**TCVN** **TIÊU CHUẨN QUỐC GIA**

# TCVN 11367-1:2016
# ISO/IEC 18033-1:2015

Xuất bản lần 1

# CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - THUẬT TOÁN MẬT MÃ - PHẦN 1: TỔNG QUAN

***Information technology - Security techniques - Encryption algorithms - Part 1: General***

**HÀ NỘI - 2016**

## Mục Lục

## Lời nói đầu

TCVN 11367-1:2016 hoàn toàn tương đương với ISO/IEC 18033-1:2015.

TCVN 11367-1:2016 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 11367 *Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã* gồm 04 phần:

- TCVN 11367-1:2016 (ISO/IEC 18033-1:2015) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 1: Tổng quan.

- TCVN 11367-2:2016 (ISO/IEC 18033-2:2006) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 2: Mật mã phi đối xứng.

- TCVN 11367-3:2016 (ISO/IEC 18033-3:2010) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối.

- TCVN 11367-4:2016 (ISO/IEC 18033-4:2011) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 4: Mã dòng.

## Giới thiệu

Các phần của tiêu chuẩn này xác định các hệ mật nhằm mục đích bảo mật dữ liệu. Việc đưa các hệ mật vào tiêu chuẩn này nhằm đẩy mạnh việc sử dụng chúng với "chất lượng tốt nhất" hiện nay trong các kỹ thuật mật mã.

Mục tiêu chính của các kỹ thuật mã hóa là bảo vệ tính bí mật của dữ liệu được lưu trữ hoặc truyền đi. Thuật toán mã hóa được áp dụng vào dữ liệu (thường được gọi là bản rõ), từ đó nhận được dữ liệu được mã hóa (hay gọi là bản mã). Quá trình này được biết đến như là mã hóa. Thuật toán mã hóa cần được thiết kế sao cho bản mã không cung cấp thông tin về bản rõ, ngoại trừ có thể độ dài của nó. Gắn liền với thuật toán mã hóa là thuật toán giải mã, biến đổi ngược bản mã thành bản rõ gốc.

Mật mã làm việc kết hợp với khóa. Trong hệ mật đối xứng, khóa được sử dụng để mã hóa và giải mã là như nhau. Trong hệ mật phi đối xứng, khóa để mã hóa và giải mã khác nhau nhưng liên quan với nhau. Trong các phần của bộ tiêu chuẩn này, TCVN 11367-2:2016 (ISO/IEC 18033-2) và ISO/IEC 18033-5 dành cho hai lớp hệ mật phi đối xứng khác nhau là hệ mật phi đối xứng tiêu chuẩn (hay hệ mật phi đối xứng), và mật mã dựa trên định danh. TCVN 11367-3:2016 (ISO/IEC 18033-3) và TCVN 11367-4:2016 (ISO/IEC 18033-4) dành cho hai lớp mật mã đối xứng khác nhau là mã khối và mã dòng.

**TIÊU CHUẨN QUỐC GIA** **TCVN 11367-1:2016**

# Công nghệ thông tin - Các kỹ thuật an toàn - Thuật toán mật mã - Phần 1: Tổng quan

*Information technology - Security techniques - Encryption algorithms - Part 1: General*

## 1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp các định nghĩa sẽ được dùng trong các phần tiếp theo của bộ tiêu chuẩn TCVN 11367 (ISO/IEC 18033). Tiêu chuẩn này đưa ra bản chất của mã hóa, mô tả các khía cạnh chung của việc áp dụng mật mã và các tính chất của mã hóa. Các tiêu chí sử dụng để lựa chọn thuật toán mật mã được đặc tả trong các phần tiếp theo của bộ TCVN 11367 (ISO/IEC 18033) được xác định tại Phụ lục A, Phụ lục B.

## 2 Thuật ngữ và định nghĩa

Trong tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa dưới đây:

**2.1**

**Mật mã phi đối xứng** (asymmetric cipher)

Thuật ngữ tương đương **"Hệ mật phi đối xứng"** (2.3)

**2.2**

**Kỹ thuật mật mã phi đối xứng** (asymmetric cryptographic technique)

Kỹ thuật mật mã sử dụng hai phép biến đổi liên quan với nhau, phép biến đổi công khai (được xác định bởi khóa công khai) và phép biến đổi riêng (được xác định bởi khóa riêng).

CHÚ THÍCH Hai phép biến đổi này có tính chất là cho biết phép biến đổi khóa công khai, về mặt tính toán không thể thu được phép biến đổi khóa riêng.

[ISO/IEC 11770-1:2010, 2.1]

**2.3**

**Hệ mật phi đối xứng** (asymmetric encipherment system, asymmetric encryption system)

Hệ thống dựa vào các kỹ thuật mật mã phi đối xứng, ở đó phép biến đổi khóa công khai được sử dụng để mã hóa và phép biến đổi khóa riêng dùng để giải mã.

[ISO/IEC 9798-1:2010, 3.2]

**2.4**

**Cặp khóa phi đối xứng** (asymmetric key pair)

Cặp khóa liên quan với nhau cho kỹ thuật mật mã phi đối xứng, ở đó khoá riêng xác định phép biến đổi riêng và khóa công khai xác định phép biến đổi công khai.

**2.5**

**Tấn công** (attack)

Thuật toán thực hiện tính toán và tạo các truy vấn đến các thuật toán mã hóa để mã hóa và/hoặc giải mã các văn bản được chọn thích ứng theo khóa bí mật đơn, với mục đích khôi phục hoặc là khóa bí mật, hoặc là bản rõ chưa biết của bản mã xác định, trong đó bản mã có thể được chọn thích ứng nhưng là một truy vấn giải mã không được phép.

**2.6**

**Chi phí tấn công** (attack cost)

Tỷ lệ giữa độ phức tạp trung bình của tấn công thuật toán đo bằng số lượng các lời gọi đến các thuật toán mã hóa thực hiện bởi các cuộc tấn công, với xác suất thành công của các cuộc tấn công đó.

CHÚ THÍCH Sử dụng ký hiệu được định nghĩa trong điều 3.1, chi phí tấn công là tỉ lệ W/P.

**2.7**

**Khối** (block)

Xâu bit có độ dài xác định

**2.8**

**Mã khối** (block cipher)

Hệ mật đối xứng với tính chất là thuật toán mã hóa thao tác trên một khối của bản rõ, nghĩa là trên một xâu bit có độ dài xác định, kết quả cho ra một khối của bản mã.

