DES
- talk about the function $f(A, J)$ that's in each round (S-box design)
- key schedule
- look at my code

$f (A = \text{Bi-1 32 bits}, J = K_{i} 48 \text{ bits})$

1. Calculate $E(A)$ - expand $A$ to 48 bits using table $E$ (like a perm matrix)
   $A$ is $\text{1E8h}$ was $7CF63D28$
   
   $E(A) = 32, 1, 2, 3, 4, 5, 4, 5$
   $00111111$ (3F is 1st byte output)

2. Calc $E(A) \oplus J$ (round key
   XOR with round key
   hex $E(A) = 3F...$
   $\oplus J = 8C$

   $B3$
3. Let step 2 output be $B = B_1, B_2, ..., B_8$

\[ B_{\text{hex}} = \overline{B3CC0749CED2} \]

\[
\begin{align*}
B_1 &= 101100 \\
B_2 &= 111100 \\
B_3 &= 110000 \\
B_4 &= 000111 \\
B_5 &= 010010 \\
B_6 &= 011100 \\
B_7 &= 111111 \\
B_8 &= 010010
\end{align*}
\]

\[ C_i = S_i(B_i) \]

\[ S_1(B_1), S_2(B_2), ..., S_8(B_8) \]

Each S-box has 4 rows, 16 cols

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
0 & 1 & 2 & 3 \\
0 & 1 & 2 & 3 \\
0 & 1 & 2 & 3 \\
\end{array}
\]

Input = 6 bits
Output = 4 bits (only non-linear component)

\[ B_i = b_1b_2b_3b_4b_5b_6 \]

row = $b_1b_6$

col = $b_2b_3b_4b_5$

\[ S_i(101100) \]

row = 10 (2)

col = 0110 (6)

$S_i[27[6]] = 2[0010]$ Output


4. Return P(C) \{ P is another perm matrix \}

\underline{S-box Design}

P0: each row is perm of 0,1,2,...,15

P1: no S-box is a, linear or affine function of its inputs.

P2: Changing one input bit to an S-box causes at least 2 output bits to change.

P3: For any S-box and any input x, S(x) and S(x \oplus 001100) differ in at least 2 bits.

P4: For any S-box, any input x, and for e \in \{0,1\}, S(x) \neq S(x \oplus 110000)

P5: If we fix one input bit, and look at one output bit, there are 32 possibilities. The #s of 0s and 1s in the output must be in between 13 and 19.
Alg

1. $IP(X) = L_0 R_0$

2. Run 16 rounds:
   \[ L_i = R_{i-1} \]
   \[ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \]

3. Output $IP^{-1}(R_{16} L_{16})$

Will have key schedule for Monday.