1. Giới thiệu S-DES

Simplified DES (S-DES), được phát triển bởi GS. Edward Schaefer trường đại học Santa Clara [1]. Giải thuật mã hóa S-DES nhận dữ liệu đầu vào trên bản rõ theo khối 8-bit (ví dụ: 10111101) và khóa 10 bit để tạo ra dữ liệu đầu ra là bản mã theo khối 8-bit. Ngược lại giải thuật giải mã S-DES nhận dữ liệu đầu vào bản mã theo khối 8-bit và khóa 10-bit để tạo ra dữ liệu đầu ra là bản rõ theo khối 8-bit.

Giải thuật mã hóa gồm 5 chức năng:

- hàm initial permutation (**IP**);
- một hàm phức tạp gọi là fK với tham số K_1 sinh ra từ khóa "key"
- một hàm hoán vị đơn giản (**SW**);
- hàm fK một lần nữa với tham số K_2 sinh ra từ khóa "key"
- một hàm hoán vị là nghịch đảo của hàm **IP** gọi là $\mathbf{IP}^{-1}$

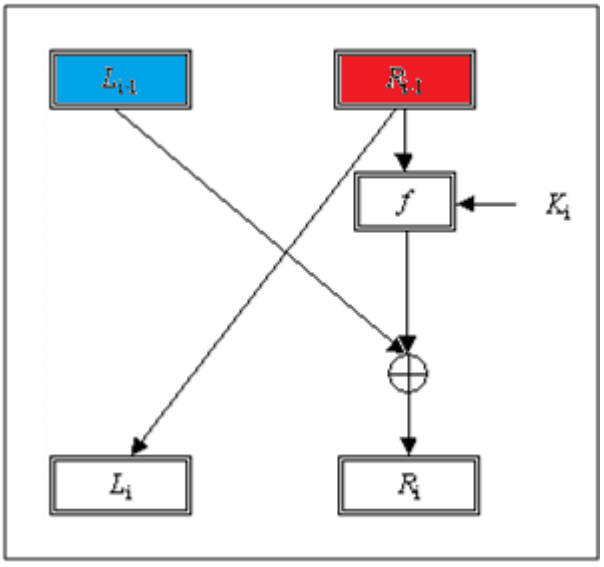
Có thể biểu diễn giải thuật mã hóa bằng hàm hợp như sau:

$$IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP$$

hoặc dạng sau: $ciphertext = \boldsymbol{IP^{-1}}\left(f_{K_2}\left(\boldsymbol{SW}\left(f_{K_1}(\boldsymbol{IP}(plaintext))\right)\right)\right)$

với: $$K_1 = \boldsymbol{P8}\left(Shift(\boldsymbol{P10}(key))\right)$$

*các hàm hoán vị **P8** và **P10** được giải thích trong mục 2.*



Hình 1 Sơ đồ biến đổi một vòng lặp (gồm f_{K_1} và SW)

2. Hàm sinh khóa trong S-DES

Khóa sử dụng trong S-DES phụ thuộc vào khóa 10-bit chia sẻ giữa người gửi và người nhận. Từ khóa này, hai khóa "con" 8-bit được sinh ra và dùng trong các bước cụ thể của giải thuật mã hóa và giải mã.

Đầu tiên, hoán vị khóa theo cách thức sau: giả sử khóa 10-bit kí hiệu là

$$k_1 \cdot k_2 \cdot k_3 \cdot k_4 \cdot k_5 \cdot k_6 \cdot k_7 \cdot k_8 \cdot k_9 \cdot k_{10}$$

Hàm hoán vị P10 được định nghĩa như sau:

$$P10(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) = (k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6)$$

Một cách biểu diễn khác của P10

P10									
3	5	2	7	4	10	1	9	8	6

Sau đó thực hiện phép dịch trái vòng (circular left shift - LS1) trên hai phần tách biệt là nửa 5-bit đầu và nửa 5-bit sau . Sau đó là hàm P8 để lấy ra và hoán vị 8 trong số 10 bit.

P8							
6	3	7	4	8	5	10	9

Ví dụ:

Tạo khóa K_1 từ khóa ban đầu "key" (1010000010): khóa ban đầu được biến đổi thành$(10000 - 01100)$. Thực hiện phép LS1 trên hai nửa trái-phải cho kết quả là $(00001 - 11000$ (*). Áp dụng biến đổi P8 ta có khóa con subkey $K_1 = 10100100$.

Tạo khóa K_2: Cặp chuỗi 5-bit sinh ra ở (*) được thực hiện phép LS2 (dịch trái vòng 2 bit) trên mỗi hai nửa trái-phải. Trong ví dụ trên, giá trị $(00001 - 11000)$ được biến đổi thành $(00100 - 00011)$. Cuối cùng, thực hiện biến đổi P8 để tạo khóa con subkey $K_2 = (01000011)$

3. Hàm mã hóa trong S-DES

Initial and Final Permutation

The initial IP function biểu diễn như sau

IP							
2	6	3	1	4	8	5	7

Hàm final Permutation biểu diễn như sau:

IP^{-1}							
4	1	3	5	7	2	8	6

Có thể dễ dàng chứng minh hàm final permutation là hàm nghịch đảo của hàm initial permutation vì $IP^{-1}(IP(X))=X$.

Ví dụ: Bản rõ (10111101) biến đổi qua IP trở thành (01111110). Chia giá trị có được thành hai phần, nửa trái (0111) và nửa phải (1110)

Hàm f_K

Thành phần phức tạp nhất trong S-DES là hàm f_k, gồm nhiều hàm permutation và substitution kết hợp với nhau. Hàm f_K được mô tả như sau. Gọi L và R là phần 4-bit trái và phần 4-bit phải của dữ liệu đầu vào f_k 8-bit; gọi F là một ánh xạ (không bắt buộc là ánh xạ 1:1) từ chuỗi 4-bit đến chuỗi 4-bit:

$$f_K(L,R) = (L \oplus F(R,SK),R)$$

với SK là khóa con (subkey) và $\oplus$ là hàm exclusive-OR trên bit.

Ánh xạ F được mô tả như sau: dữ liệu đầu vào là một số 4-bit $(n_1n_2n_3n_4)$. Phép biến đổi đầu tiên là phép expansion/permutation:

E/P							
4	1	2	3	2	3	4	1

Để dễ mô tả, phép biến đổi E/P có thể được biểu diễn theo cách khác như sau:

E/P							
n_4	n_1	n_2	n_3	n_2	n_3	n_4	n_1

Khóa con 8-bit $K_1 = (k_{11},k_{12},k_{13},k_{14},k_{15},k_{16},k_{17},k_{18})$được thêm vào giá trị này qua phép exclusive-OR:

Exclusive-OR							
$n_4 \oplus k_{11}$	$n_1 \oplus k_{12}$	$n_2 \oplus k_{13}$	$n_3 \oplus k_{14}$	$n_2 \oplus k_{15}$	$n_3 \oplus k_{16}$	$n_4 \oplus k_{17}$	$n_1 \oplus k_{18}$

4 bit đầu tiên (dòng đầu tiên của ma trận ở trên) được đưa vào S-box S0 để sinh ra dữ liệu 2-bit; 4-bit còn lại (dòng thứ hai) được đưa vào S1 để tạo nên dữ liệu 2-bit. Hai S-box được mô tả như sau

$$S0 = \left[\begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix}\right] \qquad S1 = \left[\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}\right]$$

Hàm S-box hoạt động như sau: bit thứ nhất và bit thứ tư được dùng là 2-bit xác định dòng của S-box, và bit thứ hai và bit thứ ba xác định cột của S-box. Giá trị tương ứng với hàng cột này được lấy làm giá trị đầu ra 2 0bit. Ví dụ dữ liệu đầu vào 4bit là (0100)thì dữ liệu đầu ra tương ứng với hàng 0 (bit 1&4 là 00) và cột 2 (bit 2&3 là 10) là (11). Vậy S0-box biến đổi $(0100) \rightarrow (11)$

Cuối cùng giá trị đầu ra của S-box S0 và S1 được biến đổi qua hàm permutation P4

P4			
2	4	3	1

Ví dụ:

B1: Giả sử dữ liệu có được ở bước IP là (01111110). Nửa 4-bit trái là (0111) và nửa 4-bit phải là (1110)

B2: nhân đôi giá trị 4-bit (1110) có giá trị 8-bit (11101110). Thực hiện biến đổi E/P có được (01111101)

B3: với khóa K1 $(1010 - 0100)$ ở trên, thực hiện biến đổi Exclusive-OR

$Exclusive - OR(01111101,10100100) = (01111101) \oplus (10100100) = (11011001)$

B4: thực hiện biến đổi S0-box 4-bit trái(1101)có được (11); thực hiện biến đổi S1-box 4-bit phải (1001)có được (10). Kết hợp hai kết quả ta có giá trị 4-bit $(11 - 10)$

B5: biến đổi giá trị $(11 - 10)$ với P4 ta được (1011)

B6: lấy giá trị 4-bit trái ở B1 (0111) để thực hiện Exclusive-OR giá trị có được ở B5 (1011): $(0111) \oplus (1011) = (1100)$

B7: kết hợp giá trị 4-bit trái có được ở B6 (1100)và 4-bit phải có được ở B1(1110) ta có được giá trị $(1100 - 1110)$ là đầu vào của hàm SW.

(Các bước biến đổi tiếp theo có thể được tham khảo ở phụ lục đính kèm)

Hàm hoán đổi (Switch - SW)

Hàm f_K chỉ thay đổi 4-bit bên trái của dữ liệu đầu vào. Hàm hoán đổi (SW) hoán chuyển giữa 4-bit bên trái và phải. Như vậy ở vòng lặp tiếp theo sẽ biến đổi các dữ liệu của 4-bit. Hàm SW biểu diễn như sau:

SW							
5	6	7	8	1	2	3	4

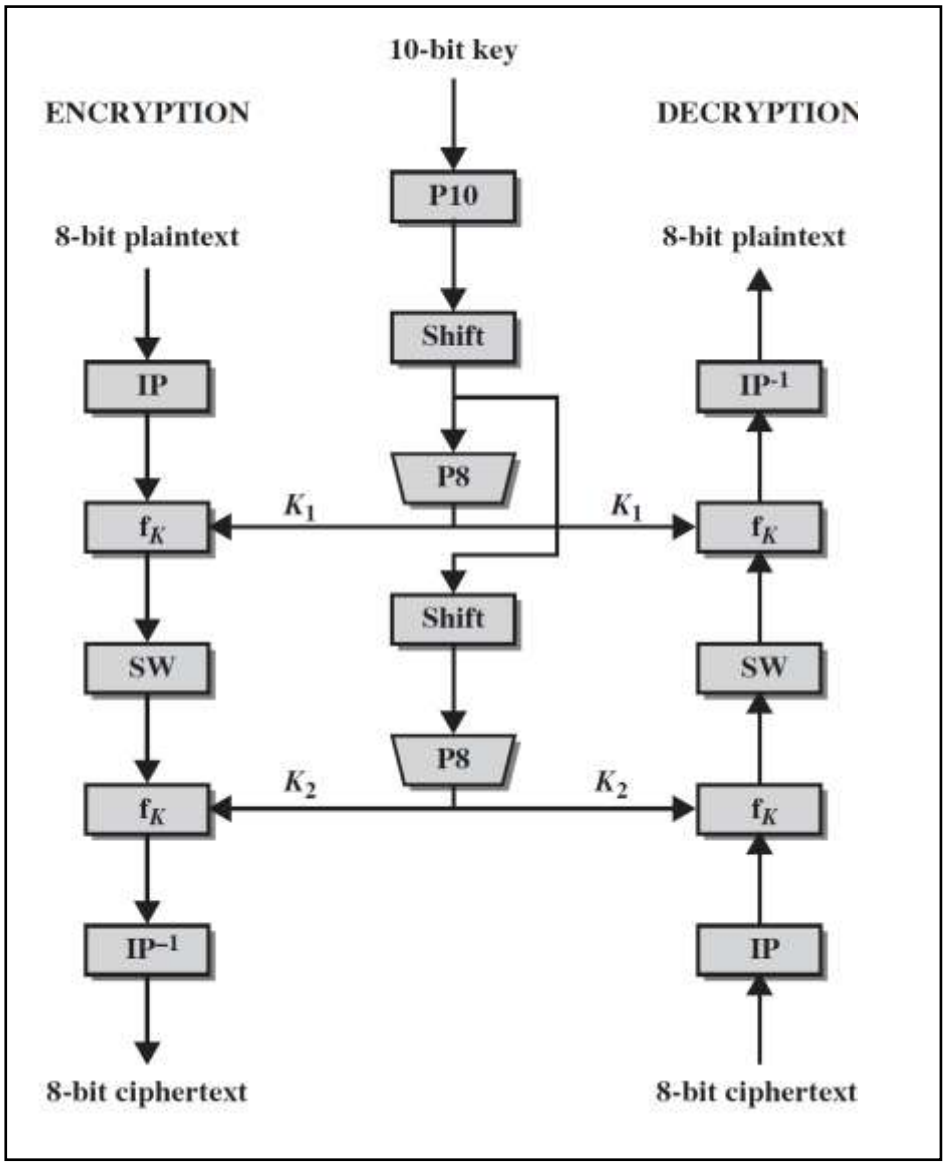
4. Mối liên hệ giữa DES và S-DES

DES biến đổi dữ liệu khối 64-bit, sơ đồ biến đổi có thể được biểu diễn như sau:

$$IP^{-1} \circ f_{K_{16}} \circ SW \circ f_{K_{15}} \circ SW \circ \cdots \circ SW \circ f_{K_1} \circ IP$$

Một khóa 56-bit được sử dụng sẽ sinh ra các khóa con subkey 48-bit. Biến đổi bao gồm một phép initial permutation 64-bit và tiếp theo là một loạt các biến đổi substitution và permutation 48-bit.

Trong hàm mã hóa, thay vì ánh xạ F biến đổi dữ liệu 4-bit, nó sẽ biến đổi dữ liệu 32bit. Sau biến đổi expansion/permutation, dữ liệu đầu ra 48 bit sẽ được thêm khóa con 48-bit bởi phép exclusive-OR. Có 8 S-box với kích thước 4 dòng và 16 cột. Bit đầu tiên và bit cuối cùng sẽ xác định hàng của giá trị đầu ra của S-box, 4-bit giữa sẽ xác định giá trị cột.



Hình 2 Sơ đồ S-DES

Phụ lục - Biến đổi dữ liệu mẫu của S-DES