TCVN TIÊU CHUẨN VIỆT NAM

TCVN 11816-1:2017
ISO/IEC 10118-1:2016

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HÀM BĂM - PHẦN 1: TỔNG QUAN

Information technology - Security techniques - Hash-functions - Part 1: General

HÀ NỘI - 2017

Mục Lục

Lời nói đầu

TCVN 11816-1 : 2017 hoàn toàn tương đương với ISO/IEC 10118-1:2016.

TCVN 11816-1 : 2017 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.

Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm - Phần 1: Tổng quan

Information technology - Security techniques - Hash-functions - Part 1: General

1 Phạm vi áp dụng

TCVN 11816 đặc tả các hàm băm và được áp dụng trong việc cung cấp các dịch vụ xác thực, toàn vẹn và chống chối bỏ. Hàm băm sử dụng một thuật toán để tạo ra một xâu bit có độ dài cố định từ một xâu bit bất kỳ. Hàm băm có thể sử dụng để:

- Rút gọn một bản tin thành một bản tóm lược để sử dụng làm đầu vào cho cơ chế ký số, và

- Bảo đảm với người dùng tính bí mật của một xâu bit cho trước.

CHÚ THÍCH Hàm băm được đặc tả trong TCVN 11816-1 không liên quan đến việc sử dụng các khóa bí mật. Tuy nhiên, những hàm băm này có thể sử dụng kết hợp với khóa bí mật để tạo ra các mã xác thực thông điệp. Mã xác thực thông điệp (MAC) cũng cấp tính xác thực nguồn gốc dữ liệu cũng như tính toàn vẹn của bản tin. Sử dụng hàm băm được đặc tả trong TCVN 11495-2:2016 (ISO/IEC 9797-2) [1] để tính toán MAC.

TCVN 11816-1 bao gồm các định nghĩa, các ký hiệu, các từ viết tắt và các yêu cầu chung cho tất cả phần khác của TCVN 11816. Tiêu chí để lựa chọn các thuật toán được đặc tả trong các phần tiếp theo của TCVN 11816 này được định nghĩa trong phụ lục B của TCVN 11816-1.

2 Tài liệu viện dẫn

Không có.

3 Thuật ngữ và định nghĩa

Với mục đích của tiêu chuẩn này, các thuật ngữ và định nghĩa sau đây được áp dụng.

Cơ sở dữ liệu các thuật ngữ được duy trì tại các địa chỉ sau:

- IEC Electropedia: http://www.electropedia.org/

- ISO trực tuyến: http://www.iso.org/obp

3.1

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

Hàm băm thỏa mãn tính chất sau: không thể tìm được 2 đầu vào khác nhau với cùng một giá trị đầu ra.

CHÚ THÍCH Việc thực hiện tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể. Tham khảo phụ lục C.

3.2

Xâu dữ liệu (data string)

Xâu bit được dùng làm đầu vào cho hàm băm.

3.3

Mã băm (hash-code)

Xâu bit là đầu ra của hàm băm.

CHÚ THÍCH Trong phần này của tiêu chuẩn chứa đựng một số các thuật ngữ có ý nghĩa giống hoặc tương tự như mã băm ví dụ như: mã phát hiện sửa đổi, mã phát hiện điều khiển, bản tóm lược, kết quả băm, giá trị băm và dấu băm.

3.4

Hàm băm (hash-function)

Hàm mà ánh xạ một xâu bit tới một xâu bit có độ dài xác định thỏa mãn 2 tính chất sau:

- Không thể tìm được một giá trị đầu vào ứng với một giá trị đầu ra cho trước.
- Không thể tìm được một đầu vào thứ 2 khác với đầu vào cho trước mà có cùng đầu ra.

CHÚ THÍCH Việc thực hiện tính toán phụ thuộc vào môi trường và các yêu cầu an toàn cụ thể. Tham khảo phụ lục C.

3.5

Giá trị khởi tạo (initializing-value)

Một giá trị sử dụng để định nghĩa điểm bắt đầu của một hàm băm.

