BỘ QUỐC PHÒNG

BỘ QUỐC PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 161/2016/TT-BQP	*Hà Nội, ngày 21 tháng 10 năm 2016*

THÔNG TƯ
Ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng

Căn cứ Luật Tiêu chuẩn và Quy chuẩn kỹ thuật ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật Chất lượng sản phẩm, hàng hóa ngày 21 tháng 11 năm 2007;

Căn cứ Nghị định số 127/2007/NĐ-CP ngày 01 tháng 8 năm 2007 của Chính phủ quy định chi tiết thi hành một số điều của Luật Tiêu chuẩn và Quy chuẩn kỹ thuật;

Căn cứ Nghị định số 09/2014/NĐ-CP ngày 27 tháng 01 năm 2014 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Cơ yếu Chính phủ;

Căn cứ Nghị định số 35/2013/NĐ-CP ngày 22 tháng 4 năm 2013 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Quốc phòng;

Theo đề nghị của Trưởng ban Ban Cơ yếu Chính phủ;

Bộ trưởng Bộ Quốc phòng ban hành Thông tư ban hành Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

Điều 1. Ban hành kèm theo Thông tư này Quy chuẩn kỹ thuật quốc gia về mật mã dân sự sử dụng trong lĩnh vực ngân hàng:

1. QCVN 4:2016/BQP, Mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng;
2. QCVN 5:2016/BQP, Chữ ký số sử dụng trong lĩnh vực ngân hàng;
3. QCVN 6:2016/BQP, Quản lý khóa sử dụng trong lĩnh vực ngân hàng.

Điều 2. Thông tư này có hiệu lực thi hành kể từ ngày 09 tháng 12 năm 2016.

Điều 3. Trưởng ban Ban Cơ yếu Chính phủ, Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này./.

BỘ TRƯỞNG

Đại tướng Ngô Xuân Lịch

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

QCVN 4:2016/BQP

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

HÀ NỘI - 2016

MỤC LỤC

Lời nói đầu .....
1. QUY ĐỊNH CHUNG .....
1.1. Phạm vi điều chỉnh .....
1.2. Đối tượng áp dụng .....
1.3. Tài liệu viện dẫn .....
1.4. Thuật ngữ và định nghĩa .....
1.5. Các ký hiệu .....
2. QUY ĐỊNH KỸ THUẬT .....
2.1. Quy định chung .....
2.2. Mã khối .....
2.2.1. TDEA - Thuật toán mã dữ liệu bội ba .....
2.2.2. AES .....
2.2.3. Camellia .....
2.3. Chế độ hoạt động của mã khối .....
2.3.1. Chế độ xích liên kết khối mã CBC (Cipher Block Chaining) .....
2.3.2. Chế độ phản hồi mã CFB (Cipher FeedBack) .....
2.3.3. Chế độ phản hồi đầu ra OFB (Output Feedback): .....
2.3.4. Chế độ đếm CTR (Counter) .....
2.4. Mã dòng .....
3. QUY ĐỊNH VỀ QUẢN LÝ .....
4. TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN .....
5. TỔ CHỨC THỰC HIỆN .....
Phụ lục A (Quy định): Mô tả DES .....
Phụ lục B (Quy định): Các phép biến đổi của AES .....

Lời nói đầu

QCVN 4 : 2016/BQP do Cục Quản lý mật mã dân sự và Kiểm định sản phẩm mật mã - Ban Cơ yếu Chính phủ biên soạn, Ban Cơ yếu Chính phủ trình duyệt, Bộ Khoa học và Công nghệ thẩm định và được ban hành theo Thông tư số 161/2016/TT-BQP ngày 21 tháng 10 năm 2016 của Bộ trưởng Bộ Quốc phòng.

QUY CHUẨN KỸ THUẬT QUỐC GIA VỀ MÃ HÓA DỮ LIỆU SỬ DỤNG TRONG LĨNH VỰC NGÂN HÀNG

National technical regulation on data encryption used in banking

1. QUY ĐỊNH CHUNG

1.1. Phạm vi điều chỉnh

Quy chuẩn kỹ thuật quốc gia này quy định mức giới hạn về đặc tính kỹ thuật mật mã của các thuật toán mã hóa dữ liệu dùng trong các sản phẩm mật mã dân sự sử dụng trong lĩnh vực ngân hàng.

1.2. Đối tượng áp dụng

Quy chuẩn này áp dụng đối với các doanh nghiệp kinh doanh sản phẩm, dịch vụ mật mã dân sự trong lĩnh vực ngân hàng; các tổ chức tín dụng (trừ quỹ tín dụng nhân dân cơ sở có tài sản dưới 10 tỷ, tổ chức tài chính vi mô) sử dụng sản phẩm, dịch vụ mật mã dân sự.

1.3. Tài liệu viện dẫn

- *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, NIST SP 800-90A Rev. 1, National Institute of Standards and Technology, June 2015. (*Khuyến cáo cho bộ sinh số ngẫu nhiên sử dụng bộ sinh bit ngẫu nhiên tất định*, NIST SP 800-90A Rev. 1, Viện tiêu chuẩn và công nghệ quốc gia (Mỹ), tháng 6 năm 2015).
- TCVN 7876:2007 Công nghệ thông tin – Kỹ thuật mật mã – Thuật toán mã dữ liệu AES.
- 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.
- ISO/IEC 10116:2006 Information technology -- Security techniques -- Modes of operation for an n-bit block cipher.
- ISO/IEC 9797-1:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher.

1.4. Giải thích từ ngữ

Trong Quy chuẩn này, các từ ngữ dưới đây được hiểu như sau:

1.4.1.

Thông tin không thuộc phạm vi bí mật nhà nước

Là thông tin không thuộc nội dung tin “tuyệt mật", "tối mật" và “mật" được quy định tại Pháp lệnh Bảo vệ bí mật nhà nước ngày 28 tháng 12 năm 2000.

1.4.2.

Mật mã

Là những quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin nhằm bảo đảm bí mật, xác thực, toàn vẹn của nội dung thông tin.

1.4.3.

Mật mã dân sự

Là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

1.4.4.

Sản phẩm mật mã dân sự

Là các tài liệu, trang thiết bị kỹ thuật và nghiệp vụ mật mã để bảo vệ thông tin không thuộc phạm vi bí mật nhà nước.

1.4.5.

Kỹ thuật mật mã

Là phương pháp, phương tiện có ứng dụng mật mã để bảo vệ thông tin.

1.4.6.

Mã hóa

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.

1.4.7.

Giải mã

Phép toán ngược với phép mã hóa tương ứng.

1.4.8.

Mã khối

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.

1.4.9.

Mã dòng

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

1.4.10.

Khóa

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

1.4.11.

Khóa dòng

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

1.5. Các ký hiệu

n độ dài tính bằng bit của bản rõ/bản mã đối với mã khối

E_k hàm mã hóa với khóa K

D_k hàm giải mã với khóa K

Nr số vòng của thuật toán AES, bằng 10,12 hoặc 14 để chọn độ dài khóa tương ứng 128, 192, hoặc 256 bit .

Nb Số các cột (các từ 32 bit) tạo nên Trạng thái.

$\oplus$ phép toán logic XOR trên xâu bit, nghĩa là nếu A và B là hai xâu cùng độ dài thì $A \oplus B$ là xâu bit bao gồm các bit là kết quả phép toán logic XOR của A và B

$\otimes$ phép nhân hai đa thức (mỗi đa thức có bậc bé hơn 4) theo mod $x^4 + 1$

$\wedge$ phép toán logic AND trên xâu bit, nghĩa là nếu A và B là các xâu bit cùng độ dài, thì $A \wedge B$ là xâu bit được tạo từ phép toán logic AND các bit tương ứng của A và B.

$\vee$ phép toán logic OR trên xâu bit, tức nếu A và B là hai xâu bit cùng độ dài, thì $A \vee B$ là xâu bit gồm các bit là kết quả của phép toán logic OR của A và B.

$\|$ phép ghép các xâu bit

$\bullet$ phép nhân trên trường hữu hạn

$\ggg_i$ phép dịch vòng sang trái i bit.

$\lll_i$ phép dịch vòng sang phải i bit

$\bar{x}$ phép bù bit của x

$a \bmod n$ với các số nguyên a và n, $a \bmod n$ ký hiệu số dư (không âm) trong phép chia a cho n. Một cách tương đương, $b = a \bmod n$ nếu b là số nguyên duy nhất thõa mãn các điều kiện sau:

(i) $0 \leq b < n$

(ii) $(b - a)$ là bội số nguyên của n

$\boxplus$ phép cộng trong số học mô-đun, nghĩa là nếu A và B là hai xâu t-bit thì $A \boxplus B$ được xác định bằng $(A + B) mod\ 2^t$

$\boxminus$ phép trừ trong số học mô-đun, nghĩa là nếu A và B là hai xâu t-bit thì $A \boxminus B$ được xác định bằng $(A - B) mod\ 2^t$

2. QUY ĐỊNH KỸ THUẬT

2.1. Quy định chung

- Quy định chi tiết về nguồn ngẫu nhiên:

Các số ngẫu nhiên được sử dụng cho các mục đích khác nhau như để sinh các tham số mật mã, các khóa mật mã, các giá trị ngẫu nhiên dùng một lần và các giá trị thách đố xác thực.

