2017 CIS 3362 Exam #2 Review Questions (taken from 2016 Exam #2)

1) In DES, which four inputs (of six bits) to S-box \( S_6 \) will create the four bit output 1101? (Please express each answer as bit strings of 0s and 1s.)

\[ \text{________, ________, ________, ________} \]

2) If the input to the E permutation (in the beginning of the Feistel function of DES) is \( 3AEF \text{ 8301} \) in hexadecimal, what are the first six hex characters (24 bits) of output?

\[ \text{____________________} \]

3) In the specification of DES, the key is represented as 64 bits, of which some are parity bits. Label all the bits (including parity bits) as \( k_1, k_2, \ldots, k_{64} \). If you knew the values of \( k_1 \) through \( k_{16} \), but had to perform a brute force search through the other bits of the key, how long, in the worst case, would it take you to find the key, given that you can search through \( 2^{20} \) keys in one second? Please express your answer in days, rounded to the nearest day.

\[ \text{____________________} \]

4) Consider the AES Key Schedule where we have

\[
\begin{align*}
    w[20] &= 01234567 \\
    w[23] &= 89abcdef \\
\end{align*}
\]

expressed in hex. Calculate \( w[24] \), filling in each intermediate step shown below:

\[
\begin{array}{|c|c|c|c|c|}
\hline
\text{RotWord} & \text{SubWord} & \text{Rcon[i/4]} & \text{XOR} & \text{FinalResult}(w[24]) \\
\hline
\end{array}
\]

5) In the AES Mix Columns operation, multiplication between terms must be performed. These multiplications are really in the field \( \text{GF}(2^8) \). Perform the following two multiplications in that field:

(a) \( 03 \times D3 \)

(b) \( 04 \times C9 \)

Note: Though we didn't explicitly cover how to do (b) in class, you can deduce how to do it by analyzing multiplication by \( 02 \), which we did cover in class and applying it to this situation.

(a) \( 03 \times D3 = \text{_______} \)

(b) \( 04 \times C9 = \text{_______} \)