CHÚ THÍCH TCVN 11816-1 chứa đựng một số các thuật ngữ có ý nghĩa giống hoặc tương tự như giá trị khởi tạo ví dụ như vector khởi tạo, giá trị bắt đầu.

3.6

Phép biến đổi đầu ra (output transformation)

Một phép biến đổi hoặc ánh xạ trên đầu ra của bước lặp để nhận được mã băm.

3.7

Đệm (padding)

Bit mở rộng đính kèm cho xâu dữ liệu.

3.8

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 –nó được dùng lặp là một phần của hàm băm, ở đó xâu dữ liệu độ dài L_1 được kết hợp với một xâu đầu ra trước đó có độ dài L_2 hoặc giá trị khởi tạo.

CHÚ THÍCH TCVN 11816-1 chứa đựng một số các thuật ngữ có ý nghĩa giống hoặc tương tự như hàm vòng ví dụ như hàm nén, hàm lặp.

4 Ký hiệu và thuật ngữ viết tắt

4.1 Ký hiệu chung

Trong toàn bộ TCVN 11816, các ký hiệu và các thuật ngữ viết tắt sau đây được áp dụng

B_i	Một byte
D	Dữ liệu
D_i	Một khối nhận được từ xâu dữ liệu D sau quá trình đệm
h	Hàm băm
H	Mã băm
H_i	Một xâu L_2 bit được sử dụng để lưu kết quả trung gian trong quá trình băm
IV	Giá trị khởi tạo
L_1	Độ dài (tính theo bit) của xâu đầu vào thứ nhất trong 2 xâu đầu vào của hàm vòng
L_2	Độ dài (tính theo bit) của xâu thứ hai trong 2 xâu đầu vào của hàm vòng cũng là độ dài xâu đầu ra của hàm vòng và của giá trị khởi tạo
L_X	Độ dài (tính theo bit) của xâu bit X
ϕ	Hàm vòng (phi)
T	Phép biến đổi đầu ra, tức là các phép cắt
$X \parallel Y$	Phép ghép nối của 2 xâu bit X và Y theo một thứ tự nhất định
$X \oplus Y$	Phép xor xâu bit X và Y $(L_X = L_Y)$

4.2 Ký hiệu riêng cho TCVN 11816-1

TCVN 18116-1 sử dụng ký hiệu riêng sau đây:

q	Số các khối trong xâu dữ liệu sau quá trình đệm và phân tách

4.3 Quy ước mã hóa

Trong một số ngữ cảnh thuật ngữ "bit/byte có trọng số cao nhất" và "bit/byte có trọng số nhỏ nhất" có nghĩa là (các bit/byte được xem như các giá trị số học) các bit/byte trái nhất của một khối dữ liệu sẽ có trọng số lớn nhất.

5 Các yêu cầu

Việc sử dụng hàm băm yêu cầu các bên liên quan phải thực hiện các hoạt động chính xác trên cùng một xâu bit dù việc biểu diễn dữ liệu tại môi trường của mỗi thực thể khác nhau có thể khác nhau. Điều này yêu cầu một hoặc nhiều thực thể phải chuyển đổi biểu diễn dữ liệu sang dạng xâu bit phù hợp để có thể áp dụng cho một hàm băm.

Một số hàm băm đặc tả trong TCVN 11816 có yêu cầu về đệm vì vậy xâu dữ liệu có yêu cầu về độ dài. Một và phương pháp đệm được trình bày trong phụ lục A của TCVN 11816-1; một số phương pháp có thể đệm cụ thể sẽ được đặc tả trong từng phần cụ thể của TCVN 11816 khi có yêu cầu.

6 Mô hình tổng quát cho các hàm băm

6.1 Tổng quan

Các hàm băm đặc tả trong TCVN 11816 yêu cầu sử dụng một hàm vòng ϕ. Trong các phần sau của TCVN 11816, một số thay thế cho hàm vòng ϕ sẽ được đưa ra.

Các hàm băm được đặc tả trong các phần sau của TCVN 11816 này cung cấp mã băm có độ dài L_H trong đó L_H nhỏ hơn hoặc bằng giá trị L_2 của hàm vòng ϕ được sử dụng.

