Problem 2

Given: Alphabet $A$, blocklength $n \in \mathbb{N}$, $U = A^n = \mathbb{G}$

a) An encryption function is an injection function $e_K : M \rightarrow \mathbb{G}$ with $K \in \mathbb{G}$

injective function $f$:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

$$\left| \{ e_K(M) \mid M \in M \} \right| = |M|$$

$$\{ e_K(M) \mid M \in M \} \subseteq \mathbb{G} \Rightarrow e_K(M) = \mathbb{G}$$

$\Rightarrow e_K$ is also surjective $\Rightarrow e_K$ is a bijection

A permutation is a bijection function $\pi : X \rightarrow X$

$\Rightarrow \forall K \in \mathbb{G}$, the encryption $e_K$ is a permutation with $X = A^n$

b) $A = \mathbb{G}^{13}$, $n = 6$, there are $N = 2^6 = 64$ elements

$\Rightarrow$ there are $64! \approx 1.2689 \times 10^{89}$ different block ciphers.
P3

(a) The bit error occurs in block $c_i$, i > 0, with blocksize BS.

<table>
<thead>
<tr>
<th>mode</th>
<th>$M_i$</th>
<th>max # errors</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>$E_k^{-1}(c_i)$</td>
<td>8S</td>
<td>Only block $c_i$ is affected</td>
</tr>
<tr>
<td>CBC</td>
<td>$E_k^{-1}(c_i) \oplus c_{i-1}$</td>
<td>BS+1</td>
<td>$M_i$ and one bit in $M_{i+1}$ is affected</td>
</tr>
<tr>
<td>OFB</td>
<td>$c_i \oplus z_i$</td>
<td>1</td>
<td>$2_0 = c_0$, $2_i = E_k(2^{i-1})$</td>
</tr>
<tr>
<td>CFB</td>
<td>$c_i \oplus E_k(c_{i-1})$</td>
<td>BS+1</td>
<td>$M_i$ and one bit in $M_{i}$</td>
</tr>
<tr>
<td>CTR</td>
<td>$c_i \oplus E_k(2_i)$</td>
<td>1</td>
<td>$2_0 = c_0$, $2_i = 2^{i-1} + 1$</td>
</tr>
</tbody>
</table>

(b) One bit is later added at block $c_i$ at position $j$, i > 0

<table>
<thead>
<tr>
<th>mode</th>
<th>block</th>
<th>position</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECB</td>
<td>$c_i$</td>
<td>1</td>
</tr>
<tr>
<td>CBC</td>
<td>$c_i$</td>
<td>1</td>
</tr>
<tr>
<td>OFB</td>
<td>$c_i$</td>
<td>j</td>
</tr>
<tr>
<td>CFB</td>
<td>$c_i$</td>
<td>j</td>
</tr>
<tr>
<td>CTR</td>
<td>$c_i$</td>
<td>j</td>
</tr>
</tbody>
</table>

In ECB and CBC all bits of all blocks $c_{i+k}$, k > 0 may be corrupt.

In OFB, CFB, CTR all bits beginning at position $j$ in block $i$ may be corrupt.
\[
\begin{align*}
\text{P1} & \quad k = (2D \ 61 \ 72 \ 69 \ 65 \ 00 \ 66 \ 61 \ 16 \ E0 \ 04 \ 33 \ 6C \ 16 \ 56 \ 66 \ 66) \\
& = (W_0 \ W_1 \ W_2 \ W_3) \\
a) \quad k_0 = k = (W_0 \ W_1 \ W_2 \ W_3) \\
b) \quad k_1 = (W_4 \ W_5 \ W_6 \ W_7) \\
\text{Follow Fig. 1 to calculate } W_4, \text{ which are the first } 4 \text{ Bytes of } k_1 \\
\text{tmp} \leftarrow W_3 = (65 \ 65 \ 66 \ 66) \\
1) \quad \text{Evaluate Sub Bytes (RotBytes(tmp))} \oplus \text{Round}(i/4) \\
\quad i/4 = 1; \ \text{Round}(i) = (\text{RC}(1), \ 00, \ 00, \ 00) = (01, \ 00, \ 00, \ 00) \\
\quad \text{RotBytes(tmp)} = (65 \ 66 \ 66 \ 65) \quad \text{// cyclic left shift of bytes} \\
\quad \text{SubBytes}(65 \ 66 \ 66 \ 65) = (4D \ 33 \ 33 \ 40) \\
\quad \text{tmp} = (4D \ 33 \ 33 \ 40) \quad \text{// } 1.3 + 1.1 \\
2) \quad W_4 \leftarrow W_0 \oplus \text{tmp} \\
\end{align*}
\]