Một số bộ sinh bit ngẫu nhiên tất định DRBG được chấp thuận để sử dụng theo quy định chung bao gồm: HASH_DRBG, HMAC_DRBG và CTR_DRBG.

Các bộ sinh bit ngẫu nhiên RBG tuân theo SP800-90A phiên bản sửa đổi lại năm 2015 để sinh bit ngẫu nhiên cũng được chấp thuận để sử dụng tiếp.

2.2. Mã khối

Trong Quy chuẩn này quy định 3 loại mã khối áp dụng cho việc mã hóa dữ liệu để bảo vệ thông tin trong lĩnh vực ngân hàng.

Độ dài khối	Tên thuật toán	Độ dài khóa quy định áp dụng
64 bit	TDEA	Không nhỏ hơn 192 bit
128 bit	AES	Không nhỏ hơn 256 bit
	Camellia	Không nhỏ hơn 256 bit

- Quy định về ngưỡng thời gian và độ an toàn khóa cụ thể:

Độ an toàn theo bit	Thuật toán mã khối	Thời gian sử dụng quy định
112	3TDEA	Đến cuối năm 2030
256	AES-256	Từ năm 2030
	Camellia-256	

2.2.1. TDEA - Thuật toán mã dữ liệu bội ba

Trong Quy chuẩn này thuật toán mã dữ liệu bội ba (TDEA-Triple Data Encryption Algorithm) xử lý các khối dữ liệu 64 bit, sử dụng khóa mật mã có độ dài không nhỏ hơn 192 bit.

Phép mã hóa/giải mã TDEA là phép toán ghép các phép toán mã hoá và giải mã DES. Khóa của TDEA gồm ba khóa K_1, K_2 và K_3 là những khóa DES khác nhau ($K_1 \neq K_2, K_2 \neq K_3$ và $K_3 \neq K_1$).

2.2.1.1. Phép mã hóa/giải mã TDEA

2.2.1.1.1. Các định nghĩa mã hóa /giải mã

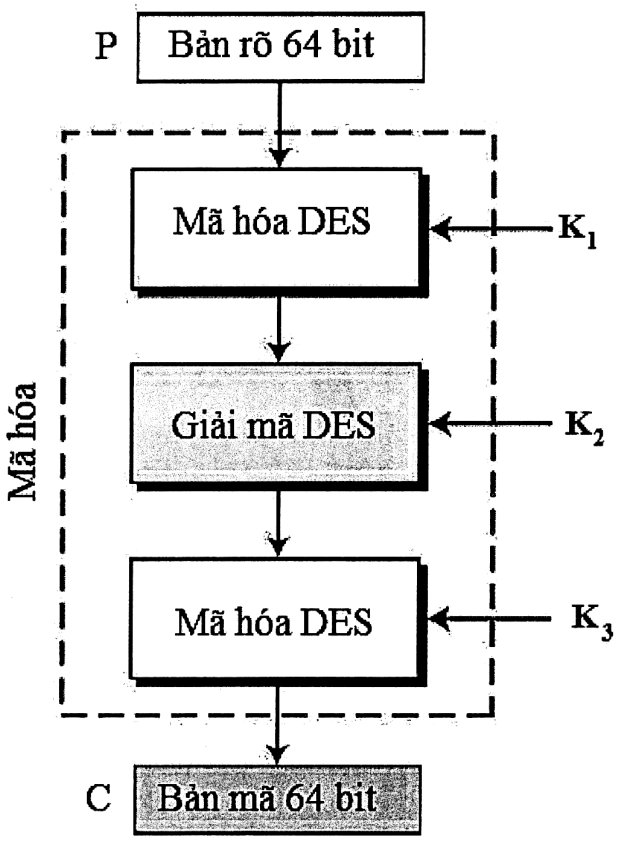
TDEA được xác định theo thuật ngữ của phép toán của DES, ở đấy E_k là phép toán mã hóa của DES với khóa K và D_k là phép giải mã của DES với khóa K.

2.2.1.1.2. Phép mã hóa

Phép biến đổi khối P có độ dài 64 bit thành khối C có độ dài 64 bit được xác định như sau:

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P))).$$

Phép mã hóa/giải mã DES được mô tả tại Phụ lục A của Quy chuẩn này.



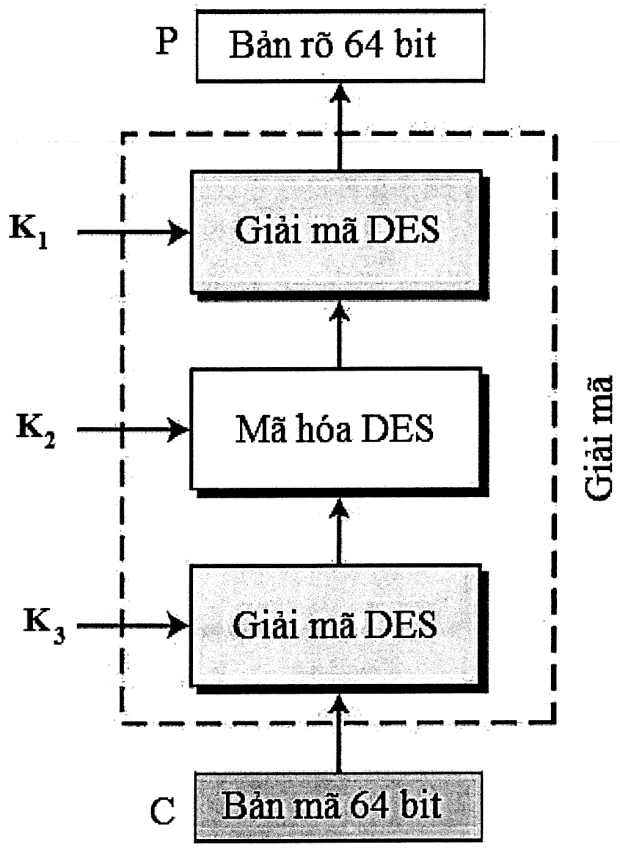
Hình 1: Sơ đồ phép mã hóa TDEA

2.2.1.1.3. Phép giải mã TDEA

Phép biến đổi khối C có độ dài 64 bit thành khối P có độ dài 64 bit được xác định như sau:

$$P = D_{K_1}(E_{K_2}(D_{K_3}(C))).$$

Phép mã hóa/giải mã DES được mô tả tại Phụ lục A của Quy chuẩn này.



Hình 2: Sơ đồ phép giải mã TDEA

2.2.1.2. Chu trình khóa

Phần lược đồ khóa DES được mô tả tại Điều A.5.

2.2.1.3. Chế độ hoạt động của TDEA

Các chế độ hoạt động của TDEA được quy định tại Mục 2.3 của Quy chuẩn này.

2.2.1.4. Khóa

Độ dài khóa sử dụng trong mã khối TDEA được quy định:

Độ dài khối	Tên thuật toán	Độ dài khóa quy định áp dụng
64 bit	TDEA	Không nhỏ hơn 192 bit

2.2.1.4.1. Các yêu cầu về khóa

Đối với các chế độ hoạt động của mã khối TDEA, 3 khóa mật mã (K_1, K_2 và K_3) xác định khóa cho hệ mật TDEA cần:

a. Phải được giữ bí mật.

b. Được sinh ra sử dụng bộ sinh bit ngẫu nhiên được quy định trong phần 2.1 của Quy chuẩn này.

c. Là các khóa mật mã khác nhau.

d. Đảm bảo toàn vẹn mà mỗi khóa không bị thay đổi trái phép kể từ khi được sinh ra, gửi đi hoặc được lưu trữ bởi một thực thể có thẩm quyền.

e. Được sử dụng theo thứ tự thích hợp theo quy định bởi chế độ hoạt động riêng biệt.

f. Không sử dụng để mã hóa nhiều hơn 2^{32} khối dữ liệu 64-bit.

g. Không sử dụng các khóa yếu và bán yếu *(Được quy định tại Điều 2.2.1.4.2).*

2.2.1.4.2. Khóa yếu

Đối với thuật toán DES có một số khóa mật mã được coi là yếu khi sử dụng. Việc sử dụng các khóa yếu này ảnh hưởng đến độ an toàn của thuật toán TDEA. Các khóa yếu không được sử dụng trong thuật toán TDEA được liệt kê dưới đây (theo định dạng thập lục phân):

```
01010101 01010101
FEFEFEFE FEFEFEFE
E0E0E0E0 F1F1F1F1
1F1F1F1F 0E0E0E0E
```