6.2 Hoạt động băm

6.2.1 Tổng quan

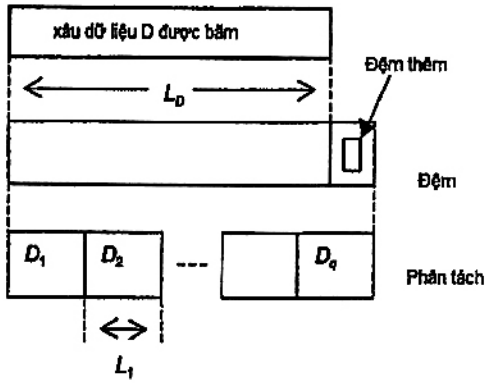
Gọi ϕ là một hàm vòng và IV là giá trị khởi tạo có độ dài L_2. Với các hàm băm được đặc tả trong các phần sau của TCVN 11816 thì giá trị của IV sẽ được cố định đối với một hàm vòng ϕ cho trước. Mã băm H của dữ liệu D sẽ được tính toán theo 4 bước.

6.2.2 Bước 1 (đệm)

Xâu dữ liệu D được đệm thêm các bit để đảm bảo độ dài của nó là bội số của L_1. Xem phục lục A để biết thêm thông tin.

6.2.3 Bước 2 (phân tách dữ liệu)

Dữ liệu D sau khi được chèn thêm các bit phụ sẽ được phân tách thành q khối D_1, D_2,..., D_q có cùng độ dài là L_1 bit. Trong đó D_1 là khối L_1 bit đầu tiên của phần dữ liệu D đã mở rộng, D_2 là khối L_1 bit tiếp theo, tương tự cho đến khối thứ q. Quá trình đệm và phân tách được mô tả trong Hình 1.



Hình 1: Quá trình đệm và phân tách dữ liệu

CHÚ THÍCH Để hiệu quả hơn thì trong một vài trường hợp việc phân tách dữ liệu thành các khối được thực hiện trước khi thực hiện đệm. Việc đệm khi đó sẽ được thực hiện trên khối cuối cùng.

6.2.4 Bước 3 (lặp)

Sau quá trình đệm và phân tách dữ liệu thì $D_1, D_2, \ldots, D_q$ là các khối dữ liệu L_1 bit.

Gọi xâu bit H_0, là giá trị khởi tạo IV thì các xâu $H_1, H_2, \ldots, H_q$, có độ dài L_2 bit được tính toán trong các vòng lặp như sau:

for i from 1 to q:

$$H_i = \phi(D_i, H_{i-1});$$

6.2.5 Bước 4 (Phép biến đổi đầu ra)

Mã băm H nhận được bằng cách thực hiện phép biến đổi T trên H_q, là đầu ra của bước 3 để nhận được mã băm cuối cùng có độ dài L_H bit. Ví dụ: Phép biến đổi T có thể là một phép cắt.

6.3 Sử dụng mô hình tổng quát

Các ví dụ về hàm băm dựa trên mô hình tổng quát sẽ được đặc tả trong các phần tiếp theo của TCVN 11816. Khi đặc tả các hàm băm riêng biệt, các tham số sau phải được định nghĩa:

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

Việc sử dụng mô hình tổng quát của các hàm băm được định nghĩa cũng đưa ra yêu cầu về việc lựa chọn tham số L_H.

Phụ lục A

(quy định)

Các phương pháp đệm

Việc tính toán mã băm được đặc tả trong các phần khác của TCVN 11816 có thể yêu cầu lựa chọn phương pháp đệm. Đầu ra của các phương pháp đệm đều là một xâu dữ liệu có độ dài (tính theo bit) là bội số của L_1. Có 2 phương pháp đệm được trình bày trong phụ lục này.

Các bit đệm (nếu có) không cần phải lưu trữ hoặc truyền tải cùng dữ liệu. Bên xác minh sẽ biết có hay không các bit đệm cũng như phương pháp đệm được sử dụng.

