb8b3a6	2cd3c769464dc946
988b6063b3b2d3cf	0a3f4674496b91f1	6beb79285da9e383
ed5d056582182065	baa3b2b7746c548e	0c0afc2e1fba5338
c4fb4f2966b27058	0676aff6595c6e11	d1ae7bff8f000138
	3be7c5a7d47b7bbb	08b7bf8d2761947e
	f3f8df583e5633d1	fb950243c0980b87
	4a87df6f5892eece	683447121ef47b19
	73bf2cd832bfc181	b043076cf44d931b
	fead044cd64757ed	af4f446c2e2cf09d
	74477d02b1ecfff2	c73cd1a4383d1f26
	a836d76f2117e1f1	6dfaa1bfc27b6606
	faa55af85c67f5b2	7c88bc330ec798f5

Mã băm

'35af124f4845eb47256a959eb84554e03b78dd0c4a1d9bf36c4a4010aa41d8c5'

B.5 Hàm băm 4

Phương pháp đệm 3

$D_{1,1}, D_{1,2}, D_{1,3}$	$H_{0,1}, H_{0,2}, H_{0,3}, H_{0,4}$ $H_{0,5}, H_{0,6}, H_{0,7}, H_{0,8}, H_{0,9}$	$H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4},$ $H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}, H_{1,9}$
4e6f772069732074	5252525252525252	35373c5888be113e
686520746963d6520	5252525252525252	685b8c0a1c87af82
666f7220616c6c20	5252525252525252	10322300513de264
8000000000000000	5252525252525252	f47883512306b378
0000000000000000	5252525252525252	3ccf820b5a6395f1
00000000000000c0	5252525252525252	6af97874f3ced2e5
	5252525252525252	64dd22a5fc7673d9
	5252525252525252	0deeed557012a0a0
	5252525252525252	546cff0e61ff9597
	5252525252525252	388dbe3bdc3ad0aa
	5252525252525252	276b38ca16da0733
	5252525252525252	1efc14b2188b4510
	5252525252525252	9943f2aa62125370
	5252525252525252	c7ee32c7e95ed829
	5252525252525252	cec2c97e170a75ec
	5252525252525252	2604a9fda4811e4b
	5252525252525252	70f5c66e35c89830
	5252525252525252	3143d2449a614041

$D_{2,1}, D_{2,2}, D_{2,3}$	$H_{1,1}, H_{1,2}, H_{1,3}, H_{1,4},$ $H_{1,5}, H_{1,6}, H_{1,7}, H_{1,8}, H_{1,9}$	$H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4},$ $H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}, H_{2,9}$
35373c5888be113e	35373c5888be113e	44d108f07ce9d076
685b8c0a1c87af82	685b8c0a1c87af82	69f7e43f7c627c48
10322300513de264	10322300513de264	a1948349260589ed
f47883512306b378	f47883512306b378	8ac7d620da4321dd
3ccf820b5a6395f1	3ccf820b5a6395f1	9f148d9316ff1278
6af97874f3ced2e5	6af97874f3ced2e5	4fd51e6f2e35da96
	64dd22a5fc7673d9	8e3d490e4875f1c9
	0deeed557012a0a0	8307522ee5e1f967
	546cff0e61ff9597	5f77293a3205e448
	388dbe3bdc3ad0aa	e56ca64c230ad045
	276b38ca16da0733	2261fbdbcf5df445
	1efc14b2188b4510	3da0a49acdf3288f
	9943f2aa62125370	b5e607b243ae52d5
	c7ee32c7e95ed829	5a49885511f4e946
	cec2c97e170a75ec	d0449c6baf4ba7ef
	2604a9fda4811e4b	c7bae60df90dd97f
	70f5c66e35c89830	3b9364cadd1572f0
	3143d2449a614041	35f52ead4810674a

