Fiestel Block Cipher - DES

\[ L_i = R_{i-1} \]
\[ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \]

\[ L_i = R_{i-1} \]
\[ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \]

32 to 48 bits
8 S Boxes
6 to 4 bits
32 to 32 (Straight) Permutation

Expansion Permutation
S-Box Substitution
P-Box Permutation

\[ L_{i-1} \]
\[ R_i \]
DES – Round Key Generation

- $L_0$, $R_0$
- $L_1$, $R_1$
- $L_r$, $R_r$
- $L_{15}$, $R_{15}$
- $L_{16}$, $R_{16}$

- $K_1$, 8 S Boxes – each 6 to 4 bits
- $K_r$
- Expansion Permutation
- S-Box Substitution
- P-Box Permutation

- $R_{i-1}$
- Compression Permutation

- Key
- Shift

- $K_i$
- $R_i$

- 32 to 48 bits
- 8 S Boxes 6 to 4 bits
- 32 to 32

- 56 to 48 bits
DES – Initial and Final Permutation
**DES – Algorithmic Overview**

- **T** – 64 bit input
- **K** – 64 bit key - leads to **K₀** – 56 bit key
  - **K₁, K₂, ..., K₁₆** (generated by round key generation)

\[ T₁ = IP(T) \] (Initial Permutation)

\[ (L₀, R₀) = T₁ \] (split into two 32 bit quantities)

\[ (L₁, R₁) = (R₀, L₀ \oplus F(R₀, K₁)) \]

\[ (L₂, R₂) = (R₁, L₁ \oplus F(R₁, K₂)) \]

\[ \vdots \]

\[ (L₁₆, R₁₆) = (R₁₅, L₁₅ \oplus F(R₁₅, K₁₆)) \]

\[ C₁ = (R₁₆, L₁₆) \] (swapping)

\[ C = FP(C₁) \] (Final Permutation)
## IP and FP

<table>
<thead>
<tr>
<th>Initial Permutation</th>
<th>Final Permutation</th>
</tr>
</thead>
<tbody>
<tr>
<td>58 50 42 34 26 18 10 2</td>
<td>40 8 48 16 56 24 64 32</td>
</tr>
<tr>
<td>60 52 44 36 28 20 12 4</td>
<td>39 7 47 15 55 23 63 31</td>
</tr>
<tr>
<td>62 54 46 38 30 22 14 6</td>
<td>38 6 46 14 54 22 62 30</td>
</tr>
<tr>
<td>64 56 48 40 32 24 16 8</td>
<td>37 5 45 13 53 21 61 29</td>
</tr>
<tr>
<td>57 49 41 33 25 17 9 1</td>
<td>36 4 44 12 52 20 60 28</td>
</tr>
<tr>
<td>59 51 43 35 27 19 11 3</td>
<td>35 3 43 11 51 19 59 27</td>
</tr>
<tr>
<td>61 53 45 37 29 21 13 5</td>
<td>34 2 42 10 50 18 58 26</td>
</tr>
<tr>
<td>63 55 47 39 31 23 15 7</td>
<td>33 1 41 9 49 17 57 25</td>
</tr>
</tbody>
</table>
DES – Round Function

\[ R_1 = F(R_0, k) \]
\[ R_0 \text{ – 32 bit round input} \]
\[ k \text{ – 48 bit round key} \]
\[ X = E(R_0) \text{ (Expansion Permutation)} \]
\[ X_1 = X \oplus k \text{ (XOR with round key)} \]
\[ X_2 = S(X_1) \text{ (apply S-Box substitution - output 32 bits)} \]
\[ R_1 = P(X_2) \text{ (apply round permutation)} \]

**E – Expansion Permutation**

|   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 32|  1|  2|  3|  4|  5|  6|  7|  8|  9|  10|  11|  12|  13|  14|  15|  16|  17|  18|  19|  20|  21|  22|  23|  24|  25|  26|  27|  28|  29|  30|  31|  32|  1 |

**P – Round Permutation**

|   | 16 |  7 |  20 |  21 |  29 |  12 |  28 |  17 |  1 |  15 |  23 |  26 |  5 |  18 |  31 |  10 |  2 |  8 |  24 |  14 |  32 |  27 |  3 |  9 |  19 |  13 |  30 |  6 |  22 |  11 |  4 |  25 |

**Diagram:**
- \( R_{i-1} \)
- **Expansion Permutation**
- **S-Box Substitution**
- **P-Box Permutation**
- \( K_i \)
- \( R_i \)
### DES – S-Boxes

<table>
<thead>
<tr>
<th>S-Boxes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$S_2$</td>
</tr>
<tr>
<td>$S_3$</td>
<td>$S_4$</td>
</tr>
<tr>
<td>$S_5$</td>
<td>$S_6$</td>
</tr>
<tr>
<td>$S_7$</td>
<td>$S_8$</td>
</tr>
</tbody>
</table>

Each $S$-Box is a permutation of 0 to 15 with 4 rows and 16 columns.

$X$ input - 48 bit data

$(X_1, X_2, \ldots, X_8)$ split $X$

$Y = (S_1(X_1), \ldots, S_8(X_8))$

- $b_6$ of $X_i$ chooses the row of $S_i$
- $b_5b_4$ of $X_i$ chooses the column of $S_i$
DES – Key Schedule

**K 64 bit key**

$r_i$ left shifts in round $i$

$r_i=1$ for $i=1,2,9,16$

$r_1=2$ for all other $i$

$K_i = PC(K)$

(Effective Key length is 56)

$(C_0, D_0) = K_1$

$(C_1, D_1) = (r_1(C_0), r_1(D_0))$

$k_1 = CP(C_1, D_1)$

$(C_2, D_2) = (r_2(C_1), r_2(D_1))$

$k_2 = CP(C_2, D_2)$

\[ \vdots \]

$k_{16} = CP(C_{16}, D_{16})$

---

**PC** (Permuted Choice)

<table>
<thead>
<tr>
<th></th>
<th>57</th>
<th>49</th>
<th>41</th>
<th>33</th>
<th>25</th>
<th>17</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>58</td>
<td>50</td>
<td>42</td>
<td>34</td>
<td>26</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>59</td>
<td>51</td>
<td>43</td>
<td>35</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>11</td>
<td>3</td>
<td>60</td>
<td>52</td>
<td>44</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>55</td>
<td>47</td>
<td>39</td>
<td>31</td>
<td>23</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>62</td>
<td>54</td>
<td>46</td>
<td>38</td>
<td>30</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>61</td>
<td>53</td>
<td>45</td>
<td>37</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>20</td>
<td>12</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**CP** - (Compression Permutation)

<table>
<thead>
<tr>
<th></th>
<th>14</th>
<th>17</th>
<th>11</th>
<th>24</th>
<th>1</th>
<th>5</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>28</td>
<td>15</td>
<td>6</td>
<td>21</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>19</td>
<td>12</td>
<td>4</td>
<td>26</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>7</td>
<td>27</td>
<td>20</td>
<td>13</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>52</td>
<td>31</td>
<td>37</td>
<td>47</td>
<td>55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>40</td>
<td>51</td>
<td>45</td>
<td>33</td>
<td>48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>49</td>
<td>39</td>
<td>56</td>
<td>34</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>42</td>
<td>50</td>
<td>36</td>
<td>29</td>
<td>32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>