A.1 Phương pháp 1

Dữ liệu cần tính mã băm được thêm vào một bit '1'. Kết quả thu được sau đó lại thêm vào một số bit '0' cần thiết để đạt độ dài yêu cầu.

CHÚ THÍCH Phương pháp 1 luôn luôn yêu cầu bổ sung ít nhất một bit đệm.

A.2 Phương pháp 2

Phương pháp này yêu cầu phải lựa chọn được một tham số r ($r \leq L_1$), ví dụ $r = 64$ và một phương pháp mã hóa độ dài bit của dữ liệu D, ví dụ L_D, là xâu bit có độ dài r. Việc lựa chọn r sẽ giới hạn độ dài của dữ liệu D, $L_D < 2r$

Mã băm được tính toán để đệm cho dữ liệu D được thực hiện như sau:

a) D được ghép với một bit '1'.

b) Kết quả của bước trước đó sẽ được ghép với một số bit '0' trong khoảng $[0, L_1 - 1]$ sao cho độ dài của xâu kết quả đồng dư với $(L_1 - r)$ modulo L_1. Kết quả sẽ là một xâu bit có độ dài là r và là bội nguyên của L_1 hoặc trong trường hợp $r = L_1$ kết quả sẽ là một xâu bit có độ dài chính xác là bội của L_1

c) Thêm vào r bit mã của L_D, sử dụng phương pháp mã hóa đã chọn, sẽ có được một phiên bản đệm của dữ liệu D.

Phụ lục B
(quy định)

Các tiêu chí để đệ trình hàm băm trong bộ tiêu chuẩn TCVN 11816 : 2017 (ISO/IEC 10118) (Tất cả các phần)

B.1 Hướng dẫn để lựa chọn hàm băm

Các hàm băm trong các phần tiếp theo của TCVN 11816 được lựa chọn từ rất nhiều các kỹ thuật đã được sử dụng và công bố. Các ngoại trừ của một số hàm băm đặc biệt không nhất thiết có nghĩa là các kỹ thuật là không an toàn. Các hàm băm được đặc tả là đại diện cho một số kỹ thuật được lựa chọn theo các tiêu chí sau đây (thứ tự các tiêu chí là không có ý nghĩa). Bộ tài liệu 5 của SC27/WG 2 (WG2 SD5) mô tả quá trình ISO/IEC JTC 1/SC 27 trong việc quyết định đưa các hàm băm mới vào TCVN 11816.

Lựa chọn hàm băm được thực hiện theo các khía cạnh sau.

a) An toàn hàm băm, tức là thuật toán được lựa chọn phải chống lại được các tấn công phân tích mã. Các mục tiêu tấn công, các tấn công chung và các tác động của tấn công phân tích mã được định nghĩa trong phụ lục C của TCVN 11816-1. Sự tồn tại các bằng chứng về an toàn hoặc giảm an toàn được xem như các lý do để tranh luận về hàm băm, nó phụ thuộc vào mô hình an toàn và các giả định về bằng chứng. Bản chất của bất kỳ đánh giá nào cũng rất quan trọng, đặc biệt là nó được đánh giá bởi các tổ chức đánh giá có uy tín.

b) Hiệu suất của hàm băm trên các nền tảng điển hình. Nó không những bao gồm các vấn đề về thời gian, không gian, mà còn có hay không có các đặc điểm vượt qua các kỹ thuật tiên tiến khác.

c) Bản chất của bất kỳ vấn đề bản quyền nào ảnh hưởng tới hàm băm.

d) Tính ứng dụng của hàm băm. Tính ứng dụng của hàm băm được đánh giá trong ngữ cảnh của việc nó được sử dụng rộng rãi như thế nào, mức độ các phân tích được công bố và làm thế nào để rà soát nó. Các tiêu chuẩn quốc gia được xem xét để có tính ứng dụng cao.

e) Cấp độ của hàm băm được thừa nhận bởi các tổ chức công nhận (tức là các tổ chức tiêu chuẩn, cơ quan an ninh quốc gia, vv.) hoặc dưới sự điều tra và/hoặc các phân tích của các tổ chức đó.

f) Mức độ chấp nhận hiện tại. Ngoại trừ các xem xét vô hiệu hóa như các quyết định, trong thực tế các tiêu chuẩn được dùng hơn các kỹ thuật được sử dụng.

g) Nói chung, số lượng của các hàm băm được tiêu chuẩn hóa trong mỗi phần của TCVN 11816 là càng nhỏ càng tốt. Có 3 ngoại lệ đối với sự tồn tại của nguyên tắc này.