**2.9**

**Mật mã** (cipher)

Thuật ngữ tương đương **"Hệ mật"** (2.17)

**2.10**

**Bản mã** (ciphertext)

Dữ liệu đã được biến đổi để giấu thông tin trong đó

[ISO/IEC 10116:2006, 3.3]

**2.11**

**Bản rõ** (cleartext, plaintext)

Thông tin chưa được mã hóa

[ISO/IEC 10116:2006, 3.11]

**2.12**

**Tấn công phân tích mã** (cryptanalytic attack)

Tấn công chống lại mật mã mà sử dụng các thuộc tính của mật mã

CHÚ THÍCH 1 Mỗi tấn công phân tích mã có mô hình tấn công riêng của nó, một số trong đó có thể hoặc không thể áp dụng được để triển khai thực hiện cụ thể. Kể từ khi áp dụng mật mã, nói chung không biết đến các nhà thiết kế mật mã, tất cả các mô hình có thể có trong các thiết lập khóa đơn được xem xét khi đánh giá tính an toàn của thuật toán.

CHÚ THÍCH 2 Các tấn công phân tích mã không bao gồm sự thực thi các tấn công cụ thể, ví dụ phân tích kênh kề.

**2.13**

**Giải mã** (decipherment, decryption)

Phép toán ngược với phép mã hóa tương ứng

[ISO/IEC 11770-1:2010, 2.6, được sửa đổi]

**2.14**

**Thuật toán giải mã** (decipherment algorithm, decryption algorithm)

Quá trình biến đổi bản mã thành bản rõ.

**2.15**

**Mã hóa** (encipherment, encryption)

Phép biến đổi (khả nghịch) dữ liệu bởi thuật toán mật mã để tạo ra bản mã, tức là giấu nội dung thông tin của dữ liệu.

[ISO/IEC 9797-1:2011, 3.6, được sửa đổi]

**2.16**

**Thuật toán mã hóa** (encipherment algorithm, encryption algorithm)

Quá trình biến đổi bản rõ thành bản mã

**2.17**

**Hệ mật** (encipherment system, encryption system)

Kỹ thuật mật mã sử dụng để bảo vệ bí mật dữ liệu bao gồm ba quá trình thành phần: thuật toán mã hóa, thuật toán giải mã và phương pháp tạo khóa.

**2.18**

**Tấn công tổng quát** (generic attack)

Tấn công chống lại mật mã mà không dựa trên thiết kế mật mã và có thể sử dụng để khôi phục khóa mã hóa hoặc bản rõ

**2.19**

**Mật mã dựa trên định danh** (identity-based cipher)

Thuật ngữ tương đương hệ mật dựa trên định danh

**2.20**

**Hệ mật dựa trên định danh** (identity-based encryption system)

Mật mã phi đối xứng, trong đó thuật toán mã hóa có một xâu tùy ý như là một khóa công khai

**2.21**

**Khóa** (key)

Dãy các kí tự điều khiển sự vận hành của các thuật toán mật mã (ví dụ, phép mã hóa, giải mã)

[ISO/IEC 11770-1:2012, 2.12, được sửa đổi]

**2.22**

**Khóa dòng** (keystream)

Dãy các kí tự giả ngẫu nhiên bí mật, được sử dụng bởi các thuật toán mã hóa và giải mã của mã dòng.

CHÚ THÍCH Nếu kẻ tấn công biết được một phần khoá dòng thì bằng tính toán kẻ tấn công không thể thu được thêm bất kì thông tin nào về phần còn lại của khoá dòng.

**2.23**

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

Mã khối với tính chất là các khối của bản rõ và bản mã đều có độ dài n bit

[ISO/IEC 10116:2006, 3.10]

**2.24**

**Bản rõ** (plaintext, cleartext)

Thông tin chưa được mã hóa

[ISO/IEC 10116:2006, 3.11]

**2.25**

**Khóa riêng** (private key)

Khóa thuộc cặp khóa phi đối xứng của thực thể chỉ được sử dụng bởi thực thể đó

CHÚ THÍCH Thông thường khoá riêng không được tiết lộ.

[ISO/IEC 11770-1: 2010, 2.35, được sửa đổi]

**2.26**

**Khóa công khai** (public key)

Khóa thuộc cặp khóa phi đối xứng của thực thể có thể được công bố công khai

[ISO/IEC 11770-1:2010, 2.36, được sửa đổi]

**2.27**

**Khóa bí mật** (secret key)

Khóa sử dụng cho kỹ thuật mật mã đối xứng và được dùng bởi một tập thực thể xác định

[ISO/IEC 11770-3:2008, 3.35]

**2.28**

**Độ mạnh an toàn** (security strength)

Con số liên quan đến số lượng công việc (ví dụ: số phép tính) được yêu cầu để phá vỡ một thuật toán mật mã hay một hệ thống

CHÚ THÍCH 1 Đối với khối phục khóa, độ mạnh an toàn của $n$ bit có nghĩa là khối lượng công việc cần thiết để phá vỡ hệ thống mật mã tương đương với $2^n$ thực thi của hệ thống mật mã. Để biết thêm thông tin về các ứng dụng của độ an toàn để chọn thuật toán mật mã cho tiêu chuẩn này, xem C.1.4.

CHÚ THÍCH 2 Trong tiêu chuẩn ISO/IEC 29192, độ mạnh an toàn được chỉ rõ bằng bit, ví dụ: 80,112,128,192 hoặc 256.

**2.29**

**Mã dòng tự đồng bộ** (self-synchronous stream cipher)

Mã dòng với tính chất là các kí tự của khóa dòng được tạo như một hàm của khóa bí mật và một số cố định các bit của bản mã trước đó.

**2.30**

**Mã dòng** (stream cipher)

Hệ mật đối xứng với tính chất là thuật toán mã hóa bao gồm tổ hợp một dãy các kí tự của bản rõ với dãy các kí tự của khóa dòng, mỗi lần một kí tự, sử dụng một hàm khả nghịch.

CHÚ THÍCH Phân biệt hai loại mã dòng mã dòng đồng bộ và mã dòng tự đồng bộ, được phân biệt bởi phương pháp nhận được khóa dòng.

**2.31**

**Mật mã đối xứng** (symmetric cipher)

Thuật ngữ tương đương **"Hệ mật đối xứng"** (2.33)

**2.32**

**Kỹ thuật mật mã đối xứng** (symmetric cryptographic technique)

Kỹ thuật mật mã sử dụng cùng một khóa bí mật cho cả người gửi và người nhận.

CHÚ THÍCH Không biết khóa bí mật, bằng tính toán không thể xác định được phép biến đổi của người gửi và người nhận.

**2.33**

**Hệ mật đối xứng** (symmetric encipherment system, symmetric encryption system)

Hệ mật dựa trên kỹ thuật mật mã đối xứng

**2.34**

**Mã dòng đồng bộ** (synchronous stream cipher)

Mã dòng với tính chất là các kí tự của khóa dòng được tạo như một hàm của khóa bí mật và có thể, véc tơ khởi tạo, độc lập với bản mã và bản rõ.