Một số cặp khóa khi mã hóa thì bản rõ và bản mã là giống hệt nhau và cũng không được sử dụng. Các khóa bán - yếu đó là (theo định dạng thập lục phân):

```
011F011F010E010E và 1F011F010E010E01
01E001E001F101F1 và E001E001F101F101
01FE01FE01FE01FE và FE01FE01FE01FE01
1FE01FE00EF10EF1 và E01FE01FF10EF10E
1FFE1FFE0EFE0EFE và FE1FFE1FFE0EFE0E
E0FEE0FEF1FEF1FE và FEE0FEE0FEF1FEF1
```

Ngoài ra còn 48 khóa sau chỉ tạo ra 4 khóa con khác nhau (thay vì 16 khóa con khác nhau) và cũng không được sử dụng. Đó là các khóa sau (theo định dạng thập lục phân):

```
01011F1F01010E0E  1F1F01010E0E0101  E0E01F1FF1F10E0E
0101E0E00101F1F1  1F1FE0E00E0EF1F1  E0E0FEFEF1F1FEFE
0101FEFE0101FEFE  1F1FFEFE0E0EFEFE  E0FE011FF1FE010E
011F1F01010E0E01  1FE001FE0EF101FE  E0FE1F01F1FE0E01
011FE0FE010EF1FE  1FE0E01F0EF1F10E  E0FEFEE0F1FEFEF1
011FFEE0010EFEF1  1FE0FE010EF1FE01  FE0101FEFE0101FE
01E01FFE01F10EFE  1FFE01E00EFE01F1  FE011FE0FE010EF1
FE01E01FFE01F10E  1FFEE0010EFEF101  FE1F01E0FE0E01F1
01E0E00101F1F101  1FFEFE1F0EFEFE0E  FE1FE001FE0EF101
01E0FE1F01F1FE0E  E00101E0F10101F1  FE1F1FFEFE0E0EFE
```

```
01FE1FE001FE0EF1  E0011FFEF1010EFE      FEE0011FFEF1010E

01FEE01F01FEF10E  E001FE1FF101FE0E      FEE01F01FEF10E01

01FEFE0101FEFE01  E01F01FEF10E01FE      FEE0E0FEFEF1F1FE

1F01011F0E01010E  E01F1FE0F10E0EF1      FEFE0101FEFE0101

1F01E0FE0E01F1FE  E01FFE01F10EFE01      FEFE1F1FFEFE0E0E

1F01FEE00E01FEF1  E0E00101F1F10101      FEFEE0E0FEFEF1F1
```

CHÚ THÍCH: Các khóa yếu và khóa bán-yếu được liệt kê ở trên được biểu diễn với tính lẻ và được chỉ ra trong phần ngoài cùng bên phải của mỗi byte.

2.2.2. AES

Đối với thuật toán AES, độ dài của khối đầu vào, khối đầu ra và Trạng thái đều là 128 bit. Như vậy Nb = 4 là số lượng các từ 32 bit (số cột) của Trạng thái.

Trong Quy chuẩn này thuật toán AES, độ dài Khóa mã K quy định áp dụng là 256 bit. Độ dài khóa được biểu diễn bằng một số Nk = 8 thể hiện số lượng các từ 32 bit (số cột) của Khóa mã. Số vòng trong quá trình thực thi thuật toán AES (được ký hiệu là Nr) với khóa độ dài 256 bit là $Nr = 14$.

Quy chuẩn này quy định cụ thể các giá trị được phép dùng cho độ dài khóa (Nk), kích cỡ khối (Nb) và số lượng vòng lặp (Nr) như Bảng 1.

	Độ dài khóa *(Nk từ)*	Độ dài khối *(Nb từ)*	Số vòng *(Nr)*
AES-256	8	4	14

Bảng 1: Các tổ hợp Khóa - Khối - Vòng

2.2.2.1. Phép mã hóa/giải mã AES

Đối với cả hai Phép mã hóa và Phép giải mã, thuật toán AES sử dụng hàm vòng bao gồm bốn phép biến đổi khác nhau trên byte:

1) Phép thay thế byte sử dụng bảng thay thế (S-box).

2) Dịch hàng của mảng Trạng thái bằng các offset khác nhau.

3) Trộn dữ liệu trong mỗi cột của mảng Trạng thái.

4) Bổ sung khóa vòng vào Trạng thái.

2.2.2.1.1. Phép mã hóa AES

Thuật toán AES gồm một dãy các phép toán được thực hiện trên mảng hai chiều của các byte, được gọi là Trạng thái. Trạng thái gồm bốn dòng byte, mỗi dòng chứa 4 byte. Trong mảng Trạng thái được ký hiệu bằng s, mỗi byte riêng biệt có hai chỉ số với số dòng r với $0 \leq r < 4$ và số cột c, với $0 \leq c < 4$. Trạng thái được ký hiệu là $S = (s_{r,c})$.

Khi bắt đầu quá trình mã hóa, 16 byte của Trạng thái được khởi tạo với ρ_i byte bản rõ, tính từ trên xuống dưới và từ trái sang phải và được minh họa trên Hình 3.

ρ_0	ρ_4	ρ_8	ρ_{12}
ρ_1	ρ_5	ρ_9	ρ_{13}
ρ_2	ρ_6	ρ_{10}	ρ_{14}
ρ_3	ρ_7	ρ_{11}	ρ_{15}

$\longrightarrow$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Hình 3: Khởi đầu Trạng thái

Sau khi cộng khóa vòng ban đầu, Trạng thái được biến đổi bằng cách thực thi hàm vòng Nr lần, với vòng cuối khác một ít với $Nr - 1$ vòng đầu. Nội dung cuối cùng của Trạng thái chính là bản mã đầu ra.

Phép mã hóa đầy đủ có thể được mô tả như sau:

(1) $S = AddRoundKey(P, W_0)$

(2) $For\ i = 1\ to\ Nr - 1$

$S = SubBytes\ (S)$

$S = ShiftRows(S)$

$S = MixColumns(S)$

$S = AddRoundKey(S, W_i)$

(3) $S = SubBytes\ (S), S = ShiftRows(S)$

(4) $C = AddRoundKey\ (S, W_{Nr})$

Các phép biến đổi riêng biệt $SubBytes(\,)$, $ShiftRows(\,)$, $MixColumns(\,)$, $AddRoundkey(\,)$ xử lí Trạng thái và được mô tả tại Phụ lục B. Tất cả Nr vòng đều giống nhau, trừ vòng cuối cùng không chứa phép biến đổi $MixColumns(\,)$. Trong phép toán ở trên, mảng W_i chứa các khóa vòng được mô tả tại Điều 2.2.2.2.

2.2.2.1.2. Phép giải mã AES

Tất cả các phép biến đổi sử dụng trong các phép mã hóa đều khả nghịch. Khi thực thi phép giải mã, dãy các phép biến đổi được sử dụng trong phép mã hóa vẫn được duy trì, nhưng thay bằng các phép biến đổi ngược như sau.

Phép giải mã đầy đủ có thể mô tả như sau:

(1) $S = AddRoundKey\ (C, W_{Nr})$

(2) $for\ i = Nr - 1\ down\ to\ 1$

$S = ShiftRows^{-1}(S)$

$S = SubBytes^{-1}(S)$

$S = AddRoundKey(S, W_i)$

$S = MixColumns^{-1}(S)$

(3) $S = ShiftRows^{-1}(S)$

$S = SubBytes^{-1}(S)$

(4) $P = AddRoundKey(S, W_0)$

Các phép biến đổi $SubBytes^{-1}(), ShiftRows^{-1}(), MixColumns^{-1}()$ thực hiện xử lý Trạng thái. Tất cả Nr vòng đều giống nhau, trừ vòng cuối không chứa phép biến đổi $MixColumns^{-1}()$.

Các phép biến đổi $SubBytes^{-1}(), ShiftRows^{-1}(), MixColumns^{-1}()$ thực hiện xử lý Trạng thái và được mô tả tại Phụ lục B. Tất cả Nr vòng đều giống nhau, trừ vòng cuối không chứa phép biến đổi $MixColumns^{-1}()$. Việc tính các khóa vòng W_i được mô tả tại Điều 2.2.2.2.

2.2.2.1.3. Quy định về S-Box và S-Box nghịch đảo trong AES

a) S-Box

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Bảng 2: S-Box: các giá trị thay thế cho byte {xy} (theo dạng thập lục phân)

b) S-Box nghịch đảo

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Bảng 3: S-Box nghịch: thay thế các giá trị theo byte {xy} (dạng thập lục phân)

2.2.2.2. Chu trình khóa

Thuật toán AES nhận khóa mật mã K và thực hiện thủ tục mở rộng khóa để tạo ra lược đồ khóa. Việc mở rộng khóa tạo ra tổng cộng 4(Nr + 1) từ: Thuật toán đòi hỏi tập khởi đầu gồm 4 từ, và mỗi vòng Nr vòng đòi hỏi 4 từ dữ liệu khóa. Lược đồ khóa nhận được là một mảng tuyến tính gồm các từ 4-byte, ký hiệu là w_j, với j nằm trong khoảng $0 \leq j < 4(Nr + 1)$.

Phép mở rộng khóa đầy đủ cho AES-256 có thể được mô tả như sau:

(1) $[w_0, w_1, w_2, w_3] = K_0, [w_4, w_5, w_6, w_7] = K_1, \boldsymbol{Nk} = 8$

(2) for j = $\boldsymbol{Nk}$ to 4($\boldsymbol{Nr}$ + 1) - 1:

if ($j \; mod \; \boldsymbol{Nk} = 0$) then

$$w_j = w_{j-Nk} \oplus SubBytes^*\left(\text{ShiftColumn}(w_{j-1})\right) \oplus R^{i/Nk}c$$

else if ($j \; mod \; \boldsymbol{Nk} = 4$) then

$$w_j = w_{j-Nk} \oplus SubBytes^*(w_{j-1})$$

else

$$w_j = w_{j-Nk} \oplus w_{j-1}$$

(3) $W_i = [w_{(4*i)}, w_{(4*i+1)}, w_{(4*i+2)}, w_{(4*i+3)}] \; for \; 0 \leq i \leq \boldsymbol{Nr}.$

Trong phép toán trên K_0 và K_1 biểu thị hai nửa của khóa mật mã K 256-bit.

2.2.2.3. Chế độ hoạt động của AES

Các chế độ hoạt động của AES được quy định tại Mục 2.3 của Quy chuẩn này.

2.2.2.4. Khóa

Độ dài khóa sử dụng trong mã khối AES được quy định

Độ dài khối	Tên thuật toán	Độ dài khóa quy định áp dụng
128 bit	AES	Không nhỏ hơn 256 bit

2.2.3. Camellia

Trong Quy chuẩn này thuật toán mã đối xứng Camellia xử lý các khối 128 bit, sử dụng khóa mật mã độ dài không nhỏ hơn 256 bit.

2.2.3.1. Phép mã hóa/giải mã Camellia

2.2.3.1.1. Phép mã hóa Camellia

Quá trình mã hóa với khóa 256-bit làm việc trên 24 vòng, được chỉ ra trên Hình 4. Phép biến đổi khối 128 bit P vào khối 128-bit C được định nghĩa như sau (L và R là các biến độ dài 64 bit, kw, k và kl là các khóa vòng 64 bit):

(1) $L_0 \parallel R_0 = P \oplus (kw_1 \parallel kw_2)$

(2) for $i = 1$ to 24:

$$L_i = \text{F}(L_{i-1}, k_i) \oplus R_{i-1}$$

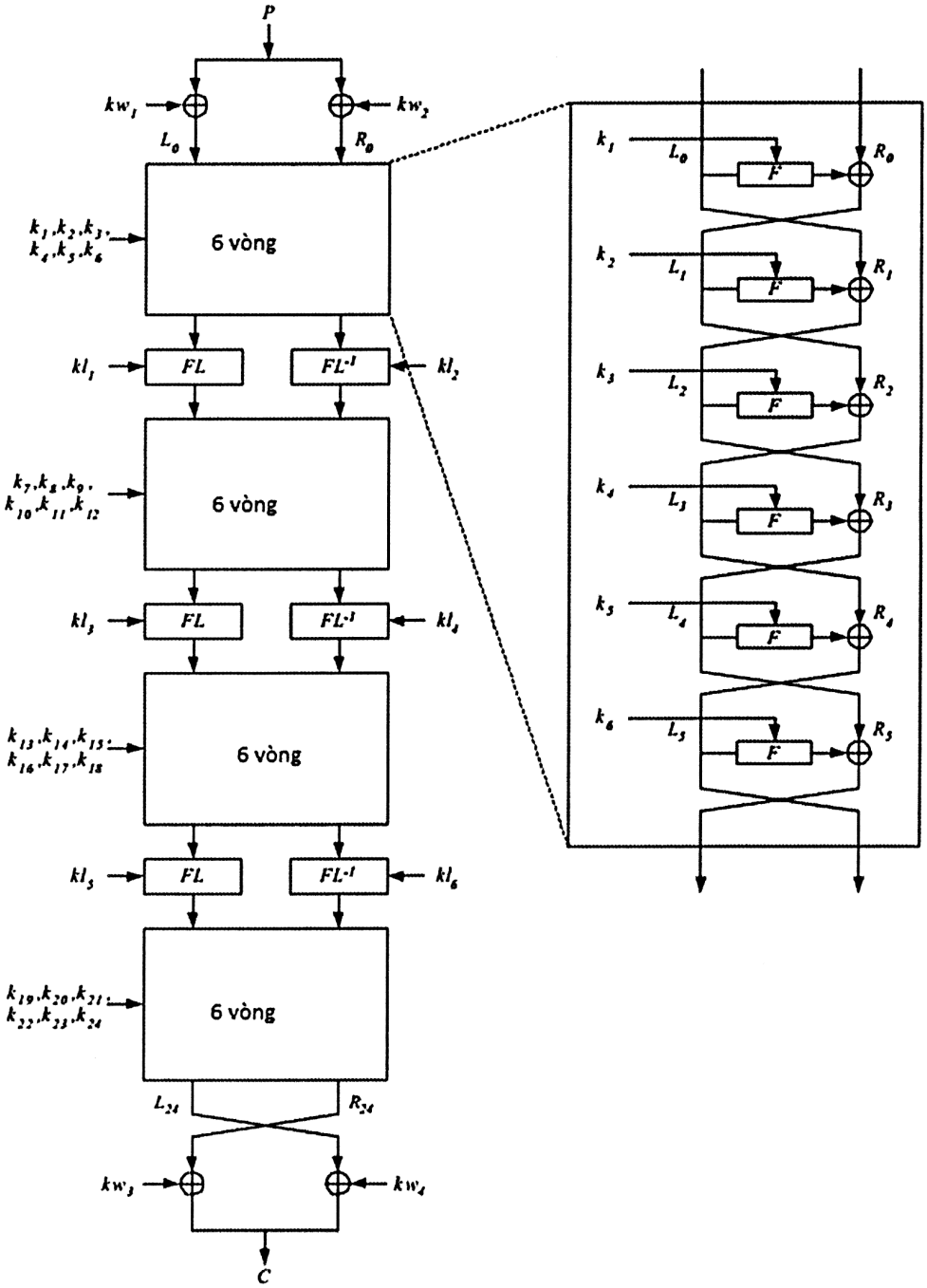
$$R_i = L_{i-1}$$

if (i = 6 or 12 or 18) then

$$L_i = FL(L_i, kl_{i/3-1})$$

$$R_i = FL^{-1}(R_i, kl_{i/3})$$

(3) $C = (R_{24} \oplus kw_3) \parallel (L_{24} \oplus kw_4)$



Hình 4: Thủ tục mã hóa Camellia cho khóa 256 bit

2.2.3.1.2. Phép giải mã Camellia

Quá trình giải mã cho khóa 256 bit được chỉ ra trên Hình 5, và là như nhau trong phép mã hóa, chỉ khác là vị trí và thứ tự các khóa vòng được đảo lại.

Phép giải mã được xác định như sau:

(1) $R_{24} \parallel L_{24} = C \oplus (kw_3 \parallel kw_4)$

(2) for $i = 24$ down to 1:

$R_{i-1} = \mathrm{F}(R_i, k_i) \oplus L_i$

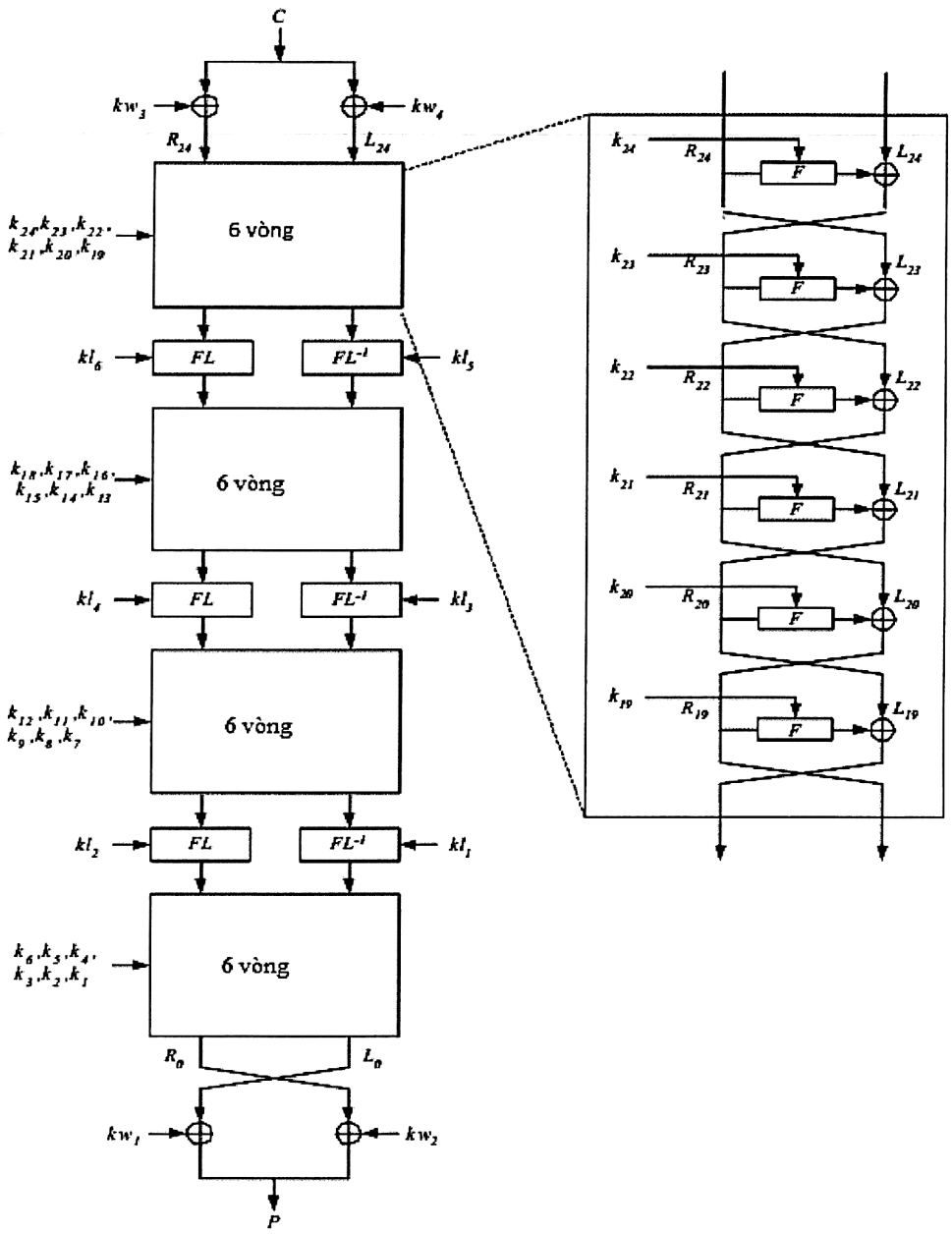
$L_{i-1} = R_i$

if (i = 19 or 13 or 7) then

$R_{i-1} = \mathrm{FL}(R_{i-1}, kl_{(i-1)/3})$

$L_{i-1} = FL^{-1}(L_{i-1}, kl_{(i-1)/3-1})$

(3) $\mathrm{P} = (\mathrm{L}_0 \oplus \mathrm{kw}_1) \parallel (\mathrm{R}_0 \oplus \mathrm{kw}_2)$



Hình 5: Thủ tục giải mã Camellia cho 256 bit

2.2.3.1.3. F-hàm

F-hàm được chỉ ra trên Hình 8. F-hàm bao gồm phép toán cộng bit XOR, tiếp đó áp dụng tám S-box song song kích thước 8x8 bit, tiếp theo tầng khuếch tán (P-hàm). x_j, y_j, z_j, z'_j là các biến, mỗi biến 8 bit; các biến L_i, k_i, L'_i là các biến 64 bit. Đầu vào 64 bit L_i trước hết được cộng XOR với khóa vòng 64-bit k_i, sau đó được chia thành 8 đoạn 8-bit y_j, như sau:

$$y_1 \parallel y_2 \parallel y_3 \parallel y_4 \parallel y_5 \parallel y_6 \parallel y_7 \parallel y_8 = L_i \oplus k_i$$

ở đây,

$$L_i = x_1 \parallel x_2 \parallel x_3 \parallel x_4 \parallel x_5 \parallel x_6 \parallel x_7 \parallel x_8.$$

Mỗi y_j sau đó được đi qua S-box kích thước 8x8 bit s_t để đưa ra 8 phân đoạn độ dài 8 bit z_j, ở đây

$$z_1 = s_1[y_1], z_2 = s_2[y_2], z_3 = s_3[y_3], z_4 = s_4[y_4], z_5 = s_5[y_5], z_6 = s_6[y_6], z_7 = s_7[y_7], z_8 = s_8[y_8]$$

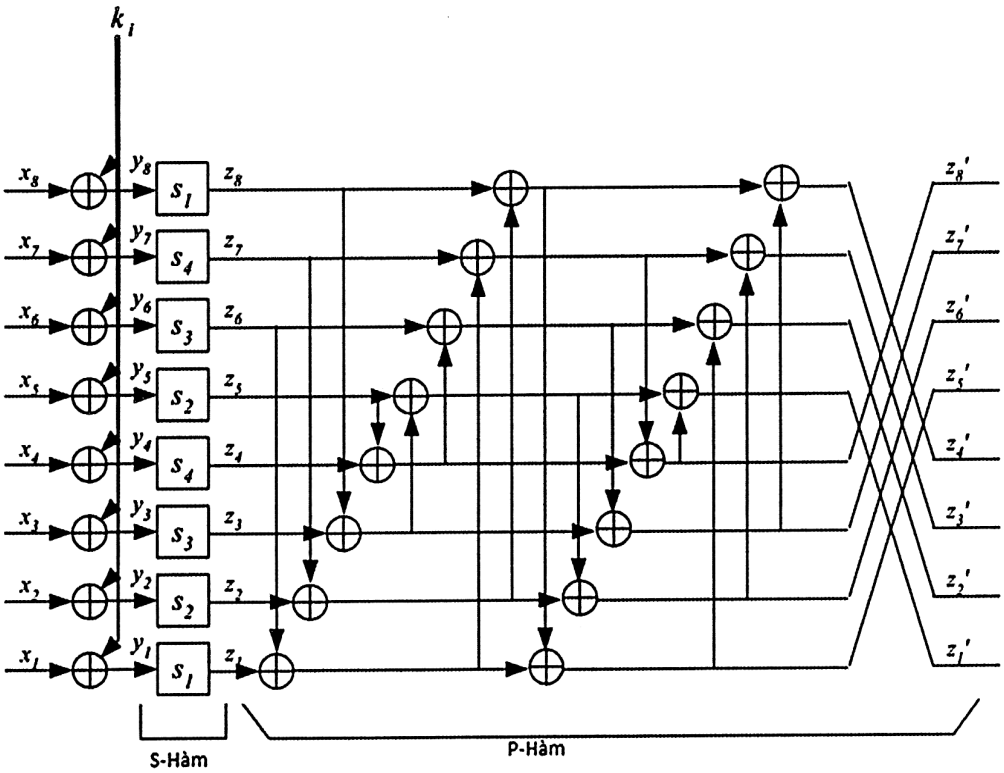
8 phân đoạn 8-bit z_j được tác động bởi P-hàm, là lớp khuếch tán cho ra 8 phân đoạn 8-bit z'_j, trong đó

$$z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8, \qquad z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8,$$

$$z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8, \qquad z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8,$$

$$z'_3 = z_1 \oplus z_2 \oplus z_5 \oplus z_6 \oplus z_7 \oplus z_8, \qquad z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8,$$

$$z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7 \qquad z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7.$$



Hình 6: F-hàm

P-hàm có thể được biểu diễn cách khác, dưới dạng véc tơ ma trận như sau:

$$\begin{pmatrix} z_8 \\ z_7 \\ \vdots \\ z_1 \end{pmatrix} \mapsto \begin{pmatrix} z'_8 \\ z'_7 \\ \vdots \\ z'_1 \end{pmatrix} = P \begin{pmatrix} z_8 \\ z_7 \\ \vdots \\ z_1 \end{pmatrix},$$

ở đây:

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Sau đó đầu ra 64-bit của F-hàm L'_i được thiết lập bằng cách ghép các biến 8-bit z'_j:

$$L'_i = z'_1 \parallel z'_2 \parallel z'_3 \parallel z'_4 \parallel z'_5 \parallel z'_6 \parallel z'_7 \parallel z'_8.$$

