

# MATH 314 Spring 2018 - Class Notes

10/10/2018

Montel Medley

**Summary:** Simplified Data Encryption Standard (SDES) structure, rules and example.

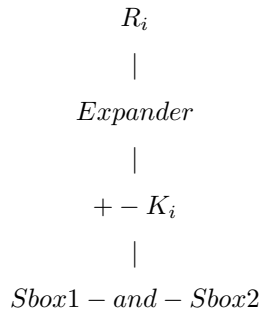
SDES (Simplified DES)

- 3 Rounds
- 12 bit block length (key has 9 bits)
- $f$  function-same design as DES, just with 12 bits

From the master key, we get around key,  $i$ , (which has 8-bits) by starting with the  $i$ th bit and taking 8 bits and wrapping around if necessary.

$L_i$  (6 bits),  $R_i$  (6 bits),  $f(R, K)$ -Round Key

SDES  $f$ -function (6 bit  $R_i$ , 8-bit  $K_i$ ) outputs 6 bits  
 $F$ -function



$K_i$  - (Round Key)  
 $Expander$  - 6 bit to 8 bit  
 $Sbox1$  (3 bits),  $Sbox2$  (3 bits)

S1	0	1	2	3	4	5	6	7
0	101	010	001	110	011	100	111	000
1	001	100	110	010	000	111	101	010
S2	0	1	2	3	4	5	6	7
0	100	000	110	101	111	001	011	010
1	101	011	000	111	110	010	001	100

*Expander*

1	2	3	4	5	6
---	---	---	---	---	---

(Diffusion)

|

1	2	4	3	4	3	5	6
---	---	---	---	---	---	---	---

Encrypt  $p = 101101110101$  using  $k = 111010110$  (SDES)  
 Round Keys

$$k_1 = 11101011$$

$$k_2 = 11010110$$

$$k_3 = 10101101$$

$$L_0 = 101101 \text{ --- } R_0 = 110101$$

$$L_1 = 110101 \text{ --- } R_1 = 000011$$

Round 1

$$110101(R_0)$$

|

$$f(110101, 11101011)$$

|

$$101110$$

+

$$101101$$

-----

$$000011 - R_1$$

In the  $f$  function:

$$110101$$

|

*Expander*

|

$$11101001$$

+

$$11101011 - k_1$$

-----

$$00000010$$

$$0000 - 0010$$

$S1 = 101$  and  $S2 = 110$

101110

Round 2

$L_1 = 110101$   $R_1 = 000011$   $L_2 = 000011$

000011( $R_1$ )

|

$f(000011, 11010110)$

|

111001

+

110101

-----

001100 -  $R_2$

In the  $f$  function:

000011

|

*Expander*

|

00000011

+

11010110 -  $k_2$

-----

11010101

1101 - 0101

$S1 = 111$  and  $S2 = 001$

111001

Round 3

$L_2 = 000011$   $R_2 = 001100$   $L_3 = 001100$

001100( $R_2$ )

|

$f(001100, 10101101)$

|  
100000  
+  
000011  
-----  
100011 -  $R_3$

In the  $f$  function:

001100  
|  
*Expander*  
|  
00111100  
+  
10101101 -  $k_3$   
-----  
10010001  
1001 - 0001  
  
100000

$S1 = 100$  and  $S2 = 000$

$C$ -ciphertext

$C = L_3 + R_3 = 001100100011$

- To decrypt, flip left and right halves.
- Do some steps using round keys in reverse order.
- Swap final left-right to get plaintext.