1. CBC's encryption is performed serially, and the next plaintext group cannot be encrypted until the ciphertext group corresponding to the previous plaintext group is obtained.
   Therefore, there are 2 plaintext blocks will be corrupted, namely number t/2 and number t/2+1.

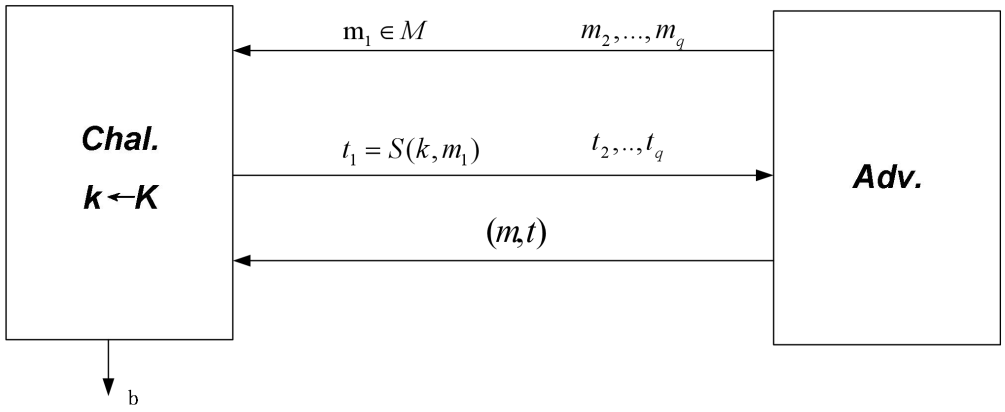
2. Define A's advantages: $Adv[A,\varepsilon] = \left|\Pr[W_0] - \Pr[W_1]\right|$.

   We know that the nonce will return to 0 when it reaches 100, and the procedure repeats.
   So, A will find the similarities every hundred.

   And the: $Adv[A,\varepsilon] = 1$.

   Therefore, the encryption is not semantic secure under a CPA attack.

3. Game as:



   $Adv_{\mathrm{MAC}}[A,I] = \Pr[Chal.outputs1] = 1/2 \neq negligible$

   Therefore, the MAC is not a secure MAC.