1. \( C_0 D_0 = PC-1(K) \), perm matrix

\[
\begin{bmatrix}
57 & 49 & 41 & 33 & \ldots & 60 & 52 & 44 & 36
\end{bmatrix} \rightarrow C_0
\]

\[
\begin{bmatrix}
63 & 55 & 47 & 39 & \ldots & 28 & 20 & 12 & 4
\end{bmatrix} \rightarrow D_0
\]

2. for \( i = 1 \) to 16

\( C_i = LS_i (C_{i-1}) \)

\( D_i = LS_i (D_{i-1}) \)

\( LS_i = \text{left cyclic shift of either 1 or 2 bits} \)

(For \( LS_1, LS_2, LS_9, LS_{16} \) = 1)
\[ C_1 = [49 \ 41 \ 33 \ldots \ 60 \ 52 \ 44 \ 36 \ 57] \]
\[ D_1 = [55 \ 47 \ 39 \ldots \ 28 \ 20 \ 12 \ 4 \ 63] \]

\[ K_i^c = PC-2(C_iD_i) \]

Yet another perm matrix

**Left Shift**

**Before**

\[
\begin{array}{llllllll}
7 & 8 & 3 & 2 & \ldots & 4 & \ldots & 1 \\
\end{array}
\]

**After**

\[
\begin{array}{llllllll}
8 & 3 & 2 & \ldots & 4 & 7 \\
\end{array}
\]

Late 1990s DES challenge showed that brute force was possible so US Gov't contest for a new secure key encryption method

- 15 entries \(\Rightarrow\) 5 finalists

\[ \rightarrow \text{Winner, originally called Rijndahl - "Raijdel"} \]

Joan Daemen, Vincent Rijmen (Belgian)

Triple DES: \(\text{DES} \left( \text{DES} \left( \text{DES}(k_1, p), k_2 \right), k_3 \right) \)
AES

1) 3 specifications: 128 bits, 192 bits, 256 bits
both block, key size same. (much clearer,
also thought about future 3 version)

2) Modification in algorithm are relatively
simple

3) Good security w/10 rounds for 128 bits

Algorithm

1. $S = \text{AddRoundKey} (P, K_0)$
2. for $i = 1$ to 9
   
   \[
   S = \text{SubBytes} (S) \\
   S = \text{ShiftRows} (S) \\
   S = \text{MixColumns} (S) \quad \text{// hardest step} \\
   S = \text{AddRoundKey} (S, K_i)
   \]
3. $S = \text{SubBytes} (S) \\
   S = \text{ShiftRows} (S) \\
   S = \text{AddRoundKey} (S, K_{10})$
4. Return $S$
Skew Matrix for AES

Order of the bytes is \( S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, \ldots, S_{35} \)

\[ \text{1 1 1 1} \quad 128 \text{ bits} = 16 \text{ bytes} \]

Skew Matrix

1. Add Round Key
   XOR with Round Key

2. Shift Rows

(Old) goes to

\[ \begin{array}{cccc}
S_{00} & S_{01} & S_{02} & S_{03} \\
S_{10} & S_{11} & S_{12} & S_{13} \\
S_{20} & S_{21} & S_{22} & S_{23} \\
S_{30} & S_{31} & S_{32} & S_{33}
\end{array} \]