$D_{1,1}, D_{1,2}, D_{1,3}$	$H_{2,1}, H_{2,2}, H_{2,3}, H_{2,4}$ $H_{2,5}, H_{2,6}, H_{2,7}, H_{2,8}, H_{2,9}$	$H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}$ $H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}, H_{3,9}$
64dd22a5fc7673d9	44d108f07ce9d076	1c76cca901cba5d6
0deeed557012a0a0	69f7e43f7c627c48	b96cd1f95dedca52
546cff0e61ff9597	a1948349260589ed	7ca446c11c899e28
388dbe3bdc3ad0aa	8ac7d620da4321dd	e526ba9d0dcfc49f
276b38ca16da0733	9f148d9316ff1278	a22b3dc0a231acf4
1efc14b2188b4510	4fd51e6f2e35da96	e53f010576888ebc
	8e3d490e4875f1c9	f3b5906d11c43a05
	8307522ee5e1f967	3c36b712ab49681d
	5f77293a3205e448	14b4c16475053acb
	e56ca64c230ad045	f001a8ca0d852e6a
	2261fbdbcf5df445	134a555ea2cdd353
	3da0a49acdf3288f	81e8a2d31d279a6d
	b5e607b243ae52d5	ca55673c5bb6f505
	5a49885511f4e946	6dd666af5dfb707e
	d0449c6baf4ba7ef	1d9d223fcf99f110
	c7bae60df90dd97f	46da8b95c927403b
	3b9364cadd1572f0	7fff085eff33d9e9
	35f52ead4810674a	572fc59a39cb4043

$D_{4,1}, D_{4,2}, D_{4,3}$	$H_{3,1}, H_{3,2}, H_{3,3}, H_{3,4}$	$H_{4,1}, H_{4,2}, H_{4,3}, H_{4,4}$
	$H_{3,5}, H_{3,6}, H_{3,7}, H_{3,8}, H_{3,9}$	$H_{4,5}, H_{4,6}, H_{4,7}, H_{4,8}, H_{4,9}$
9943f2aa62125370	1c76cca901cba5d6	77f6113309990295
c7ee32c7e95ed829	b96cd1f95dedca52	edf3e00dfc8cc0b6
cec2c97e170a75ec	7ca446c11c899e28	8b6516b5c4b6ad38
2604a9fda4811e4b	e526ba9d0dcfc49f	fc571e26e4c5e7ca
70f5c66e35c89830	a22b3dc0a231acf4	1a1db32389fd15d7
3143d2449a614041	e53f010576888ebc	c7a280bd5f4ebd75
	f3b5906d11c43a05	808f8a05ab60e731
	3c36b712ab49681d	05901262a5bf2c19
	14b4c16475053acb	8ac554b724bde667
	f001a8ca0d852e6a	7c06331a8adf8d6e
	134a555ea2cdd353	00bafa8a6f62f8fa
	81e8a2d31d279a6d	3c21d5eabde939c6
	ca55673c5bb6f505	f881454248849271
	6dd666af5dfb707e	7c423d111187e791
	1d9d223fcf99f110	5b4b7ac7fce35e12
	46de8b95c927403b	a99cd3df62ea97fa
	7fff085eff33d9e9	3a3263d188f5ff0b
	572fc59a39cb4043	1fa1c82c69e7f961

$D_{5,1}, D_{5,2}, D_{5,3}$	$H_{4,1}, H_{4,2}, H_{4,3}, H_{4,4}$	$H_{5,1}, H_{5,2}, H_{5,3}, H_{5,4}$
	$H_{4,5}, H_{4,6}, H_{4,7}, H_{4,8}, H_{4,9}$	$H_{5,5}, H_{5,6}, H_{5,7}, H_{5,8}, H_{5,9}$
35373c5888be113e	77f6113309990295	cdac9fdaff9e80f1
685b8c0a1c87af82	edf3e00dfc8cc0b6	c464af255041b323
10322300513de264	8b6516b5c4b6ad38	c8d6aa10e8f147a2
f47883512306b378	fc571e26e4c5e7ca	dedfd219ae0c2a4c
3ccf820b5a6395f1	1a1db32389fd15d7	96e3c0f64293b529
6af97874f3ced2e5	c7a280bd5f4ebd75	8b264625901920d1
	808f8a05ab60e731	d12be37468aaea96
	05901262a5bf2c19	ad5ceb214786b5e8
	8ac554b724bde667	617bb4b093fc5310
	7c06331a8adf8d6e	524f75ead2e90641
	00bafa8a6f62f8fa	acea1480ca6f8442
	3c21d5eabde939c6	850172e1da4bbfb7
	f8814542488849271	ff99ea1fdd4aba2b
	7c423d111187e791	6181aef8cfac2724
	5b4b7ac7fce35e12	cd3647e4deb06d7a
	a99cd3df62ea97fa	9d542fc808ae980c
	3a3263d188f5ff0b	e0fc52b0d4c1d8e1
	1fa1c82c69e7f961	53dc66bfbc492875

