Assignment 5: Network Security and Link Layer

1. (1 point) How big is the MAC address space? The IPv4 address space? The IPv6 address space?
2. (3 points) Consider RSA with $p = 17$ and $q = 13$.

   a. What are n and z?

   b. Let e be 11. Find d such that $ed = 1$ (mod z) and $d < z$.

   c. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding cipher text.

   Hint: To simplify the calculations, use the fact: $[(a \bmod n) \bullet (b \bmod n)] \bmod n = (a \cdot b) \bmod n$
3. (2 points)

   a. Suppose that the receiver receives a two-dimensional even parity matrix as follows. Is there an error in the matrix? If yes, which bit is in error?

1	0	1	0
0	1	0	1
1	1	1	0
0	0	1	1

   b. Now suppose the received parity matrix is the following. Can you detect if there are one or more bit errors in it? Can you *correct* the error(s)?

1	0	0	0
0	1	1	1
1	1	0	0
0	0	1	1

4. (4 points) Consider the 5-bit generator G = 11001 and the following D (the data bits). What is the value of R (the check bits) for each D?

   a. 1010101010

   b. 1001010101

   c. 0101101010

   d. 1010100000