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

MỤC LỤC

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.

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

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

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

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

|| phép ghép các xâu bit

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

(i) $0 \le b < n$

(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 $(A + B) \bmod 2^t$

$\boxminus$ 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 $(A - B) \bmod 2^t$

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 bít	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 hóa và giải mã DES. Khóa của TDEA gồm ba khóa *K1, K_2 và K_3* là những khóa DES khác nhau *($K1 \neq K_2$, $K_2 \neq K_3$, 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

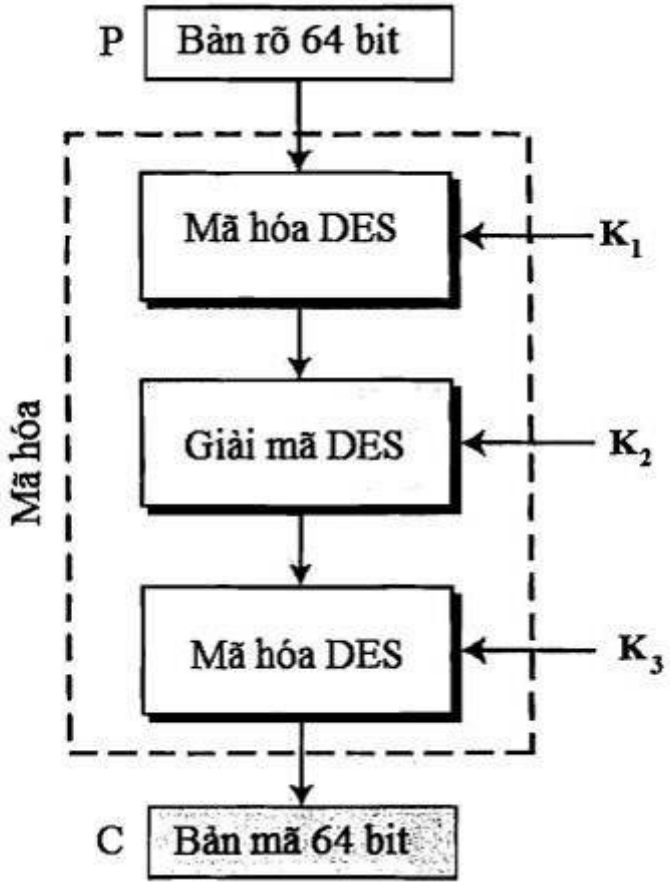
TDEA được xác định theo thuật ngữ của phép toán của DES, ở đấy E_k là phép toán mã hóa của DES với khóa *K* và D_k là phép giải mã của DES với khóa *K*.

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.



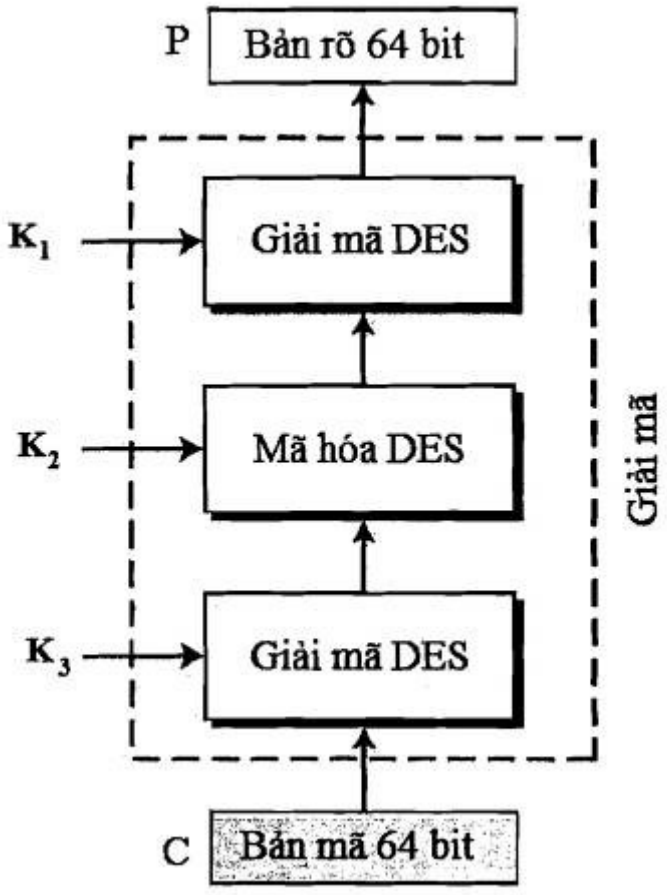
Hình 1: Sơ đồ phép mã hóa TDEA

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 bít (số cột) của Trạng thái.

Trong Quy chuẩn này thuật toán AES, độ dài k hóa 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.

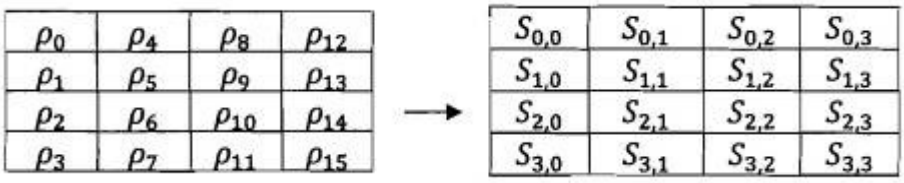
3) Trộn dữ liệu trong mỗi cột của mảng Trạng thái.

