

Homework 28

Compute the entropy for the following key spaces for a shift cipher on \mathbf{Z}_{26} . Compute enough decimal places to see differences between them.

1. Pick $0 \leq K < 26$, all equally likely;
2. Pick $0 \leq a < 35$, all equally likely and let $K = a \bmod 26$;
3. Pick $0 \leq a < 2^{15}$, all equally likely and let $K = a \bmod 26$.

Homework 28 Solution

1. The entropy is

$$26 \cdot (-1) \cdot \frac{1}{26} \lg(1/26) = \lg(26) \approx 4.700439718141$$

2. It is easy to check that 9 numbers get picked twice, and 17 get picked once. So, 9 numbers have probability $2/35$ and the other 17 have probability $1/35$. So, the entropy is

$$9 \cdot (-1) \cdot \frac{2}{35} \lg(2/35) + 17 \cdot (-1) \cdot \frac{1}{35} \lg(1/35) \approx 4.614997302659$$

3. First $2^{15} \equiv 8 \pmod{26}$ (e.g., by square and multiply). So, 8 numbers get picked $\frac{2^{15}-8}{26} + 1 = 1261$ times, and 18 get picked $\frac{2^{15}-8}{26} = 1260$ times. So, the entropy is

$$8 \cdot (-1) \cdot \frac{1261}{2^{15}} \lg(1261/2^{15}) + 18 \cdot (-1) \cdot \frac{1260}{2^{15}} \lg(1260/2^{15}) \approx 4.70043962141$$