

Introduction to mathematical cryptography
Homework problems
Week 9

17. Prove the properties (H2) and (H3) of entropy.
18. We toss a fair coin a few times, and stop at the first head. Let X be the number of the tosses. Compute $H(X)$. (*Hint:* First, observe that $P(X = n) = 2^{-n}$, since X is n if and only if the first $n - 1$ tosses are all tails, and the n th one is a head. Therefore, you need to compute

$$H(2^{-1}, 2^{-2}, 2^{-3}, \dots).$$

It might be useful to compute the square of the identity

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

(which is valid for all $|x| < 1$). If you have learned absolute convergence, explain why this manipulation is correct – if not, don't worry about that.)

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.