## 3 Ký hiệu và từ viết tắt

### 3.1 Ký hiệu

| | |
|---|---|
| $n$ | Số nguyên |
| $P$ | Xác suất thành công của một tấn công thành công lên một thuật toán mật mã |
| $W$ | Khối lượng công việc hoặc độ phức tạp của một tấn công, đo bằng số lượng lời gọi đến thuật toán mật mã |

### 3.2 Từ viết tắt

| Từ viết tắt | Tiếng Anh | Tiếng Việt |
|---|---|---|
| ECB | Electronic codebook | Chế độ sách mã điện tử |
| MAC | Message authentication code | Mã xác thực thông báo |
| SC | Subcommittee | Tiểu ban kỹ thuật |
| SD | Standing document | Tài liệu hiện hành |
| WG | Working group | Nhóm công tác |

## 4 Bản chất của mật mã

### 4.1 Mục đích của mã hóa

Mục đích chủ yếu của các hệ mật là bảo vệ tính bí mật của dữ liệu được lưu trữ hoặc truyền đi. Các thuật toán mật mã đạt được mục tiêu này bằng cách biến đổi bản rõ thành bản mã sao cho bằng cách tính toán không thể tìm ra bất kì thông tin nào về nội dung của bản rõ từ bản mã, trừ khi biết được khóa giải mã. Tuy nhiên, trong nhiều trường hợp phép mã hóa nói chung không giấu được độ dài của bản rõ, vì thông thường độ dài bản mã bằng hoặc lớn hơn một ít so với độ dài bản rõ tương ứng.

Một điều quan trọng nữa cần nhấn mạnh là mã hoá không phải luôn luôn bảo vệ được tính toàn vẹn của dữ liệu gốc. Trong nhiều trường hợp, không cần biết khóa, kẻ tấn công vẫn có thể thay đổi bản mã với hiệu quả dự đoán được lên bản rõ được khôi phục. Để đảm bảo tính toàn vẹn và tính xác thực của

dữ liệu, thông thường phải sử dụng các kỹ thuật bổ sung khác, như các kỹ thuật được mô tả trong ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 14888, ISO/IEC 19772 và ISO/IEC 29192.

### 4.2 Mã đối xứng và phi đối xứng

Mật mã làm việc trong sự kết hợp cùng với khóa

Trong *mật mã đối xứng* các thuật toán mã hóa và giải mã sử dụng cùng một khóa bí mật. Để thực hiện các phép mã hóa và giải mã cần biết khóa bí mật này, do đó chỉ có hai phía có thẩm quyền tiếp cận dữ liệu mới được biết khóa bí mật này.

Trong *mật mã phi đối xứng* mã hóa và giải mã sử dụng các khóa khác nhau nhưng liên quan với nhau. Do đó các khóa được tạo ra ở dạng các *cặp khoá* tương ứng, trong đó một khóa là khóa mã hóa, khóa kia là khóa giải mã. Thậm chí biết khóa mã hóa, giả thiết là bằng tính toán không thể để biết bất kì thông tin nào về bản rõ từ bản mã tương ứng. Có khả năng, trong nhiều tình huống có thể tạo ra khóa mã hóa một cách công khai, nên khóa này thường được gọi là *khóa công khai*, còn khóa giải mã tương ứng thì chỉ có một người sở hữu và được giữ bí mật (nên khoá này được gọi là khóa riêng hay khóa bí mật). Bất kì ai biết khóa mã hóa công khai sẽ có khả năng mã hóa dữ liệu gửi cho người giữ khóa bí mật tương ứng, chỉ có khóa giải mã bí mật mới giải mã được dữ liệu đã mã hóa đó.

CHÚ THÍCH Trong nhiều trường hợp mật mã phi đối xứng đòi hỏi nhiều hơn các phép toán phức tạp về mặt tính toán so với mật mã đối xứng, nên thông thường không được sử dụng để mã hóa khối lượng dữ liệu lớn, mà sử dụng để mã hóa các khóa phiên trong liên lạc (những khóa phiên này sau đó được dùng với mật mã khóa đối xứng). Tuy vậy một số mật mã phi đối xứng trong TCVN 11367-2:2016 (ISO/IEC 18033-2) được thiết kế theo cách thức sao cho chúng phù hợp với việc mã hóa khối lượng dữ liệu lớn.

TCVN 11367-2:2016 (ISO/IEC 18033-2) và ISO/IEC 18033-5 dành cho hai lớp hệ mật phi đối xứng khác nhau là hệ mật phi đối xứng tiêu chuẩn (hay hệ mật phi đối xứng), và mật mã dựa trên định danh. TCVN 11367-3:2016 (ISO/IEC 18033-3) và TCVN 11367-4:2016 (ISO/IEC 18033-4) dành cho hai lớp mật mã đối xứng khác nhau là mã khối và mã dòng.

### 4.3 Quản lý khóa

Việc sử dụng tất cả các loại hình mật mã đều căn cứ vào vấn đề quản lý khoá mật mã. Tất cả các loại hình mật mã, cả đối xứng và phi đối xứng, đòi hỏi tất cả các bên sử dụng mật mã để tiếp cận khóa cần thiết. Điều này làm phát sinh nhu cầu *quản lý khóa*. Quản lý khóa bao gồm tạo khóa, phân phối khóa và tiếp tục quản lý khóa sau đó. Cấu trúc đầy đủ của quản lý khóa được đưa ra tại tiêu chuẩn ISO/IEC 11770-1.

Bài toán quản lý khóa phụ thuộc vào việc khóa dùng cho mật mã đối xứng hay phi đối xứng. Với mật mã đối xứng, khóa bí mật được tạo ra theo thỏa thuận và dùng chung cho các cặp (hoặc nhóm lớn) thực thể. Với mật mã khóa công khai cần tạo ra từng cặp khóa, trong đó khóa công khai được phân phối theo cách sao cho đảm bảo tính xác thực của chúng. Trong mật mã dựa trên định danh, khóa công khai là xâu dữ liệu tùy ý, thường được chọn từ một số thông tin nào liên quan đến người giải mã (decryptor).

Các phương pháp thiết lập khóa bí mật dùng chung sử dụng kỹ thuật mật mã khóa công khai được đặc tả tại ISO/IEC 11770-2. Các phương pháp thiết lập khóa bí mật dùng chung sử dụng kỹ thuật mật mã

phi đối xứng được đặc tả trong ISO/IEC 11770-3. Tiêu chuẩn này cũng mô tả các các kỹ thuật phân phối khóa công khai tin cậy sử dụng kỹ thuật mật mã phi đối xứng.