1) Hai hàm băm có các đặc tính khác nhau, tức là các hàm băm này có độ dài mã băm khác nhau hoặc các hàm băm này có các yêu cầu khác nhau về không gian thực hiện, các yêu cầu về tính toán là rất khác nhau, và cả hai tập thuộc tính đều có ý nghĩa thực tiễn, cả hai hàm băm dạng trên có thể sẽ được tiêu chuẩn hóa.

2) Nói chung với mong muốn có nhiều hàm băm được tiêu chuẩn hóa dựa trên các nguyên tắc căn bản, do vậy nếu một hàm băm bị tổn hại bởi một tấn công phân tích mã thì một hàm băm khác sẽ có cơ hội tốt để an toàn.

3) Nói chung với mong muốn có các hàm băm được tiêu chuẩn hóa với biên độ an toàn cao đối với một mức độ bảo mật của ứng dụng tùy ý.

B.2 Tiêu chí chất lượng tối thiểu đối với việc đệ trình một hàm băm mới

Các tiêu chí được đưa ra trong Điều B.2 nghĩa là việc đệ trình các hàm băm mới sẽ không bao gồm trong các phần tiếp theo của TCVN 11816. Theo trình tự các hàm băm được đề cập đến trong TCVN 11816 phải tuân theo các yêu cầu sau.

a) Phân tích mã đã được thực thi và kết quả đã được biết đến: sẽ không có tấn công phân tích mã được biết đến mà có thể phá được hàm băm. Phụ lục C sẽ cung cấp nhiều hơn các thông tin liên quan đến việc tấn công các hàm băm.

b) Miền công cộng: Việc mô tả hàm băm phải được công bố ít nhất 3 năm trên miền công cộng. Ví dụ, Việc trình bày hàm băm có thể bao gồm chấp nhận các hội thảo và các ấn phẩm nhưng không giới hạn bởi những vấn đề sau:

1) Hội nghị và hội thảo làm việc IACR

i) Hội nghị quốc tế về lý thuyết và các ứng dụng mật mã và an toàn thông tin (Asiacrypt)

ii) Hội nghị quốc tế về mật mã học(Crypto)

iii) Hội nghị quốc tế về lý thuyết và các ứng dụng về kỹ thuật mật mã (Eurocrypt)

iv) Hội thảo quốc tế của phần mềm mã hóa nhanh (FSE)

v) Hội thảo quốc tế của phần cứng mật mã và hệ thống nhúng (CHES)

2) Hội nghị hàng năm của IEEE

i) Hội nghị chuyên đề về an toàn và riêng tư

ii) Hội nghị chuyên đề về nền tảng khoa học máy tính (FOCS)

3) Hội nghị hàng năm của ACM

i) Hội nghị chuyên đề về lý thuyết máy tính (ACM-STOC)

ii) Máy tính và an toàn truyền thông (ACM-CCS)

4) Các Hội nghị quốc tế nổi tiếng với trên 15 năm kinh nghiệm

I) An toàn USENIX

ii) Hội nghị chuyên đề Châu âu về vấn đề nghiên cứu an toàn máy tính (ESORICS)

iii) Hội nghị Australia về an toàn và riêng tư (ACISP)

iv) Mật mã tài chính và an toàn dữ liệu (FC)

v) Hội nghị quốc tế về an toàn thông tin và mật mã học (ICISC)

vi) Hội nghị về việc lựa chọn vùng mật mã (SAC)

5) Các tạp chí nổi tiếng

i) ACM

I) Tạp chí ACM

II) Truyền thông của ACM

ii) Elsevier

I) Truyền thông máy tính

II) Thông tin và tính toán

III) Tạp chí hệ thống và máy tính (JCSS)