Mã băm

'cdac9fdaff9e80f1c464af255041b323c8d6aa10e8f147a2dedfd219ae0c2a4c96e3c0f64293b5298b264625901920d1'

Phụ lục C
(quy định)

Mô đun ASN.1

Phụ lục này liệt kê mô đun ASN.1 của hàm băm sử dụng mã khối n-bit được đặc tả trong TCVN 11816-2

```
Hash-functionsPart2 {
   iso(1) standard(0) hash-functions(10118) part2(2)
      asn1-module(1) hash-functions-using-blockcipher(0) }
   DEFINITIONS EXPLICIT TAGS ::= BEGIN

-- Thuật toán mã hóa định danh -

ALGORITHM ::= CLASS {
&id OBJECT IDENTIFIER UNIQUE,
&Type OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }

-- XUẤT RA TẤT CẢ --

OID ::= OBJECT IDENTIFIER  -- alias

-- Đồng bộ --

is10118-2 OID ::= {iso(1) standard(0) part2(2) }
id-dhf OID ::= { is10118-2 algorithm(0) }

is18033-3 OID ::= { iso(1) standard(0) is18033(18033) part3(3) }
id-bc64  OID ::= { is18033-3 cipher-64-bit(1) }
id-bc128 OID ::= { is18033-3 cipher-128-bit(2) }

-- Chỉ định -

id-hash-1 OID ::= { id-dhf hash-function-1(1) }
id-hash-2 OID ::= { id-dhf hash-function-2(2) }
id-hash-3 OID ::= { id-dhf hash-function-3(3) }
id-hash-4 OID ::= { id-dhf hash-function-4(4) }

EncryptionAlgorithmIdentifier {ALGORITHM:BlockAlgorithms}::= SEQUENCE {
algorithm ALGORITHM.&id({BlockAlgorithms}),
parameters ALGORITHM.&Type({BlockAlgorithms}{@algorithm}) OPTIONAL
}

BlockAlgorithms ALGORITHM ::= {
{ OID id-bc64-tdea PARMS KeyLengthID } |
{ OID id-bc64-misty1 PARMS KeyLength } |
{ OID id-bc64-cast128 PARMS KeyLength } |
{ OID id-bc128-aes PARMS KeyLengthID } |
{ OID id-bc128-camellia PARMS KeyLengthID } |
{ OID id-bc128-seed PARMS KeyLength },
... -- Except additional algorithms --
}
KeyLength ::= INTEGER
KeyLengthID ::= CHOICE {
int KeyLength,
oid OID
```

```
}

END -- Hash-functionsPart2 --
```

Thư mục tài liệu tham khảo

[1] KNUDSEN, L.R. PRENEEL, B. Hash-functions based on block ciphers and quaternary codes, Advances in Crytology, Proc. AsiaCrypt'96, LNCS 1163, K. Kim, T. Matsumoto, Eds., Springer-Verlag, 1996,

[2] KNUDSEN, L.R. PRENEEL, B. Fast and secure hashing based on codes, Advances in Crytology, Proc. Crypto'97, LNCS 1294, B. Kallski, Ed., Springer-Verlag, 1997, pp. 485-498

[3] ISO 646:1991, *Information technology - ISO 7-bit coded character set for information interchange*

[4] COPPERSMITH, D. MATYAS, S.M. PEYRAVIAN, M. Rationale for Bit Fixing in the MDC-2 Algorithm, IBM T.J. Watson Research Center, Yorktown Heights, N.Y, 10598, Research Report RC 21471, May 7 1999

[5] MENEZES ALFRED J. , PAUL C. VAN OORSHOT, Scott A. VANSTONE, *Handbook of Applied Cryptography*. Fifth Printing (August 2001)

[6] KNUDSEN, L.R. MENDEL, F. RECHBERGER, C. THOMSEN, S.S. Cryptanalysis of MDC-2, Advances in Crytology, Proc. Eurocrypt 2009, LNCS 5479, A. Joux, Ed., Springer-Verlag, 2009, pp. 106-120

[7] ISO/IEC 18033-3:2005, *Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers*