S-DES (simplified Data Encryption Standard) Assignment template:

ENCRYPTION TEMPLATE

<table>
<tr>
<td>
To the input (plaintext), apply initial permutation IP:

IP							
2	6	3	1	4	8	5	7

In the next steps, we will develop 4 bits with which to replace the left half of this "blue" result.
</td>
<td>
Input:

—— —— —— —— —— —— —— ——

—— —— —— —— —— —— —— ——
</td>
</tr>
<tr>
<td>
To right 4 bits of above result, apply expansion/permutation E/P (generating 8 bits from 4). The bit numbering is that of the 4-bit right-nibble, not of the 8-bit byte (e.g., indicated bit 2 refers to byte's bit 6).

E/P							
4	1	2	3	2	3	4	1
</td>
<td>
—— —— —— —— —— —— —— ——
</td>
</tr>
<tr>
<td>
Upon above result, perform binary XOR operation with
subkey K1:

K1							
1	0	1	0	0	1	0	0
</td>
<td>
—— —— —— —— —— —— —— ——
</td>
</tr>
<tr>
<td>
Determine a row and a column from above XOR result. For the row, combine bits 1 and 4 and convert to decimal. For the column, combine bits 2 and 3 and convert to decimal.

Determine another row and column. For this second row, combine bits 5 and 8; for this second column, bits 6 and 7.

Identify the entry in s-box S0 at the first row/first column you determined. S0 shows it in decimal; convert it to binary (two bits). Enter those bits as the first
</td>
<td>
</td>
</tr>
</table>

half of the 4-bit number at right. Identify the entry in s-box S1 at the second row/second column you determined. Convert it to binary; enter those two bits as the second half of the number at right.

S0 =		c0	c1	c2	c3
	r0	1	0	3	2
	r1	3	2	1	0
	r2	0	2	1	3
	r3	3	1	3	2

___ ___ ___ ___

S1 =		c0	c1	c2	c3
	r0	0	1	2	3
	r1	2	0	1	3
	r2	3	0	1	0
	r3	2	1	0	3

To above result, apply permutation P4:

P4			
2	4	3	1

___ ___ ___ ___

Upon the above P4 result, perform binary XOR operation, combining it with the left 4-bits of our first result (application of IP to original plaintext input, blue cell above).

We are trying to replace the left half of that first result. These XOR result bits are the replacement bits for it.

___ ___ ___ ___

Rewrite that "blue" first result with its left half replaced. (Look it up,

keep/copy its right half, use the preceding result as the new left half.)	___ ___ ___ ___ ___ ___ ___ ___
Swap the two 4-bit halves of the above (previous) result. In the next steps, we will again develop 4 replacement bits, and with them replace the left half of this "green" swap result. The steps will be the same ones used for that purpose already.	___ ___ ___ ___ ___ ___ ___ ___
To right 4 bits of above swap result, apply expansion/permutation E/P (generating 8 bits from 4): 	E/P							
---	---	---	---	---	---	---	---
4	1	2	3	2	3	4	1		___ ___ ___ ___ ___ ___ ___ ___
Upon above result, perform binary XOR operation with subkey K2: 	K2							
---	---	---	---	---	---	---	---
0	1	0	0	0	0	1	1		___ ___ ___ ___ ___ ___ ___ ___
Determine a row and a column from above result. For the row, combine bits 1 and 4 and convert to decimal. For the column, combine bits 2 and 3 and convert to decimal. Determine another row and column. For this second row, combine bits 5 and 8; for this second column, bits 6 and 7. Identify the entry in s-box S0 at the first row/first column you determined. It's given in decimal; convert it to binary (two bits). Enter those bits as the first half of the 4-bit number at right. Identify the entry in s-box S1 at the second row/second column you	

determined. Convert it to binary; enter
those two bits as the second half of the
number at right.

S0 =		c0	c1	c2	c3
	r0	1	0	3	2
	r1	3	2	1	0
	r2	0	2	1	3
	r3	3	1	3	2

—— —— —— ——

S1 =		c0	c1	c2	c3
	r0	0	1	2	3
	r1	2	0	1	3
	r2	3	0	1	0
	r3	2	1	0	3

To above result, apply permutation P4:

P4			
2	4	3	1

—— —— —— ——

Upon the above P4 result, perform
binary XOR operation, combining it
with the left 4-bits of the earlier swap
result (green cell above).

We are trying to replace the left half of
that swap result. These XOR result bits
are the replacement bits for it.

—— —— —— ——

Rewrite that "green" swap result with its
left half replaced. (Look it up,
keep/copy its right half, use the
preceding result as the new left half.)

—— —— —— —— —— —— —— ——

To above result, apply reverse of initial
permutation IP, which is IP^{-1}:

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

This result is ciphertext. It is the S-DES
encryption of the plaintext input.

—— —— —— —— —— —— —— ——