IV) Tạp chí các thuật toán riêng biệt

iii) IEEE

I) IEEE các giao dịch trong lý thuyết thông tin

II) IEEE các giao dịch trong máy tính

III) IEEE an toàn và riêng tư

iv) IEICE

I) Các giao dịch trong nền tảng điện tử, truyền thông và khoa học máy tính

II) IEIEC các giao dịch trong thông tin và hệ thống

v) Tạp chí SIAM trong tính toán

vi) Springer

I) Combinatorica

II) Mật mã học và truyền thông

III) Thiết kế, mã và mật mã học

IV) Tạp chí mật mã

VI) Tạp chí quốc tế về an toàn truyền thông

6) Bản chính thức như một tiêu chuẩn bằng tiếng anh được thực hiện sẵn để công bố chung bởi một tổ chức tiêu chuẩn hóa được thừa nhận.

7) Cuộc thi quốc tế với duy nhất mục đích lựa chọn hàm băm hiện đại nhất có thể chạy tối thiểu 2 năm, và ở đây các phân tích và các công bố được mở ra đối với công chúng. Việc đệ trình tới cuộc thi quốc tế này có thể được xem xét phát hành.

c) Tồn tại tài liệu phân tích mã: Trước khi đưa ra, hàm băm phải có các báo cáo về phân tích mã trong các bài báo phản biện hoặc các Hội nghị như liệt kê trong b).

d) Áp dụng công nghiệp: Bằng chứng mạnh phải được cung cấp từ các ứng dụng thương mại có sử dụng hàm băm và khả năng triển khai các ứng dụng trên toàn cầu.

e) Hiệu năng: Cho trước độ dài của mã băm, việc đo lường hiệu suất phải được cung cấp cho nhiều véc-tơ khác nhau như bit/chu kỳ hoặc bit/watt. Một bằng chứng mạnh hàm băm cần phải cung cấp chính là hiệu năng có thể chấp nhận được trên các véc-tơ hiệu năng đã được tối ưu hóa với mục đích so sánh với các hàm băm đã tồn tại trong tiêu chuẩn.

Phụ lục C
(tham khảo)

Các xem xét an toàn

C.1 Các tấn công mục tiêu

Có rất nhiều tấn công mục tiêu liên quan đến hàm băm (Xem ví dụ, tài liệu tham khảo [2]). Đặc biệt quan trọng dưới đây.

Nghiên cứu va chạm – Tấn công mục tiêu là tìm 2 xâu dữ liệu khác nhau M_1, M_2 sao cho $h(M_1) = h(M_2)$.

Nghiên cứu tiền ảnh – Đưa ra xâu bit H có độ dài thích hợp, tấn công mục tiêu là tìm ra xâu M sao cho $h(M) = H$.

Nghiên cứu tiền ảnh thứ 2 – Đưa ra xâu dữ liệu M, tấn công mục tiêu là tìm một xâu dữ liệu M' sao cho $h(M') = h(M)$ và $M \neq M'$.

Tấn công mở rộng độ dài – Đưa ra xâu bit $h(M)$ cho một vài xâu dữ liệu không rỗng M, tấn công mục tiêu là tìm ra bất kỳ xâu dữ liệu M' nào và giá trị của $h(M \| M')$.

CHÚ THÍCH Hiện nay việc phân tích mã của hàm băm hiện đại nhất có liên quan đến việc sử dụng rất nhiều các tấn công mục tiêu mà không liệt kê hết ở phần trên. Những tấn công mục tiêu này được đưa vào xem xét trong quá trình tiêu chuẩn hóa, nhưng chúng chỉ là tiêu chí phụ trợ. Hơn nữa trong các ứng dụng cũng không phải luôn luôn yêu cầu hàm băm kháng lại tất cả các tấn công mục tiêu. Điển hình là chỉ một vài tập con của các yêu cầu này được xem xét.