## 5. Sử dụng mật mã và các tính chất của mật mã

### 5.1 Mật mã phi đối xứng

Thuật toán mã hóa trong mật mã phi đối xứng xác định một ánh xạ từ tập hợp các thông báo rõ có thể (thường là tập hợp các xâu bit) vào tập hợp các thông báo đã mã hóa (thường cũng là tập hợp các xâu bit). Tập các thông báo có thể và tập các bản mã phụ thuộc vào cả việc chọn mật mã và cặp khóa.

Đối với mật mã phi đối xứng, thuật toán mã hóa phụ thuộc vào khóa công khai, trong khi việc giải mã phụ thuộc vào khóa bí mật. Bởi vậy nếu các khối mã tương ứng với các khối của bãn rõ có thể tính được thì không ai, ngoài người sở hữu khóa bí mật, có thể suy ra được khối bản rõ tương ứng với khối bản mã đã chọn. Tuy nhiên nếu kẻ thu chặn bản mã biết được khóa công khai được sử dụng để sinh ra bản mã, đồng thời biết rằng bản rõ được chọn từ một tập hợp nhỏ các bản rõ có thể, thì anh ta hoàn toàn có thể tính ra bản rõ bằng phương pháp vét cạn tất cả các bản rõ có thể.

Kết quả là để đạt được mức an toàn mong muốn, cần phải kết hợp dữ liệu ngẫu nhiên vào quá trình mã hóa sao cho khối bản mã tương ứng với khối bản rõ đã chọn không thể dự đoán được. Chi tiết về kỹ thuật kết hợp dữ liệu ngẫu nhiên vào quá trình mã hoá được mô tả trong TCVN 11367-2:2016 (ISO/IEC 18033-2).

### 5.2 Mã khối

#### 5.2.1 Tổng quan

Mã khối là mã đối xứng với tính chất là thuật toán mã hóa thao tác trên các khối của bản rõ, tức trên các xâu bit với độ dài xác định, kết quả cho ra các khối của bản mã. Trong mã khối, mỗi khóa xác định một ánh xạ riêng khả nghịch từ tập các khối rõ sang tập các khối mã (ánh xạ khả nghịch tương ứng được sử dụng để giải mã). Nếu, và đây là trường hợp thường xảy ra, tất cả khối rõ và khối mã có cùng độ dài gồm n bit, thì từng khóa, đơn giản là xác định một phép hoán vị trên tập hợp tất cả các khối n bit.

Mã khối có thể được sử dụng trong nhiều cách khác nhau. Hai trong số các ứng dụng quan trọng nhất được mô tả trong 5.2.2 và 5.2.3, nhưng có nhiều cách sử dụng khác như sử dụng trong hàm băm (xem ISO/IEC 10118-2) và bộ tạo số ngẫu nhiên (xem ISO/IEC 18031).

#### 5.2.2 Các chế độ hoạt động

Có nhiều cách trong đó mã khối n-bit được sử dụng để mã hóa bản rõ. Các phương pháp này được biết đến như là các *chế độ hoạt động* của mã khối. Chế độ hoạt động của mã khối được xác định tại ISO/IEC 10116. Nếu số lượng bit trong bản rõ bằng n, thì mã hóa bản rõ đơn giản chỉ là áp dụng quá trình mã hóa vào khối rõ này, chế độ mã hóa được gọi là chế độ sách mã điện tử (ECB). Tuy nhiên với bản rõ có độ dài tuỳ ý thì cần áp dụng cách tiếp cận linh hoạt hơn. Vì lí do này và các lí do khác, trong thực tế cần áp dụng một trong các chế độ hoạt động được xác định tại ISO/IEC 10116.

#### 5.2.3 Mã xác thực thông báo (MACs)

Mặc dù mã hóa không cung cấp tính toàn vẹn của dữ liệu, song hoàn toàn có thể, bằng một phương pháp đặc biệt, sử dụng mã khối để đảm bảo chức năng này. Nói riêng, có thể sử dụng mã khối để tính mã xác thực thông báo (MAC) cho từng xâu bit. Mã xác thực này có thể sử dụng để đảm bảo tính toàn vẹn và bảo vệ tính xác thực gốc của xâu bit. Các phương pháp đạt được điều này được quy định trong ISO/IEC 9797-1. Lưu ý rằng đôi khi cũng nên sử dụng mã khối cho cả mã hóa và tính MAC cho bản rõ. Trong những trường hợp như thế nói chung nên sử dụng hai khóa bí mật khác nhau, một khóa dùng cho mã hóa, khóa khác dùng cho tính mã xác thực MAC. Ngoài ra, các kỹ thuật mã hóa xác thực đồng thời cung cấp bảo vệ tính bảo mật và toàn vẹn sử dụng một khóa bí mật duy nhất được quy định trong tiêu chuẩn ISO/IEC 19772.

CHÚ THÍCH Trong trường hợp đặc biệt khi sự kết hợp MAC và mã hóa cho phép sử dụng cùng một khóa bí mật, khi đó không cần sử dụng hai khóa khác nhau.

### 5.3 Mã dòng

Mã dòng luôn dựa trên bộ tạo dòng khóa, tức là một hàm với đầu vào là khóa bí mật (và có thể cả bản mã trước đó), đầu ra là dãy các kí tự được gọi là khóa dòng. Dãy này dùng để mã hóa bản rõ bằng cách kết hợp từng kí tự của nó với từng kí tự của bản rõ, trong đó sử dụng một hàm khả nghịch (ví dụ phép toán loại trừ OR từng bit).

Thông thường nếu sử dụng một khóa và một véc tơ khởi tạo nhiều lần cho bộ tạo khóa, thì kết quả sẽ cho ra các khóa dòng giống nhau. Nếu sử dụng khóa dòng để mã hai hay nhiều hơn một bản rõ, khi đó có nguy cơ kẻ thu chặn bất hợp pháp bản mã sẽ có khả năng thu được thông tin về cả hai bản rõ. Do đó cần cung cấp các phương tiện để đảm bảo mỗi khoá dòng được sử dụng để mã một bản rõ. Các vấn đề sử dụng khóa được xem xét tại TCVN 11367-4:2016 (ISO/IEC 18033-4).

Trừ khi sử dụng các kỹ thuật định dạng bản rõ đặc biệt, mã dòng không bảo vệ được tính toàn vẹn của bản rõ. Trong trường hợp khi mã hóa bằng mã dòng là phép toán loại trừ OR từng bit bản rõ với khóa dòng, thì sự thay đổi một bit riêng lẻ trong bản mã dẫn đến sự thay đổi một bit riêng lẻ trong bản rõ được khôi phục. Ngoài ra, mã dòng cũng để lộ độ dài chính xác của bản rõ.