S-box s1

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	70	82	2c	ec	b3	27	c0	e5	e4	85	57	35	ea	0c	ae	41
1	23	ef	6b	93	45	19	a5	21	ed	0e	4f	4e	1d	65	92	bd
0	86	b8	af	8f	7c	eb	1f	ce	3e	30	dc	5f	5e	c5	0b	1a
3	a6	e1	39	ca	d5	47	5d	3d	d9	01	5a	d6	51	56	6c	4d
4	8b	0d	9a	66	fb	cc	b0	2d	74	12	2b	20	f0	b1	84	99
5	df	4c	cb	c2	34	7e	76	05	6d	b7	a9	31	d1	17	04	d7
6	14	58	3a	61	de	1b	11	1c	32	0f	9c	16	53	18	f2	22
7	fe	44	cf	b2	c3	b5	7a	91	24	08	e8	a8	60	fc	69	50
8	aa	d0	a0	7d	a1	89	62	97	54	5b	1e	95	e0	ff	64	d2
9	10	c4	00	48	a3	f7	75	db	8a	03	e6	da	09	3f	dd	94
a	87	5c	83	02	cd	4a	90	33	73	67	f6	f3	9d	7f	bf	e2
b	52	9b	d8	26	c8	37	c6	3b	81	96	6f	4b	13	be	63	2e
c	e9	79	a7	8c	9f	6e	bc	8e	29	f5	f9	b6	2f	fd	b4	59
d	78	98	06	6a	e7	46	71	ba	d4	25	ab	42	88	a2	8d	fa
e	72	07	b9	55	f8	ee	ac	0a	36	49	2a	68	3c	38	f1	a4
f	40	28	d3	7b	bb	c9	43	c1	15	e3	ad	f4	77	c7	80	9e

S-box s2

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	e0	05	58	d9	67	4e	81	cb	c9	0b	ae	6a	d5	18	5d	82
1	46	df	d6	27	8a	32	4b	42	db	1c	9e	9c	3a	ca	25	7b
2	0d	71	5f	1f	f8	d7	3e	9d	7c	60	b9	be	bc	8b	16	34
3	4d	c3	72	95	ab	8e	ba	7a	b3	02	b4	ad	a2	ac	d8	9a
4	17	1a	35	cc	f7	99	61	5a	e8	24	56	40	e1	63	09	33
5	bf	98	97	85	68	fc	ec	0a	da	6f	53	62	a3	2e	08	af
6	28	b0	74	c2	bd	36	22	38	64	1e	39	2c	a6	30	e5	44
7	fd	88	9f	65	87	6b	f4	23	48	10	d1	51	c0	f9	d2	a0
8	55	a1	41	fa	43	13	c4	2f	a8	b6	3c	2b	c1	ff	c8	a5
9	20	89	00	90	47	ef	ea	b7	15	06	cd	b5	12	7e	bb	29
a	0f	b8	07	04	9b	94	21	66	e6	ce	ed	e7	3b	fe	7f	c5
b	a4	37	b1	4c	91	6e	8d	76	03	2d	de	96	26	7d	c6	5c
c	d3	f2	4f	19	3f	dc	79	1d	52	eb	f3	6d	5e	fb	69	b2
d	f0	31	0c	d4	cf	8c	e2	75	a9	4a	57	84	11	45	1b	f5
e	e4	0e	73	aa	f1	dd	59	14	6c	92	54	d0	78	70	e3	49
f	80	50	a7	f6	77	93	86	83	2a	c7	5b	e9	ee	8f	01	3d

S-box s3

	0	1	2	3	4	5	6	7	8	g	a	b	c	d	e	f
0	38	41	16	76	d9	93	60	f2	72	c2	ab	9a	75	06	57	a0
1	91	f7	b5	c9	a2	8c	d2	90	f6	07	a7	27	8e	b2	49	de
2	43	5c	d7	c7	3e	f5	8f	67	1f	18	6e	af	2f	e2	85	0d
3	53	f0	9c	65	ea	a3	ae	9e	ec	80	2d	6b	a8	2b	36	a6
4	c5	86	4d	33	fd	66	58	96	3a	09	95	10	78	d8	42	cc
5	ef	26	e5	61	1a	3f	3b	82	b6	db	d4	98	e8	8b	02	eb
6	0a	2c	1d	b0	6f	8d	88	0e	19	87	4e	0b	a9	0c	79	11
7	7f	22	e7	59	e1	da	3d	c8	12	04	74	54	30	7e	b4	28
8	55	68	50	be	d0	c4	31	cb	2a	ad	0f	ca	70	ff	32	69
9	08	62	00	24	d1	fb	ba	ed	45	81	73	6d	84	9f	ee	4a
a	c3	2e	c1	01	e6	25	48	99	b9	b3	7b	f9	ce	bf	df	71
b	29	cd	6c	13	64	9b	63	9d	c0	4b	b1	a5	89	5f	b1	17
c	f4	bc	d3	46	cf	37	5e	47	94	fa	fc	5b	97	fe	5a	ac
d	3c	4c	03	35	f3	23	b8	5d	6a	92	d5	21	44	51	c6	7d
e	39	83	dc	aa	7c	77	56	05	1b	a4	15	34	1e	1c	f8	52
f	20	14	e9	bd	dd	e4	a1	e0	8a	f1	d6	7a	bb	e3	40	4f

S-box s4

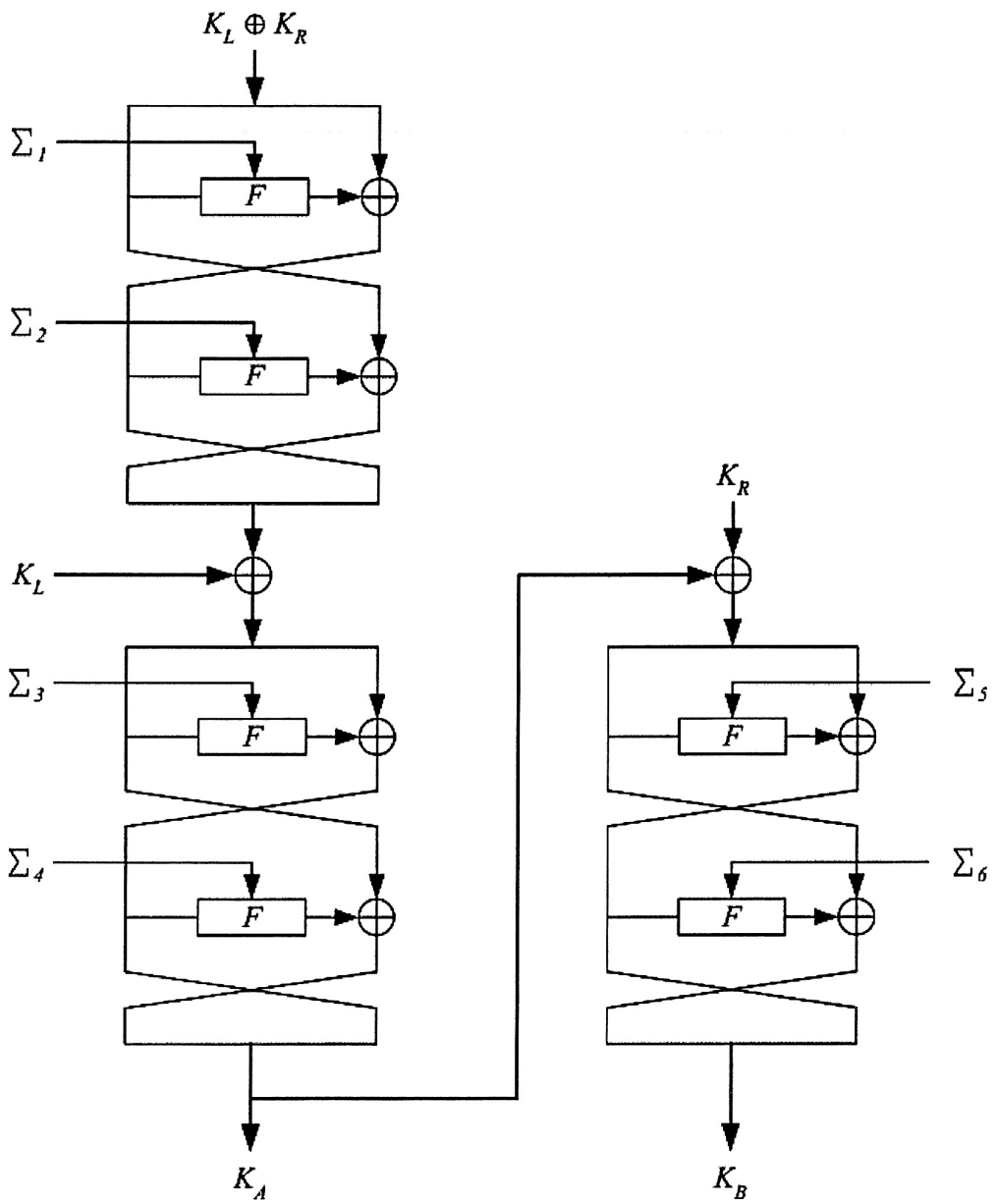
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	70	2c	b3	c0	e4	57	ea	ae	23	6b	45	a5	ed	4f	1d	92
1	86	af	7c	1f	3e	dc	5e	0b	a6	39	d5	5d	d9	5a	51	6c
2	8b	9a	fb	b0	74	2b	f0	84	df	cb	34	76	6d	a9	d1	04
3	14	3a	de	11	32	9c	53	f2	fe	cf	c3	7a	24	e8	60	69
4	aa	a0	a1	62	54	1e	e0	64	10	00	a3	75	8a	e6	09	dd
5	87	83	cd	90	73	f6	9d	bf	52	d8	c8	c6	81	6f	13	63
6	e9	a7	9f	bc	29	f9	2f	b4	78	06	e7	71	d4	ab	88	8d
7	72	b9	f8	ac	36	2a	3c	f1	40	d3	bb	43	15	ad	77	80
8	82	ec	27	e5	85	35	0c	41	ef	93	19	21	0e	4e	65	bd
9	b8	8f	eb	ce	30	5f	c5	1a	e1	ca	47	3d	01	d6	56	4d
a	0d	66	cc	2d	12	20	b1	99	4c	c2	7e	05	b7	31	17	d7
b	58	61	1b	1c	0f	16	18	22	44	b2	b5	91	08	a8	fc	50
c	d0	7d	89	97	5b	95	ff	d2	c4	48	f7	db	03	da	3f	94
d	5c	02	4a	33	67	f3	7f	e2	9b	26	37	3b	96	4b	be	2e
e	79	8c	6e	8e	f5	b6	fd	59	98	6a	46	ba	25	42	a2	fa
f	07	55	ee	0a	49	68	38	a4	28	7b	c9	c1	e3	f4	c7	9e