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 $0 \le r < 4$ và số cột *c*, với $0 \le c < 4$. 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 p_i byte bản rõ, tính từ trên xuống dưới và từ trái sang phải và được minh họa trên Hình 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 lí 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 lí 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 $0 \le j < 4(Nr + 1)$.

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 ($j \bmod \boldsymbol{Nk} = 0$) then

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

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

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

else

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

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

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 lí 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:

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

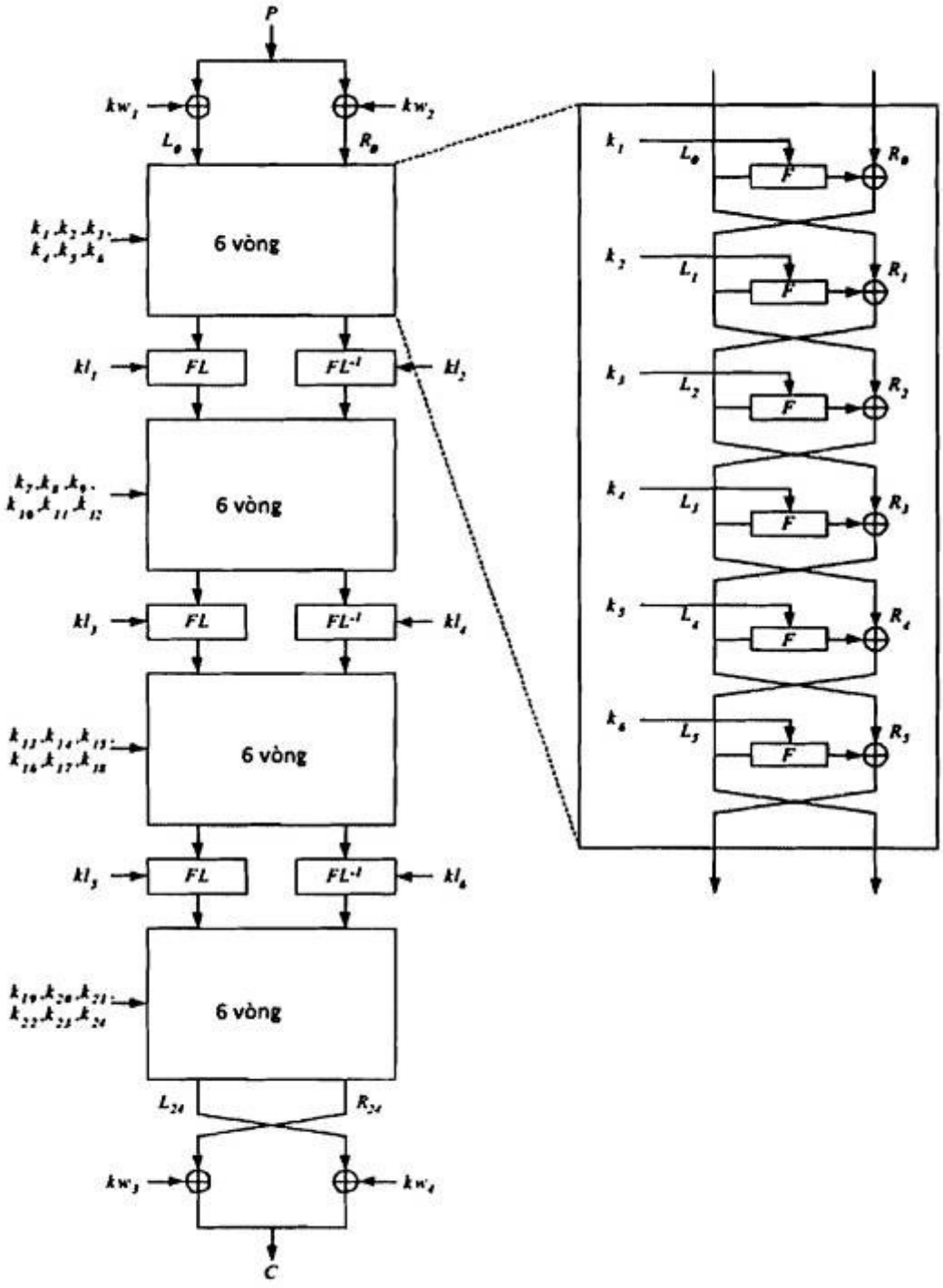
$R_i = L_{i-1}$

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) $\mathrm{C} = (\mathrm{R}_{24} \oplus \mathrm{kw}_3) \parallel (\mathrm{L}_{24} \oplus \mathrm{kw}_4)$



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

(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) $\mathrm{P} = (\mathrm{L_0} \oplus \mathrm{kw_1}) \| (\mathrm{R_0} \oplus \mathrm{kw_2})$