### 5.4 Cơ chế dựa trên định danh

Kỹ thuật mã hóa dựa trên định danh là một cơ chế mã hóa phi đối xứng cho phép một xâu tùy ý được sử dụng như một khóa công khai. Bằng cách sử dụng một xâu dễ nhận biết (ví dụ một địa chỉ email) là một khóa công khai, người mã hóa có thể có được nó một cách đáng tin cậy mà không cần phải truy cập và kiểm tra chứng thư khóa công khai. Trong một số trường hợp nó có thể sắp xếp để khóa công khai để có một khoảng thời gian tồn tại ngắn, ví dụ bao gồm ngày hoặc tem thời gian trong khóa công khai cùng với định danh cho chủ sở hữu. Trong trường hợp như vậy, có thể không cần một cơ chế thu hồi rõ ràng cho khóa công khai, không giống như trường hợp khi sử dụng chứng thư số khóa công khai (xem ISO/IEC 11770-3). Khi chứng thư số khóa công khai là không đòi hỏi, và một cơ chế thu hồi cũng có thể không cần thiết, mã hóa dựa trên định danh có tiềm năng cung cấp lợi thế thực tế đáng kể với các kỹ thuật mã hóa phi đối xứng dựa trên chứng thư số.

Việc sử dụng mã hóa dựa trên định danh liên quan đến một bên thứ ba tin cậy đặc biệt được gọi là Bộ tạo khóa riêng. Thực thể này có trách nhiệm tạo các khóa riêng của người sử dụng cá nhân. Do vậy bên thứ ba này có các cách thức để giải mã tất cả các thông báo dành cho các khách hàng của mình. Đặc tính này có thể không luôn luôn được mong muốn, trong trường hợp đó, nên sử dụng thay thế

bằng kỹ thuật mã hóa phi đối xứng dựa trên chứng thư số, như được tiêu chuẩn hóa trong tiêu chuẩn TCVN 11367-2:2016 (ISO/IEC 18033-2).

## 6. Định danh đối tượng

Tiêu chuẩn này đặc tả tên gọi duy nhất (định danh đối tượng OSI) cho mỗi thuật toán riêng biệt. Trong các ứng dụng, khi định danh đối tượng được sử dụng, những định danh đối tượng được mô tả trong tiêu chuẩn này có thể được sử dụng trong tham chiếu tới các định danh đối tượng khác có thể có trong các thuật toán được xem xét.

# Phụ lục A

(Quy định)

## Các tiêu chí lựa chọn mật mã để có thể đưa vào trong tiêu chuẩn này

### A.1 Hướng dẫn sử dụng để đánh giá các thuật toán mã hóa

Mật mã được đưa vào trong các phần tiếp theo của bộ tiêu chuẩn TCVN 11367 (ISO/IEC 18033) được chọn từ một lượng lớn và đa dạng các kỹ thuật mật mã đã được công bố và sử dụng. Những kỹ thuật mật mã không được chọn đưa vào TCVN 11367 (ISO/IEC 18033) không có nghĩa các kỹ thuật này không an toàn. Các mật mã được mô tả chỉ đại diện cho một tập nhỏ các kỹ thuật được chọn theo các tiêu chí sau đây (thứ tự trình bày các tiêu chí không có ý nghĩa).

Việc đánh giá được thực hiện theo các phương diện sau của hệ mật:

a) *Tính an toàn* của mật mã, tức thuật toán mật mã được chọn cần chống được tấn công phân tích mã. Sự tồn tại một chứng minh về tính an toàn được coi như bằng chứng quan trọng trong việc chọn mật mã, việc chứng minh này phụ thuộc vào mô hình an toàn và các giả thiết chứng minh. Bản chất của bất kì đánh giá nào cũng có tầm quan trọng lớn, vì chúng được tiến hành bởi các tổ chức đánh giá được thừa nhận rộng rãi.

b) *Hiệu năng* của mật mã trên tập hợp đa dạng các nền tảng thông dụng. Điều này không chỉ bao gồm đến các khía cạnh, như hiệu quả về thời gian và không gian, mà còn bao gồm cả vấn đề, liệu mật mã được chọn có các tính chất tạo nên ưu thế so với các kỹ thuật mật mã khác.

c) Bản chất của các *vấn đề cấp phép* ảnh hưởng lên mật mã.

d) *Sự kiểm nghiệm* của mật mã. Sự kiểm nghiệm của mật mã được đánh giá ở các phương diện cường độ sử dụng, mức độ công bố rộng rãi của các phân tích về nó, mức độ được nghiên cứu kỹ lưỡng.

e) Mức độ *được xác nhận* của mật mã bởi tổ chức công nhận (ví dụ tổ chức tiêu chuẩn hóa, các cơ quan về an toàn thông tin của nhà nước, v.v) hoặc theo những khảo cứu và/ hoặc theo phân tích nhằm mục tiêu được chấp nhận bởi cơ quan này.

f) *Mức độ chấp nhận của thị trường* đối với mật mã. Trừ khi các xem xét khác phủ định quyết định đó – mật mã đã được sử dụng rộng rãi trên thị trường được ưa chuộng hơn những kỹ thuật ít được dùng khác.

g) Nói chung *số lượng* mật mã được tiêu chuẩn hóa trong mỗi phần của TCVN 11367 (ISO/IEC 18033) nên nhỏ ở mức có thể. Có ba ngoại lệ cho nguyên tắc này

- Khi hai mật mã có các đặc trưng khác nhau, ví dụ hai mã khối n-bit với các giá trị n khác nhau, hoặc các mật mã với các yêu cầu về tính toán và không gian thực thi khác nhau và hai tập các đặc trưng đều quan trọng về mặt thực hành thì cả hai loại mật mã nên được tiêu chuẩn hóa.

- Nói chung người ta đều muốn có sẵn các mật mã được tiêu chuẩn hóa dựa trên các nguyên tắc nền tảng khác nhau, sao cho nếu một mật mã là yếu đối với tấn công phân tích mật mã, thì mật mã kia có cơ hội vẫn an toàn.

- Nói chung người ta đều mong muốn có các mật mã được tiêu chuẩn hóa dựa trên nhiều hơn một bài toán khó, ví dụ phân tích số nguyên hoặc các bài toán logarit rời rạc trong một loạt các thiết lập, bao

gồm các nhóm nhân của một trường hữu hạn và một nhóm các điểm trên đường cong elliptic trên trường hữu hạn.

h) Một quy trình mà Tiểu ban kỹ thuật Tiêu chuẩn SC 27 sau khi quyết định về mật mã mới trong tiêu chuẩn này có thể được tìm thấy trong WG 2 SD 5.

## A.2 Khả năng tấn công lên các thuật toán mã hóa

Hiệu quả của các tấn công phân tích mật mã được biết đến lên một thuật toán mã hóa có vai trò trong việc quyết định một thuật toán có thể được đệ trình để xem xét đưa vào phần tiếp theo của tiêu chuẩn này.

Mục đích của Phụ lục này là so sánh chi phí tấn công cho tấn công phân tích mật mã cụ thể với tấn công tổng quát tốt nhất cho mô hình nhất định và mục tiêu xác định liệu các tấn công được đánh giá có phá vỡ thuật toán mã hóa hay không. Nếu chi phí tấn công lớn hơn hoặc bằng với chi phí tấn công của tấn công tổng quát tốt nhất tương ứng, tấn công phân tích này sẽ không được cho là phá vỡ thuật toán mã hóa. Nếu chi phí tấn công nhỏ hơn chi phí tấn công của tấn công tổng quát tốt nhất tương ứng cho các mô hình và mục tiêu, thì phân tích mật mã đó được coi là phá vỡ thuật toán mã hóa. Xem định nghĩa thuật ngữ tấn công.

Với mục đích của Phụ lục này, tấn công thực hiện cụ thể sẽ không được xem xét.

CHÚ THÍCH Xem Phụ lục C để có thông tin cơ sở về tấn công.

## A.3 Tiêu chí tối thiểu cho việc đệ trình mật mã mới

Các tiêu chí quy định tại điều này có nghĩa cho việc đệ trình các mật mã chưa bao gồm trong các phần tiếp theo của tiêu chuẩn này. Để một mật mã được xem xét để đưa vào phần tiếp theo của tiêu chuẩn này, các thuật toán được thực hiện theo các yêu cầu sau:

a) Độ dài khóa tối thiểu: Thuật toán mã hóa cần cung cấp một độ dài khóa tối thiểu là 128 bit đối với thuật toán mã hóa đối xứng. Đối với thuật toán mã hóa phi đối xứng, chiều dài khóa trong các bit thường dài hơn, nhưng có thể được ánh xạ tới một chiều dài khóa đối xứng tương ứng. Trong trường hợp này, thuật toán phi đối xứng phải đề nghị cung cấp độ dài khóa tương đương tối thiểu là 128-bit.

CHÚ THÍCH Để biết thêm thông tin về độ dài khóa tương đương với mật mã khóa đối xứng và phi đối xứng, hãy tham khảo JTC 1/SC 27 tài liệu chuẩn 12 (SC 27 SD 12) tại http://www.jtc1sc27.din.de/sbe/SD12

b) Kết quả phân tích mã đã biết: Không có tấn công phân tích mã đã biết mà phá vỡ thuật toán mã hóa như mô tả trong C.1.4.

VÍ DỤ: Một mật mã đối xứng với độ dài khóa 256 bit được đệ trình. Có một tấn công phân tích mã lên mật mã này. Tấn công phân tích mã này có thể tìm được khóa với độ phức tạp $2^{250}$ và xác suất thành công là 1 và nhanh hơn so với tấn công tổng quát tốt nhất trong cùng một mô hình và mục tiêu. Mật mã này qua tiêu chí a, nhưng thất bại ở tiêu chí b và do đó sẽ không được xem xét để đưa vào.

c) Miền công cộng: Mô tả mật mã sẽ được công bố trong một thời gian tối thiểu 3 năm trong miền công cộng. Công bố được chấp nhận được bao gồm, nhưng không giới hạn như sau:

1) Hội nghị IACR và các hội thảo:

i) Asiacrypt, Crypto, Eurocrypt

ii) Hội thảo quốc tế về Mã hóa phần mềm nhanh (FSE)

iii) Hội thảo quốc tế về Hệ thống nhúng và phần cứng mật mã (CHES)

iv) Hội nghị về Lý thuyết và thực hành trong mật mã khóa công khai (PKC)

2) Hội nghị IEEE hàng năm

i) Hội nghị chuyên đề về bảo mật và riêng tư

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

3) Hội nghị ACM hàng năm

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

ii) An toàn truyền thông và máy tính (ACM-CCS)

4) Hội nghị quốc tế nổi tiếng mà có lịch sử hơn 15 năm tổ chức

i) An toàn USENIX

ii) Hội nghị chuyên đề của châu Âu về Nghiên cứu an toàn máy tính (ESORICS)

iii) Hội nghị của Úc về An toàn thông tin và riêng tư (ACISP)

iv) An toàn dữ liệu và mật mã tài chính (FC)

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

vi) Các lĩnh vực được lựa chọn trong Cryptography (SAC)

5) Các tạp chí nổi tiếng [ít nhất là hệ thống Cơ sở dữ liệu và Lập trình Logic (DBLP) được trích dẫn]:

i) ACM

- Tạp chí của ACM
- Truyền thông của ACM

ii) Elsevier

- Truyền thông máy tính
- Thông tin và Tính toán
- Tạp chí Máy tính và Khoa học hệ thống (JCSS)
- Tạp chí về thuật toán rời rạc

iii) IEEE

- IEEE giao dịch trên lý thuyết thông tin
- IEEE giao dịch trên máy tính
- IEEE an toàn và bảo mật

iv) IEICE

- IEICE giao dịch trên nguyên tắc cơ bản của Điện tử, Truyền thông và Khoa học máy tính
- IEICE giao dịch trên thông tin và hệ thống

v) SIAM

- Tạp chí SIAM về máy tính

vi) Springer

- Combinatorica
- Mật mã và truyền thông
- Thiết kế, mã và mật mã
- Tạp chí về Mật mã học
- Tạp chí quốc tế về an toàn thông tin

6) Các chuẩn khác

- Công bố chính thức như một tiêu chuẩn trong tiếng Anh đã được công bố công khai bởi một tổ chức Tiêu chuẩn hóa được công nhận.

7) Một cuộc thi với mục đích duy nhất của việc lựa chọn thuật toán mã hóa mới của một loại đặc biệt (ví dụ như mã khối, mã dòng, mật mã phi đối xứng) và hoạt động tối thiểu là 2 năm, và nơi các nghiên cứu và các ấn phẩm được mở cho công chúng. Các phiên bản chưa sửa đổi của thuật toán cần trong miền công cộng ít nhất là 3 năm thì có thể được xem xét khi đệ trình vào tiêu chuẩn này.

d) Phân tích mật mã: Trước khi đưa vào một mật mã, cần phải có bài báo phân tích mật mã được công bố trên các tạp chí được xem xét hoặc hội nghị như được liệt kê trong c).

e) Chấp nhận công nghiệp: Các bằng chứng mạnh mẽ cần cung cấp về các ứng dụng thương mại sử dụng mật mã và khả năng quốc tế hóa các ứng dụng.

f) Hiệu năng: Đối với mức độ an toàn được xác định trước (ví dụ như độ dài khóa), đo lường hiệu suất có thể được định lượng bằng nhiều đơn vị, chẳng hạn như bit/chu kỳ hoặc bit/watt. Cung cấp bằng chứng mạnh mẽ rằng mật mã cung cấp hiệu năng tốt hơn so với chuẩn mật mã hiện hành đối với các số liệu có liên quan đến ứng dụng dự định, trong khi cung cấp một mức độ an toàn ít nhất là so sánh với các mật mã đã được chuẩn hóa hiện có trong tiêu chuẩn này.

## Phụ lục B

(Quy định)

## Tiêu chí cho việc hủy bỏ mật mã khỏi tiêu chuẩn này

Các thuật toán mã hóa đã được tiêu chuẩn hóa trong các phần tiếp theo của bộ tiêu chuẩn TCVN 11367 (ISO/IEC 18033) bị xóa khỏi tiêu chuẩn nếu tính an toàn của mật mã không thể được đảm bảo để chống lại phương pháp mới được phát triển để phân tích mã và kết quả là an toàn thực tế của thuật toán mã hóa không có thể được đảm bảo. Tiêu chuẩn hiện thời được xem xét thường xuyên để đảm bảo tính chính xác và khả năng đáp ứng của tiêu chuẩn đó. Trong đánh giá, phân tích mã mới được công bố của thuật toán mã hóa được công bố trong tiêu chuẩn này được xem xét. Để đánh giá các kỹ thuật phân tích mã mới công bố, các thủ tục được mô tả trong SC 27 như sau đây.

Các yếu tố được xem xét trong quá trình đánh giá các kỹ thuật phân tích mã mới ảnh hưởng đến các thuật toán mã hóa đã được công bố trong tiêu chuẩn này là:

a) Tính đúng đắn của phân tích mã. Các kỹ thuật phân tích mã mới được tiết lộ trong các diễn đàn. Đôi khi, phân tích mã được công bố phóng đại về độ mạnh an toàn, hoặc về độ phức tạp phân tích của tấn công phân tích mã. Hơn nữa, mô hình đề xuất trong đó tấn công phân tích mã được đề xuất là một yếu tố quan trọng trong việc xác định giá trị của nó. Trước tác động của một kỹ thuật mới về các thuật toán được công bố được đánh giá, phải đạt được sự đồng thuận rằng phân tích mã được công bố là hợp lệ.

b) Tính khả thi thực tế của phân tích mã. Một số kết quả phân tích mã được quan tâm về mặt lý thuyết, nhưng không nhất thiết áp dụng thuật toán mã hóa toàn toàn. Cũng có thể xảy ra trường hợp mà phân tích mã của mật mã đạt đến tấn công trên lý thuyết lên thuật toán mã hóa, nhưng tấn công là không thực tế hoặc vì các mô hình tấn công hoặc vì sự phức tạp tấn công có liên quan. Nếu tấn công là thực tế, tác động nghiêm trọng cho người sử dụng các thuật toán mã hóa có thể tồn tại, thì việc loại bỏ thuật toán mã hóa khỏi tiêu chuẩn này được xem xét.

c) Tác động với sản phẩm của thuật toán mã hóa trong công nghiệp: Khi xem xét loại bỏ một thuật toán, dự báo tác động ảnh hưởng đến ngành công nghiệp cần được thực hiện đầy đủ trong bản kê khai cùng với báo cáo các điểm yếu trong thuật toán mật mã, đặc biệt nếu các điểm yếu không nghiêm trọng trên quan điểm nhìn nhận thực tế.

Tùy thuộc vào kết quả của việc xem xét, một thuật toán có thể bị loại bỏ khỏi tiêu chuẩn này nếu nó đặt ra những rủi ro thực tế cho người sử dụng. Nếu một thuật toán không bị loại bỏ, nhưng tính an toàn của nó bị ảnh hưởng bởi một kỹ thuật phân tích mã mới được tiết lộ, sau đó thông tin về tác động của kỹ thuật này trên mức độ an toàn được cung cấp của các thuật toán được mô tả trong Tài liệu hiện hành 12 SC 27 (SC 27 SD 12) sẵn có miễn phí tại http://www.jtc1sc27.din.de/sbe/SD12

# Phụ lục C

(Tham khảo)

# Tấn công lên thuật toán mã hóa

## C.1 Phân tích mã lên thuật toán mã hóa

### C.1.1 Mục tiêu và mô hình tấn công

Phân tích mã là một quá trình theo đó một thuật toán mật mã được phân tích để xác định độ mạnh của thuật toán mã hóa nhằm chống rò rỉ thông tin về bản rõ chưa biết và/hoặc khóa chưa biết. Phân tích mã liên quan đến một mô hình mà xác định truy cập của kẻ tấn công đã truy vấn các thuật toán mã hóa, một tấn công thuật toán mà giữa đầu vào bản rõ/bản mã và đầu ra bản rõ chưa biết và/hoặc khóa chưa biết với mục tiêu hoặc là khôi phục các bản rõ chưa biết hoặc khóa chưa biết.

Mô hình điển hình bao gồm:

- Kẻ tấn công chỉ truy cập vào bản mã.

- Kẻ tấn công truy cập để biết bản rõ và bản mã tương ứng.

- Kẻ tấn công có thể truy vấn thuật toán mã hóa với bản rõ được chọn để có được bản mã với khóa chưa biết.

- Kẻ tấn công có thể truy vấn thuật toán mã hóa với bản rõ được chọn và truy vấn thuật toán giải mã với bản mã được chọn để có được bản mã tương ứng (bản rõ theo thứ tự) với khóa chưa biết.

- Kẻ tấn công có thể truy vấn thuật toán mã hóa và/hoặc giải mã với các văn bản được lựa chọn với các khóa khác nhau mà có một số quan hệ được biết hoặc được chọn với khóa chưa biết.

Mô hình trong đó chỉ có một khóa mã hóa được tham gia thì gọi là thiết lập đơn khóa, trong khi mô hình cuối cùng trong danh sách trên là thiết lập khóa có liên quan. Mục đích của Phụ lục này, chỉ xem xét các mô hình trong các thiết lập đơn khóa, kết hợp với hai mục tiêu bất kỳ (khôi phục bản rõ chưa biết hoặc khóa chưa biết). Kẻ tấn công được phép truy vấn thuật toán mã hóa hoặc giải mã với bản rõ chọn sẵn hoặc bản mã với khóa chưa biết để có được các bản mã và bản rõ tương ứng. Nếu mục tiêu là để khôi phục lại khóa mã hóa chưa biết, thì không có hạn chế áp dụng đối với các truy vấn. Nếu mục tiêu là để khôi phục lại bản rõ từ bản mã chưa biết, trong mô hình này áp dụng hạn chế trong đó kẻ tấn công không được phép truy vấn thuật toán để giải mã bản mã cho trước, nhưng có thể truy vấn thuật toán mã hóa để giải mã bất kỳ bản mã chọn sẵn khác.

