COMPSCI-466: Homework 5

Problem 1. (100 points.) Let D be the set of all strings whose length is a positive multiple of 128. Define hash function $H\colon \{0,1\}^{128} \times D \to \{0,1\}^{128}$ as follows:

Algorithm $H_K(M)$:
  Parse M as $M[1]M[2]\ldots M[m]$
  $C[0] \leftarrow 0^{128}$
  For $i = 1$ to m do:
    $B[i] \leftarrow \mathsf{AES}_K(C[i-1] \oplus M[i])$
    $C[i] \leftarrow \mathsf{AES}_K(B[i] \oplus M[i])$
  Return $C[m]$

Above we parse M as consisting of m blocks of 128-bits each. Show that H is not collision-resistant by giving a practical adversary A such that its advantage $\mathbf{Adv}^{\mathrm{cr}}_H(A)$ is high. As usual, your adversary should be given in concise pseudocode (70 points) and you should formally analyze its advantage and resource usage (30 points).