2.2.3.2. Chu trình khóa

Với quy định khóa có độ dài 256 bit, khóa K là khóa 128-bit K_L và khóa 128-bit K_R. Như vậy,

$$K = K_L \parallel K_R$$

Lược đồ tạo khóa sử dụng F-hàm của mô-đun mã hóa, và là giống nhau cho cả phép mã hóa và giải mã. Khóa *K* được mã bằng các phương tiện của F-hàm, sử dụng các hằng của lược đồ tạo khóa, ở đây các hằng Σ_i, được xác định như những giá trị liên tục biểu diễn trong hệ Hexa của căn bậc hai số nguyên tố thứ *i*. Tiếp đó các khóa vòng được tạo, một phần từ những giá trị được dịch vòng của khóa K ($K = K_L \parallel K_R$) và phần còn lại từ các giá trị được dịch vòng của các khóa "được mã hóa" K_A và K_B (ở đây K_A, K_B có độ dài 128 bit).



Hình 7: Phần chính của lược đồ khóa

Đối với khóa 256-bit, đầu ra của phần chính của lược đồ tạo khóa là khóa con 128 bit K_A và khóa con 128-bit K_B. Lược đồ tạo khóa bao gồm ba phép toán 2-vòng. Mỗi phép toán 2 vòng được "khóa hóa" bằng một cặp hằng Σ_i.

Đầu vào 128-bit của phép toán 2-vòng thứ nhất nằm bên trái của Hình 9 là $K_L \oplus K_R$ và phép toán này được "khóa hóa" bởi hai hằng 64-bit Σ_1 và Σ_2. Tiếp đó đầu ra 128-bit từ phép toán 2-vòng thứ nhất được cộng bit XOR với K_L trước khi là đầu vào của phép toán 2-vòng thứ hai ở bên trái Hình 9. Phép toán 2-vòng thứ hai này được "khóa hóa" bởi các hằng 64 bit là Σ_3 và Σ_4. Đầu ra 128-bit của phép toán 2-vòng thứ hai là K_A, sau đó K_A lại được XOR với khóa con 128-bit K_R trước khi kết quả thu được làm đầu vào của phép toán 2-vòng thứ ba được chỉ ra ở phía phải của Hình 9. Phép toán 2-vòng thứ ba này được "khóa hóa" bởi hai hằng 64 bit là Σ_5 và Σ_6. Đầu ra 128 bit của phép toán 2-vòng thứ ba này là K_B.

Phép toán lập lược đồ tạo khóa đầy đủ được mô tả như sau (K_a, K_A và K_B có độ dài 128 bit):

(1) $K_a = 2RoundFeistel(K_L \oplus K_R, \Sigma_1, \Sigma_2)$

(2) $K_A = 2RoundFeistel(K_a \oplus K_L, \Sigma_3, \Sigma_4)$

(3) $K_B = 2RoundFeistel(K_A \oplus K_R, \Sigma_5, \Sigma_6)$ (chỉ dùng cho khóa 192/256 bit)

ở đây đầu vào 128-bit cho 2RoundFeistel được tách thành hai phần 64-bit $L_0 \parallel R_0$, đầu ra 128-bit từ 2RoundFeistel cũng được tách thành hai phần 64 bit $L_2 \parallel R_2$ và cả hai đầu vào "khóa vòng" 64-bit của 2RoundFeistel là Σ_i và Σ_{i+1}.

2RoundFeistel được mô tả như sau:

(1) với j = 0,1:

$$L_{j+1} = F(L_j, \Sigma_{i+j}) \oplus R_j$$

$$R_{j+1} = R_j$$

Các hằng của lược đồ khóa 64-bit được xác định trên Bảng 4

	Hằng
Σ_1	a09e667f3bcc908b
Σ_2	b67ae8584caa73b2
Σ_3	c6ef372fe94f82be
Σ_4	54ff53a5fld36f1c
Σ_5	10e527fade682d1d
Σ_6	b05688c2b3e6c1fd

Bảng 4: Các hằng trong lược đồ khóa

Cuối cùng, các khóa vòng 64-bit, $k, kw,$ và kl được dẫn xuất từ các khóa con 128-bit, K_L, K_R, K_A và K_B.

Hàm	Khóa vòng	Giá trị
	kw_1	$(K_L \lll_0)_L$
	kw_2	$(K_L \lll_0)_R$
F (vòng 1)	k_1	$(K_B \lll_0)_L$
F (vòng 2)	k_2	$(K_B \lll_0)_R$
F (vòng 3)	k_3	$(K_R \lll_{15})_L$
F (vòng 4)	k_4	$(K_R \lll_{15})_R$
F (vòng 5)	k_5	$(K_A \lll_{15})_L$
F (vòng 6)	k_6	$(K_A \lll_{15})_R$
FL	kl_1	$(K_R \lll_{30})_L$
FL^{-1}	kl_2	$(K_R \lll_{30})_R$

F (vòng 7)	k_7	$(K_B \lll_{30})_L$
F (vòng 8)	k_8	$(K_B \lll_{30})_R$
F (vòng 9)	k_9	$(K_L \lll_{45})_L$
F (vòng 10)	k_{10}	$(K_L \lll_{45})_R$
F (vòng 11)	k_{11}	$(K_A \lll_{45})_L$
F (vòng 12)	k_{12}	$(K_A \lll_{45})_R$
FL	kl_3	$(K_L \lll_{60})_L$
FL^{-1}	kl_4	$(K_L \lll_{60})_R$
F (vòng 13)	k_{13}	$(K_R \lll_{60})_L$
F (vòng 14)	k_{14}	$(K_R \lll_{60})_R$
F (vòng 15)	k_{15}	$(K_B \lll_{60})_L$
F (vòng 16)	k_{16}	$(K_B \lll_{60})_R$
F (vòng 17)	k_{17}	$(K_L \lll_{77})_L$
F (vòng 18)	k_{18}	$(K_L \lll_{77})_R$
FL	kl_5	$(K_A \lll_{77})_L$
FL^{-1}	kl_6	$(K_A \lll_{77})_R$
F (vòng 19)	k_{19}	$(K_R \lll_{94})_L$
F (vòng 20)	k_{20}	$(K_R \lll_{94})_R$
F (vòng 21)	k_{21}	$(K_A \lll_{94})_L$
F (vòng 22)	k_{22}	$(K_A \lll_{94})_R$
F (vòng 23)	k_{23}	$(K_L \lll_{111})_L$
F (vòng 24)	k_{24}	$(K_L \lll_{111})_R$
	kw_3 kw_4	$(K_B \lll_{111})_L$ $(K_B \lll_{111})_R$

Bảng 5: Khóa vòng cho khóa bí mật 256 bit

2.2.3.3. Chế độ hoạt động của Camellia

Các chế độ hoạt động của Camellia được quy định tại Mục 2.3 của Quy chuẩn này.

