

MATH 445, HOMEWORK 5

1. Compute the unicity distance for a Caesar shift.
2. Explain how the Vigenère cipher can be considered to be a block cipher, and compute the unicity distance for it.
3. Consider a block cipher where each block has n characters, and each block is encrypted by a chosen permutation of the n characters. (For example, if $n = 4$ and the fixed permutation sends 1 to 3, 2 to 1, 3 to 4, and 4 to 2, then the encryption of ABCD is BDAC, the encryption of FFGG is FGFG.) Here the permutation is the key. Assume that the plaintext consists of written English. What is the unicity distance of this block cipher? How does the unicity distance behave as $n \rightarrow \infty$? (Use Stirling's formula.)