/0 (4pts) **Q1**: What are the properties that MACs achieve? Define each property you mention.

efficient

/1 (1pts) **Q2**: Which one of the following MAC constructions is the fastest and why: ECBC-MAC, NMAC, PMAC?

PMAC.

/0 (2pts) **Q3**: What is one-way hash function and what property it achieves?

function that hash the input and make the out Puts of the same inPuts differs in outPut.

$m_1 = m_2$

$c_1 \neq c_2$

/0 (2pts) **Q4**: Let $H : M \rightarrow T$ be a collision resistant hash function. Which of the following is collision resistant? Explain your answer.

1. $H'(m) = H(m)||H(m)$

   Not a Collision resistant

2. $H'(m) = H(0)$

   Collision resistant

/0 (1pt) **Q5**: Let *m* be a message consisting of *L* AES blocks (say *L=100*). Alice encrypts *m* using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number *L/4* is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted? Explain your answer.

~~100 AES blocks~~ 100 Plaintext blocks will be Corrupted.

All encrypted text depends oneach other.