2.2.3.4. Khóa

Độ dài khóa sử dụng trong mã khối Camellia được quy định

Độ dài khối	Tên thuật toán	Độ dài khóa quy định áp dụng
128 bit	Camellia	Không nhỏ hơn 256 bit

2.3. Chế độ hoạt động của mã khối

Mục này của Quy chuẩn sử dụng một số ký hiệu sau:

C	Khối bản mã
CTR	Giá trị đếm
i	Biến lặp
j	Kích thước của biến bản rõ/bản mã
K	Khóa mật mã
n	Độ dài khối bản mã/bản rõ đối với một mã khối
m	Số khối bản mã được lưu trữ
P	Khối bản rõ
q	Số các biến bản rõ/bản mã
r	Kích thước bộ đệm phản hồi
SV	Biến khởi đầu
X	Khối đầu vào mã khối
Y	Khối đầu ra mã khối

2.3.1. Chế độ xích liên kết khối mã CBC (Cipher Block Chaining)

Chế độ CBC được xác định bởi một tham số xen kẽ $m > 0$, số khối bản mã phải được lưu trữ trong khi xử lý trong chế độ này. Giá trị của m cần nhỏ (thông thường $m = 1$) và lớn nhất là 1024.

a) Các biến được sử dụng trong chế độ CBC:

1) Dãy q khối bản rõ có độ dài n bit $P_1, P_2, \dots, P_q$.

2) Khóa bí mật K.

3) Dãy các biến khởi đầu có độ dài n bit $SV_1, SV, \dots, SV_m$.

b) Các biến đầu ra là dãy q biến bản mã có độ dài n bit $C_1, C_2, \dots, C_q$

2.3.1.1. Phép mã hóa

Phép mã hóa của chế độ CBC như sau:

$$C_i = e_K(P_i \oplus SV_i), 1 \le i \le \min(m, q)$$

Nếu $q > m$, các khối bản rõ theo sau được mã hóa như sau:

$$C_i = e_K(P_i \oplus C_{i-m}), m + 1 \le i \le \mathrm{q}$$

CHÚ THÍCH: Tại bất kỳ thời điểm nào trong quá trình tính toán, giá trị của khối bản mã m gần nhất cần được lưu trữ.

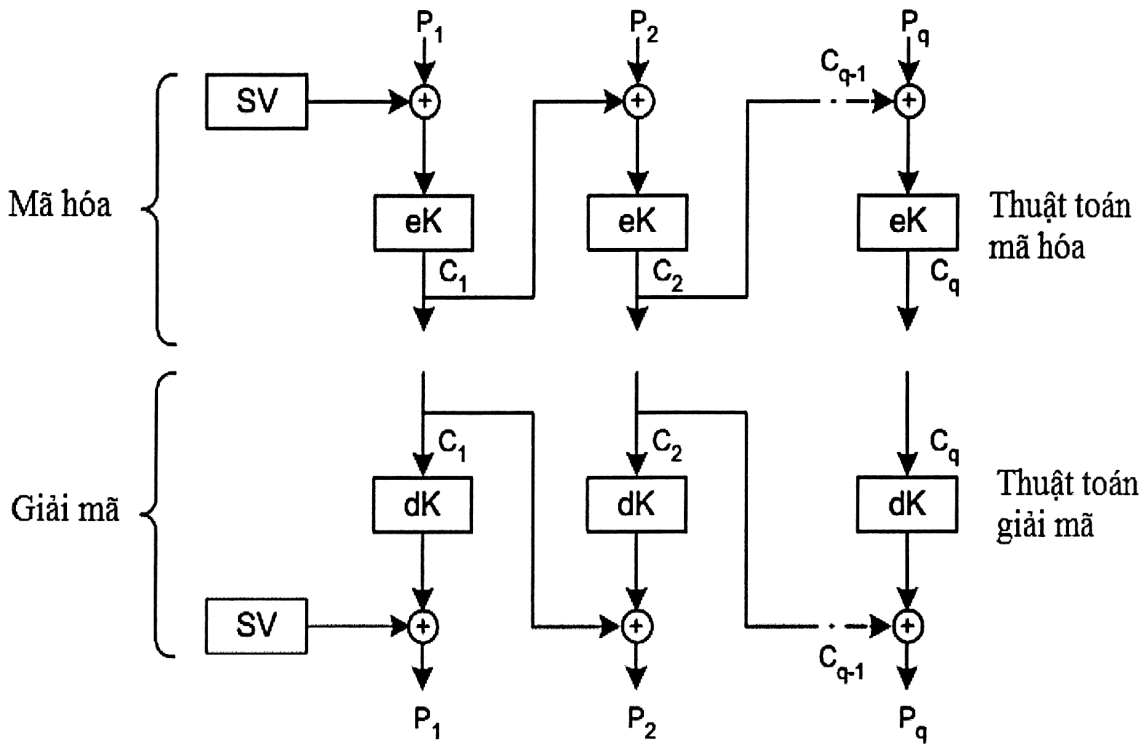
2.3.1.2. Phép giải mã

Phép giải mã của chế độ CBC như sau:

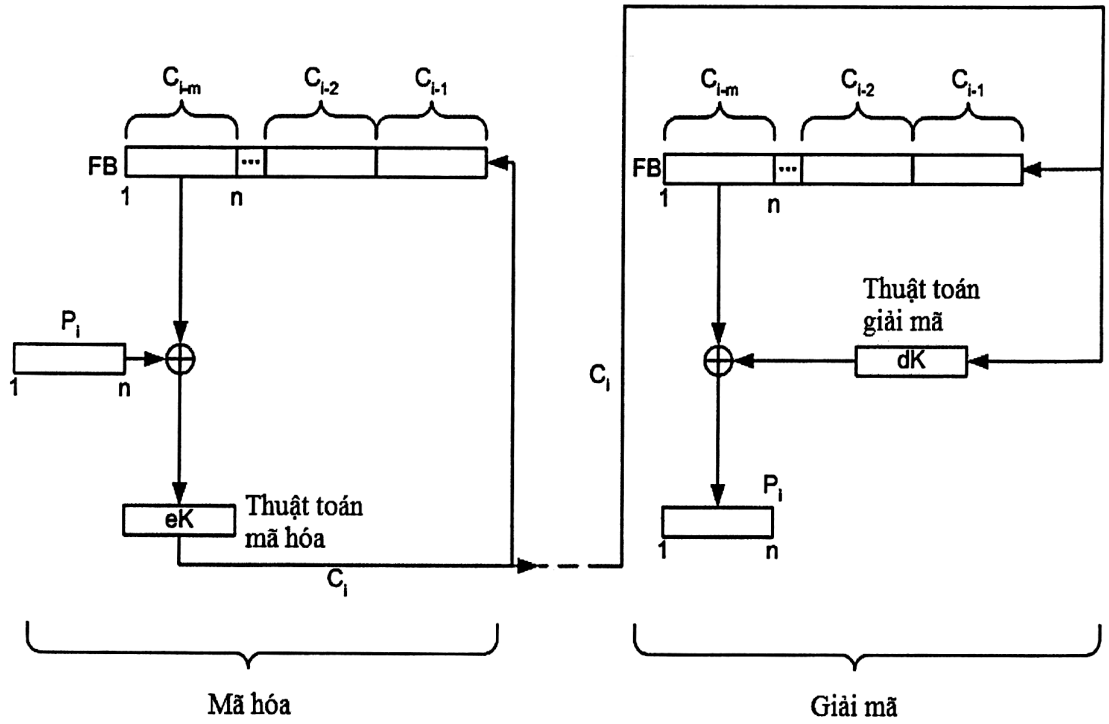
$$P_i = d_K(C_i) \oplus SV_i, 1 \leq i \leq \min(m, q)$$

Nếu $q > m$, các khối bản rõ theo sau được mã hóa như sau:

$$P_i = d_K(C_i) \oplus C_{i-m}, m + 1 \leq i \leq q$$



Hình 8: Chế độ xích liên kết khối mã với $m = 1$



Hình 9: Chế độ xích liên kết khối mã

- Biến khởi đầu SV được sinh ngẫu nhiên, giữ bí mật và thông báo cho nhau.

- Yêu cầu về đệm (padding)

+ Nếu độ dài bản rõ không phải là bội số của n thì yêu cầu sử dụng phương pháp đệm (padding) sau để bổ sung bản rõ sao cho độ dài của bản rõ là bội số của n:

Thêm một bit 1 vào cuối bản rõ, tiếp sau là các bit 0 (có thể không cần) để được bản rõ có độ dài là bội số của n. Đây chính là phương pháp đệm 2 trong tiêu chuẩn ISO/IEC 9797-1 hoặc ISO/IEC 10118-1.

(Xem tiếp Công báo số 1179 + 1180)

VĂN PHÒNG CHÍNH PHỦ XUẤT BẢN

Địa chỉ:	Số 1, Hoàng Hoa Thám, Ba Đình, Hà Nội
Điện thoại liên hệ:	
- Nội dung:	080.44417; Fax: 080.44517
- Phát hành:	080.48543
Email:	congbao@chinhphu.vn
Website:	http://congbao.chinhphu.vn
In tại:	Xí nghiệp Bản đồ 1- Bộ Quốc phòng

Giá: 10.000 đồng