Exercise 6.1 (Playing fair revised). (4 points)

We are given a biased coin whose probability for flipping heads is \( p_H = 30\% \).

(i) Compute the information entropy of such a coin toss.  
(ii) What is the maximal entropy which can be expected of such a coin toss?  
(iii) What is the value of the entropy of a fair coin? Compare that to your previous results.

Exercise 6.2 (Entropy of a day). (3 points)

Suppose that on some machine, clock time is measured in nanoseconds \( 1 = 3 \times 10^{-9} \) seconds, and that we take the current time, modulo 24 hours, to be a random value. How many random bits would this provide? How many, if we take the time modulo one hour? Modulo one minute?

Exercise 6.3 (Distinguishing distributions). (3 points)

Consider the example from the lecture:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( g_2(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>001101</td>
</tr>
<tr>
<td>001</td>
<td>001011</td>
</tr>
<tr>
<td>010</td>
<td>011010</td>
</tr>
<tr>
<td>011</td>
<td>010110</td>
</tr>
<tr>
<td>100</td>
<td>101100</td>
</tr>
<tr>
<td>101</td>
<td>100110</td>
</tr>
<tr>
<td>110</td>
<td>110100</td>
</tr>
<tr>
<td>111</td>
<td>110010</td>
</tr>
</tbody>
</table>

Let \( A(y) \in \{0, 1\} \) be random, if the first four bits of \( y \) are half 0’s and half 1’s, otherwise let \( A(y) = 1 \), if \( y_5 = \text{minority}(y_1, y_2, y_3, y_4) \), and else \( A(y) = 0 \). Compute the prediction power of this algorithm.
Exercise 6.4 (Probabilities).

Consider the following generator \( g : \mathbb{B}^3 \rightarrow \mathbb{B}^5 \) and let \( (X_1, \ldots, X_5) := g(U_3) \).

\[
\begin{array}{cc|cc}
 x & g(x) & x & g(x) \\
 000 & 11100 & 100 & 00110 \\
 001 & 00101 & 001 & 11110 \\
 010 & 01011 & 110 & 01010 \\
 011 & 10101 & 111 & 01101 \\
\end{array}
\]

(i) Compute the distribution of the projection on the second to fourth bit, thus of \( (X_2, X_3, X_4) \).

(ii) Compute a table of the probabilities \( W(b \leftarrow X_4(y)) \) for all possible initial sections \( y \in \mathbb{B}^3 \) and all \( b \in \mathbb{B} \).

Exercise 6.5 (Distinguishers and predictors).

We are given the following generator \( g : \mathbb{B}^3 \rightarrow \mathbb{B}^6 \):

\[
\begin{array}{cc|cc}
 x & g(x) \\
 000 & 001100 \\
 001 & 001110 \\
 010 & 010101 \\
 011 & 011011 \\
 100 & 101000 \\
 101 & 100101 \\
 110 & 110010 \\
 111 & 110011 \\
\end{array}
\]

The algorithm \( U \) answers 1 if and only if at most four bits are 1, and 0 otherwise. The algorithm \( P \) returns the second bit.

(i) Show: \( U \) is a \( \frac{7}{64} \)-distinguisher between the output distribution \( p = g(u_3) \) of the generator and the uniform distribution \( u_6 \) on 6 bits.

(ii) Show: \( P \) is a \( \frac{1}{4} \)-predictor for the sixth bit under \( p \).

(iii) Find a predictor of higher quality and compute its prediction power.