Solution of Problem 1

Theorem 4.3 shall be proven.

a) $X$ is a discrete random variable with $p_i = P(X = x_i)$, $i = 1, \ldots, m$. It holds

$$H(X) = -\sum_i p_i \log(p_i) \geq 0,$$

as $p_i \geq 0$ and $-\log(p_i) \geq 0$ for $0 < p_i \leq 1$ and $0 \cdot \log 0 = 0$ per definition.

Equality holds, if all addends are zero, i.e.,

$$p_i \log(p_i) = 0 \iff p_i \in \{0, 1\} \quad i = 1, \ldots, m,$$

as $p_i > 0$ and $-\log(p_i) > 0$, thus, $-p_i \log(p_i) > 0$ for $0 < p_i < 1$.

b) It holds

$$H(X) - \log(m) = -\sum_i p_i \log(p_i) - \sum_{i=1} \log(m)$$

$$= \sum_{i:p_i>0} p_i \log \left( \frac{1}{p_i \cdot m} \right)$$

$$= (\log e) \sum_{i:p_i>0} p_i \ln \left( \frac{1}{p_i \cdot m} \right)$$

$$\leq (\log e) \sum_{i:p_i>0} p_i \left( \frac{1}{p_i \cdot m} - 1 \right)$$

$$= (\log e) \sum_{i:p_i>0} \left( \frac{1}{m} - p_i \right) = 0$$

As $\ln(x) = x - 1$ only holds for $x = 1$ it follows that equality holds iff $p_i = 1/m$, $i = 1, \ldots, m$. In particular, as $p_i = \frac{1}{m}$, it follows $p_i > 0$, $i = 1, \ldots, m$.

c) Define for $i = 1, \ldots, m$ and $j = 1, \ldots, d$

$$p_{ij} = P(X = x_i \mid Y = y_j).$$
Show $H(X \mid Y) - H(X) \leq 0$ which is equivalent to the claim.

$$H(X \mid Y) - H(X) = -\sum_{i,j} p_{i,j} \log(p_{i,j}) + \sum_{i} p_{i} \log(p_{i})$$

$$= -\sum_{i,j} p_{i,j} \log \left( \frac{p_{i,j}}{p_{j}} \right) + \sum_{i} p_{i,j} \log(p_{i})$$

$$= (\log e) \sum_{i,j:p_{i,j}>0} p_{i,j} \ln \left( \frac{p_{i}p_{j}}{p_{i,j}} \right)$$

$$\leq \ln(x) \leq x-1$$

$$\leq (\log e) \sum_{i,j:p_{i,j}>0} p_{i,j} \left( \frac{p_{i}p_{j}}{p_{i,j}} - 1 \right)$$

$$= (\log e) \sum_{i,j:p_{i,j}>0} (p_{i}p_{j} - p_{i,j}) = 0$$

Note that from $p_{i,j} > 0$ it follows $p_{i}, p_{j} > 0$. Equality hold for $p_{i}p_{j} = p_{i,j}$ which is equivalent to X and Y being stochastically independent.

This means that the mutual information $I(X, Y) = H(X) - H(X \mid Y)$ is nonnegative.

d) It holds

$$H(X, Y) = -\sum_{i,j} p_{i,j} \log(p_{i,j})$$

$$= -\sum_{i,j} p_{i,j} [\log(p_{i,j}) - \log(p_{i}) + \log(p_{i})]$$

$$= -\sum_{i,j} p_{i,j} \log \left( \frac{p_{i,j}}{p_{i}} \right) - \sum_{i} \sum_{j} p_{i,j} \log(p_{i})$$

$$= H(Y \mid X) + H(X).$$

e) It holds

$$H(X, Y) \overset{(d)}{=} H(X) + H(Y \mid X) \overset{(c)}{\leq} H(X) + H(Y)$$

with equality as in (c) iff X and Y are stochastically independent.
Solution of Problem 2
Recall: $H(x) = - \sum p_i \log(p_i)$.

a) $H(\hat{M}) = -\frac{1}{4} \log_2(\frac{1}{4}) - \frac{3}{4} \log_2(\frac{3}{4}) = \frac{1}{2} + \frac{3}{2} - \frac{3}{4} \log_2(3) \approx 0.811$

