TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11763:2020

ISO/IEC 18032 : 2005

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – BỘ TẠO SỐ NGUYÊN TỐ

Information technology – Security techniques – Prime number generation

HÀ NỘI - 2020

Mục Lục

Lời nói đầu

TCVN 13176 : 2020 hoàn toàn tương đương với ISO/IEC 18032 : 2005.

TCVN 13176 : 2020 (ISO/IEC 18032:2005) 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.

Công nghệ thông tin – Các kỹ thuật an toàn – Bộ sinh số nguyên tố

Information technology – Security techniques – Prime number generation

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các phương pháp sinh và kiểm tra số nguyên tố được yêu cầu trong các giao thức và thuật toán mật mã.

Đầu tiên, tiêu chuẩn này quy định các phương pháp để kiểm tra xem một số có phải là số nguyên tố hay không. Các phương pháp kiểm tra đưa ra trong tiêu chuẩn này có thể được chia thành 2 nhóm:

- Các phương pháp kiểm tra tính nguyên tố xác suất, các phương pháp này có một xác suất lỗi nhỏ. Tất cả các phép kiểm tra xác suất được quy định ở đây có thể kết luận một hợp số là số nguyên tố. Một phép kiểm tra quy định tại đây có thể xác định một số nguyên tố là hợp số.

- Các phương pháp kiểm tra tất định, đảm bảo đưa ra kết luận chính xác. Những thuật toán này được gọi là các chứng chỉ tính nguyên tố.

Thứ hai, tiêu chuẩn này quy định các phương pháp sinh số nguyên tố. Một lần nữa, cả hai phương pháp xác xuất và tất định được quy định tại đây.

CHÚ THÍCH Những độc giả có nền tảng về lý thuyết thuật toán có thể đã có những kiến thức về những thuật toán xác suất và tất định. Chúng tôi nhấn mạnh rằng các thuật toán tất định trong tiêu chuẩn này vẫn sử dụng các bit ngẫu nhiên, và "tính tất định" chỉ hàm ý khẳng định rằng đầu ra là đúng với xác suất bằng 1.

Phụ lục B mô tả các biến của các phương pháp sinh số nguyên tố để có thể đáp ứng các yêu cầu mật mã cụ thể.

Các phương pháp sinh, chứng minh và xác nhận tính nguyên tố được định nghĩa bởi Tiêu chuẩn này được áp dụng cho các hệ thống mật mã dựa trên các thuộc tính của số nguyên tố.

CHÚ THÍCH Các thông số kỹ thuật của các phép kiểm tra trong Tiêu chuẩn này định nghĩa các thuộc tính được kiểm tra trong hình thức đơn giản nhất có thể. Theo đó các thông số kỹ thuật trực tiếp sẽ không nhất thiết tạo ra các triển khai hiệu quả nhất. Đặc biệt trong trường hợp kiểm tra Frobenius-Grantham.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với những tài liệu có năm công bố, chỉ áp dụng bản được nêu. Đối với tài liệu không có năm công bố, phiên bản cuối cùng được áp dụng (bao gồm sửa đổi, bổ sung)