Exercise 1

Show that, in any cryptosystem, it holds that $H(K|C) \geq H(P|C)$. Under which condition do we have equality?

Solution: Rewrite $H(P,K|C)$ with the identities given in Exercise 5.3, using $H((A|B)|C) = H(A|B,C)$:

$$H(P,K|C) = H(P|C) + H(K|P,C) = H(K|C) + H(P|K,C).$$

In any cryptosystem , given the key and ciphertext, the plaintext is uniquely determined, so $H(P|K,C) = 0$. Therefore,

$$H(P|C) + H(K|P,C) = H(K|C).$$

Which implies

$$H(P|C) = H(K|C) - H(K|P,C).$$

Since entropy is non-negative it follows that:

$$H(K|C) \geq H(P|C).$$

Equality holds if and only if $H(K|P,C) = 0$, which means that given the plaintext P and ciphertext C, the key K is uniquely determined. That is, for each pair (p,c), there is at most one key k such that $c = e_k(p)$.

Exercise 2

Compute $H(K|C)$ and $H(K|P,C)$ for the Affine cipher when used to encrypt a single letter from the English alphabet. Assume that keys and plaintexts are uniformly chosen.

Solution: We have $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and the key space $\mathcal{K} = \{(a,b) \mid a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\}$ with $|\mathcal{K}| = 12 \times 26 = 312$. (We have 12 elements of $\mathbb{Z}_{26}$ coprime to 26, so there are 12 units in $\mathbb{Z}_{26}$)

First, compute $H(K|C)$. Since keys are uniformly chosen, $P(K = k) = 1/312$. For a fixed ciphertext c, we have:

$$P(C = c) = \sum_k P(C = c|K = k)P(K = k).$$

For each key k, encryption is a permutation, so $P(C = c|K = k) = 1/26$, giving:

$$P(C = c) = \sum_k \frac{1}{26} \cdot \frac{1}{312} = \frac{1}{26}.$$

By Bayes' theorem:

$$P(K = k|C = c) = \frac{P(C = c|K = k)P(K = k)}{P(C = c)} = \frac{(1/26)\cdot(1/312)}{1/26} = \frac{1}{312}.$$

For each c, the distribution of K given $C = c$ is the same over every key, of which we have 312;

$$H(K|C = c) = \sum_k \frac{1}{312} \log 312 = \log 312.$$

Now, compute $H(K|P,C)$. For any plaintext-ciphertext pair, the key $k = (a,b)$ has:

$$c = ap + b \pmod{26}.$$

For each invertible $a \in \mathbb{Z}_{26}^*$ (Which we have 12 of), there is a unique $b = c - a \cdot p \pmod{26}$. So we have 12 keys that encrypt p to c: (continued on next page)

$$P(K=k|P=p,C=c)=\begin{cases}1/12 & \text{if } c=e_k(p),\\ 0 & \text{otherwise.}\end{cases}$$

Then the entropy is given by:

$$\begin{aligned}H(K|P=p,C=c)&=\sum_k P(K=k|P=p,C=c)\log\frac{1}{P(K=k|P=p,C=c)}\\&=12\cdot\left(\frac{1}{12}\log 12\right)\\&=\log 12.\end{aligned}$$