$H(\hat{K}) = -\frac{1}{2} \log_2(\frac{1}{2}) - 2\frac{1}{4} \log_2(\frac{1}{4}) = \frac{1}{2} + 1 = 1.5$

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>$\frac{1}{2}$</td>
</tr>
</tbody>
</table>

$P(\hat{C} = 1) = P(\hat{M} = a) \cdot P(\hat{K} = K_1) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$P(\hat{C} = 2) = P(\hat{M} = a) \cdot P(\hat{K} = K_2) + P(\hat{M} = b) \cdot P(\hat{K} = K_1) = \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} = \frac{7}{16}$

$P(\hat{C} = 4) = P(\hat{M} = b) \cdot P(\hat{K} = K_3) = \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}$

$\Rightarrow P(\hat{C} = 3) = 1 - P(\hat{C} = 1) - P(\hat{C} = 2) - P(\hat{C} = 4) = 1 - \frac{2}{16} - \frac{7}{16} - \frac{3}{16} = \frac{4}{16}$

$\Rightarrow H(\hat{C}) = -\frac{1}{8} \log_2(\frac{1}{8}) - \frac{7}{16} \log_2(\frac{7}{16}) - \frac{3}{16} \log_2(\frac{3}{16}) - \frac{1}{4} \log_2(\frac{1}{4}) \approx 1.850$

$\Rightarrow H(\hat{K} | \hat{C}) \text{ Thm. 4.7} = H(\hat{M}) + H(\hat{K}) - H(\hat{C}) \approx 0.811 + 1.5 - 1.850 = 0.461$

b) Lem. 4.12 b) demands $|C_+| \leq |K_+|$ for perfect secrecy.
   But in this case, we get $4 = |C_+| > |K_+| = 3$.

Solution of Problem 3
Show for any function $f : X(\Omega) \times Y(\Omega) \rightarrow \mathbb{R}$, that $H(X, Y, f(X, Y)) = H(X, Y)$.

By definition, we have:

$H(X, Y, Z = f(X, Y)) \overset{\text{Def.}}{=} \sum_{x,y,z} P(X = x, Y = y, Z = z) \log (P(X = x, Y = y, Z = z))$

With

$P(X = x, Y = y, Z = z) = \begin{cases} P(X = x, Y = y) & \text{if } Z = f(X, Y) \\ 0 & \text{if } Z \neq f(X, Y) \end{cases}$

it follows that

$H(X, Y, Z = f(X, Y)) = \sum_{x,y} P(X = x, Y = y) \log(P(X = x, Y = y)) = H(X, Y)$.

Note: It holds $0 \cdot \log 0 = 0$.
Solution of Problem 4

a) \[ H(M) = - \sum_i P(M_i) \log_2 P(M_i) = -\left( \frac{1}{3} \log_2 \frac{1}{3} + \frac{2}{3} \log_2 \frac{2}{3} \right) \]

b) (i) For each \( M \in \mathcal{M}_N, C \in \mathcal{C}_N \) there exists exactly one \( K \in \mathcal{K}_N \) such that \( e(M, K) = C \), namely \( K = (s_1, \ldots, s_N) \) with \( s_j = (c_j - a_j) \mod m \).

(ii) \( \tilde{K}_N \) is uniformly distributed over \( \mathcal{K}_N \), as
\[
P(\tilde{K}_N = K) = P(\tilde{K}_1 = s_1, \ldots, \tilde{K}_N = s_N) = \prod_{i=1}^N P(\tilde{K}_i = s_i) = \frac{1}{m^N} = \frac{1}{|\mathcal{K}_N|}
\]
for all \( K = (s_1, \ldots, s_N) \)

(iii) Disadvantage of Vernam Cipher: The main disadvantage of the Vernam Cipher is that: \( |\mathcal{K}_N| \geq |\mathcal{M}_N| \) (one needs at least as many keys as plaintexts) and these keys need to be communicated over a secure channel in advance.

c) \[ H(C, M) \stackrel{\text{chain-rule}}{=} H(C) + H(M|C) \stackrel{\text{perf. sec.}}{=} H(C) + H(M) \]

d) Due to the independence of \( X \) and \( Y \) we have \( p_Y(y|x) = p_Y(y) \), and
\[
\bar{H}(Y|X) = - \sum_x \sum_y p_Y(y) \log_2 p_Y(y) = |X| H(Y) \geq H(Y)
\]