C.2 Các tấn công chung

Các tấn công chung là tấn công có thể áp dụng đối với tất cả các hàm băm và không tin cậy của việc thiết kế hàm băm.

VÍ DỤ: Một ví dụ về tấn công chung là tìm kiếm một tấn công mạnh vào tiền ảnh. Đưa ra một giá trị của mã băm, kẻ tấn công phân tích giá trị của $h(M)$, và cố gắng thử với các xâu M có thể và so sánh chúng với mã băm đã có. Nếu 2 mã băm đó trùng nhau thì có nghĩa là mục tiêu tìm kiếm tiền ảnh đã đạt được.

C.3 Tác động của tấn công phân tích mã

TCVN 11816 (tất cả các phần), tính kháng của hàm băm có khả năng chống lại các tấn công mục tiêu được đặc tả trong ngữ cảnh để đáp ứng mục tiêu "bất khả thi tính toán". Giống như một chú thích trong định nghĩa, nghĩa của cụm từ bất khả thi tính toán phụ thuộc vào các yêu cầu về an toàn và môi trường cụ thể. Một nghĩa chung chung được sử dụng bởi các học viên ngành an toàn thì đó là một thuộc tính mà việc thực hiện đòi hỏi một lượng lớn tài nguyên tính toán nằm ngoài khả năng sẵn có.

Một cách tiếp cận nghiêm ngặt hơn là so sánh hiệu quả của tấn công đặc biệt chống lại các tấn công chung với cùng một tấn công mục tiêu. Nếu toàn bộ các tấn công phân tích mã được đưa ra cho tấn công mục tiêu là không có hiệu quả hơn với các tấn công chung tương ứng, thì hàm băm được cho là kháng lại được với tấn công mục tiêu. Tuy nhiên, nếu có một tấn công phân tích mã hiệu quả đáng kể hơn các tấn công chung tương ứng, khi đó hàm băm được cho là bị phá.

Hiệu quả của một tấn công phân tích mã được xác định bởi 3 tham số: độ phức tạp tấn công, dung lượng bộ nhớ yêu cầu và xác suất thành công.

Độ phức tạp của tấn công phân tích mã được chuẩn hóa với số lượng các lần gọi theo thứ tự hàm vòng để xác định mức độ phức tạp của nó liên quan đến các tấn công chung. Độ phức tạp này có thể thay đổi tùy theo tính chất của tấn công. Trong hầu hết các trường hợp thì độ phức tạp của thuật toán tấn công có thể chỉ được ước tính.

VÍ DỤ 1 Xem xét một vài tấn công mục tiêu cố định. Giả thiết cho một hàm băm cụ thể, một tấn công với độ phức tạp W, Xác suất thành công P, dung lượng bộ nhớ yêu cầu N, và kèm theo các điều kiện sau:

- N không vượt quá dung lượng bộ nhớ cần thiết cho mọi tấn công chung so với tấn công mục tiêu này;

- P không nhỏ hơn xác suất thành công của bất kỳ tấn công chung nào so với tấn công mục tiêu này;

- W ít hơn đáng kể so với độ phức tạp của bất kỳ tấn công chung nào so với tấn công mục tiêu này.

Trong trường hợp này, hàm băm được xem là bị phá đối với tấn công mục tiêu.

VÍ DỤ 2 Xem xét hàm băm với độ dài mã băm 256 bit. Nếu một tấn công tìm kiếm tiền ảnh với độ phức tạp khoảng 2^{192} số lần gọi hàm vòng, dung lượng bộ nhớ yêu cầu khoảng 2^{20} byte và xác suất thành công gần bằng 1, khi đó hàm băm được cho là bị phá đối với tìm kiếm tiền ảnh.

Thư mục tài liệu tham khảo

[1] TCVN 11495-2:2016 (ISO/IEC 9797-2): Công nghệ thông tin – Các kỹ thuật an toàn – Mã xác thực thông điệp – Phần 2: Các cơ chế sử dụng hàm băm chuyên dụng (Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function).

[2] PRENEEL B. Analysis and design of Cryptographic Hash Function, Doctoral Dissertation, Katholieke Universiteit Leuven, 1993.