TCVN TIÊU CHUẨN QUỐC GIA

TCVN 12854-5 : 2020
ISO/IEC 29192-5 : 2016

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – MẬT MÃ HẠNG NHẸ – PHẦN 5: CÁC HÀM BĂM

Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions

HÀ NỘI - 2020

Mục Lục

Lời nói đầu

TCVN 12854-5: 2020 hoàn toàn tương đương với ISO/IEC 29192-5:2016.

TCVN 12854-5: 2020 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 12854 (ISO/IEC 29192) *Công nghệ thông tin – Các kỹ thuật an toàn – Mật mã hạng nhẹ* gồm các tiêu chuẩn sau:

- TCVN 12854-1 (ISO/IEC 29192-1:2012): 2020 (ISO/IEC 29192-1:2012) Phần 1: Tổng quan

- TCVN 12854-2: 2020 (ISO/IEC 29192-2:2012) Phần 2: Mã khối

- TCVN 12854-3: 2020 (ISO/IEC 29192-3:2012) Phần 3: Mã dòng

- TCVN 12854-4: 2020 (ISO/IEC 29192-4:2013) Phần 4: Các cơ chế sử dụng kỹ thuật phi đối xứng.

- TCVN 12854-5: 2020 (ISO/IEC 29192-5:2016) Phần 5: Các hàm băm.

Công nghệ thông tin – Các kỹ thuật an toàn – Mật mã hạng nhẹ – Phần 5: Các hàm băm

Information technology - Security techniques - Lightweight cryptography - Part 5: Hash-functions

1 Phạm vi áp dụng

Tiêu chuẩn này quy định ba hàm băm phù hợp cho các ứng dụng yêu cầu triển khai mật mã hạng nhẹ.

- PHOTON: hàm băm hạng nhẹ với kích thước hoán vị lần lượt là 100, 144, 196, 256 và 288 bit tương ứng với độ dài mã băm là 80, 128, 160, 224 và 256 bit.
- SPONGENT: hàm băm hạng nhẹ với các kích thước hoán vị lần lượt là 88, 136, 176, 240 và 272 bit tương ứng với độ dài mã băm là 88, 128, 160, 224 và 256 bit.
- Lesamnta-LW: một hàm băm hạng nhẹ với kích thước hoán vị 384 bit và độ dài mã băm là 256 bit.

TCVN 12854-1 (ISO/IEC 29192-1:2012) (ISO/IEC 29192-1:2012) sẽ được tham chiếu cho các yêu cầu đối với mật mã hạng nhẹ.

2 Tài liệu viện dẫn

Các tài liệu sau đây, toàn bộ hoặc một phần, được dùng để tham chiếu trong tiêu chuẩn này và là không thể thiếu được đối với ứng dụng của nó. Đối với các tài liệu viên dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 12854-1 (ISO/IEC 29192-1:2012) (ISO/IEC 29192-1:2012), Công nghệ thông tin - Các kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 1: Tổng quan

3 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này, các thuật ngữ và định nghĩa sau được áp dụng.

3.1

Pha hấp thụ (absorbing phase)

Pha đầu vào của một hàm Sponge.

[NGUỒN: tham khảo [4]]