CHÚ THÍCH Những mô hình này cho phép hai loại truy vấn, một là các truy vấn đến thuật toán mã hóa được thực thi trong giai đoạn thu thập dữ liệu và sau đó xử lý bằng thuật toán tấn công, và mô hình khác là các truy vấn được điều chỉnh theo đầu ra của thuật toán tấn công. Sau này được biết đến là tấn công bản mã hoặc bản rõ chọn sẵn thích hợp, các thiết lập mạnh nhất có thể trong mô hình đơn khóa.

### C.1.2 Tấn công tổng quát

Tấn công tổng quát là tấn công trong đó áp dụng đối với thuật toán mã hóa mà không dựa vào cấu trúc thuật toán. Một trong những ví dụ về tấn công tổng quát là tấn công vét cạn tìm kiếm khóa. Cho trước một cặp bản rõ/bản mã, kẻ tấn công mã hóa bản rõ bằng các khóa có thể, và so sánh bản mã kết quả với bản mã cho trước. Nếu hai bản mã giống nhau, khóa mã đó là đúng. Một ví dụ khác của tấn công tổng quát là tấn công từ điển. Đối với một khóa cố định, kẻ tấn công tính toán trước một từ điển hoàn

chỉnh của cặp bản rõ/bản mã. Cho một bản mã không biết được, kẻ tấn công kiểm tra từ điển xem nó có chứa bản mã không. Nếu có, kẻ tấn công sẽ trích xuất ra bản rõ tương ứng trong từ điển.

### C.1.3 Chi phí tấn công

Độ phức tạp của tấn công phân tích mã thông thường là số lần gọi đến thuật toán mã hóa để xác định mức độ liên quan phức tạp của nó với tấn công tổng quát. Thông thường có thể được đơn giản trong trường hợp các mô hình yêu cầu gọi đến thuật toán mã hóa, nhưng có thể là phức tạp (ví dụ như tấn công đại số) khi các tấn công liên quan đến tính toán ngoại tuyến phức tạp mà không liên quan truy vấn đến thuật toán mã hóa. Trong trường hợp sau, độ phức tạp của thuật toán tấn công có thể được ước tính.

Độ phức tạp của tấn công phân tích mã được ký hiệu là W và một số mô tả dưới dạng $2^k$ biểu thị độ phức tạp trung bình tương đương của tấn công về số lượng lời gọi đến thuật toán mã hóa.

Một số tấn công lên thuật toán mã hóa là xác suất, tức là chúng không thành công trong tất cả các lần. Xác suất thành công của một tấn công được ký hiệu là P, trong đó P nhận giá trị dương trong đoạn 0 và 1.

Chi phí tấn công được định nghĩa là tỷ lệ W/P. Một ví dụ, đối với tấn công tìm kiếm vét cạn, P = 1 và $W= 2^n-1$, trong đó n là độ dài khóa tính theo bit, do đó tỷ lệ $W/P = 2^n-1$. Nếu tỷ lệ W/P lớn hơn $2^n - 1$ với tấn công phân tích mã cụ thể, thì với mục đích của Phụ lục này, tấn công phân tích mã đó được coi là chậm hơn so với tấn công vét cạn tìm kiếm khóa.

### C.1.4 Tác động của tấn công phân tích mã

Phương pháp cổ điển xác định việc tấn công phân tích mã phá vỡ một thuật toán là để xem xét độ mạnh an toàn của thuật toán mã hóa. Cách tiếp cận cổ điển không đi vào xem xét các mô hình tấn công có thể để so sánh với tấn công tổng quát, cũng không đưa vào danh sách xác suất thành công của các cuộc tấn công. Đối với mục đích của Phụ lục này, các phương pháp sau đây được sử dụng khi xem xét các thuật toán mã hóa có thể được đưa vào phần tiếp theo của tiêu chuẩn này.

Với một mục tiêu và mô hình tấn công cụ thể, sẽ tồn tại tấn công tổng quát lên thuật toán mật mã. Đối với một tấn công phân tích mã lên một thuật toán cụ thể có một xác suất kết hợp để tấn công thành công. Độ phức tạp và chi phí tấn công có thể được tính toán.

## C.2 Tấn công kênh kề lên thuật toán mã hóa

Có một số tấn công khác lên thuật toán mã hóa mà không phụ thuộc trực tiếp vào khía cạnh lý thuyết của thuật toán mã hóa, mà phụ thuộc vào khía cạnh thực hiện. Tấn công loại này thường được gọi là tấn công kênh kề.

Tấn công kênh kề bao gồm như sau:

- Phân tích điện năng

- Phân tích thời gian

- Phân tích lỗi

Phân tích điện năng đo điện năng tiêu thụ để lấy thông tin về các tính toán diễn ra bên trong thuật toán mã hóa. Phân tích thời gian đo thời gian khác nhau trong quá trình thực thi thuật toán mã hóa để xác định thông tin về các tính toán diễn ra bên trong thuật toán mã hóa. Phân tích lỗi gây ra lỗi bên trong

thuật toán mã hóa trong quá trình thực hiện và sau đó các thuộc tính truyền lỗi được sử dụng để thử và xác định trạng thái bên trong chưa biết của thuật toán mã hóa hoặc thông tin về khóa chưa biết.

Tất cả tấn công này áp dụng như nhau để giải mã và thực thi cụ thể. Có thể thực hiện các biện pháp đối phó.

## Thư mục tài liệu tham khảo

[1]. ISO/IEC 9796 (all parts), *Information technology – Security techniques – Digital signature schemes giving message recovery.*

[2]. ISO/IEC 9797 (all parts), *Information technology – Security techniques – Message authentication Codes (MACs).*

[3]. ISO/IEC 9798-1:2010, *Information technology – Security techniques – Entity authentication Codes - Part1:General.*

[4]. ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for n-bit block cipher.*

[5]. ISO/IEC 10118-2:2000, *Information technology – Security techniques – Hash functions - Part2: Hash function using n-bit block cipher algorithm.*

[6]. ISO/IEC 11770 (all parts), *Information technology – Security techniques – Key managements.*

[7]. ISO/IEC 14888 (all parts), *Information technology – Security techniques – Digital signature with appendix.*

[8]. ISO/IEC 19772, *Information technology – Security techniques – Authentication encryption*

[9]. ISO/IEC 29192 (all parts), Information technology — Security techniques — Lightweight cryptography

[10]. *Cryptographic algorithms and key lengths* (SC 27 SD 12), http://www.jtc1sc27.din.de/sbe/SD12

[11]. *Introduction and Removal of Cryptographic Techniques (SC 27/WG 2 SD 5),* http://www.jtc1sc27.din.de/sbe/wg2sd5