# Assignment 5: Network Security and Link Layer[1]

Please submit your answers in a single PDF file.

1. (1 point) How big is the MAC address space? The IPv4 address space? The IPv6 address space?
2. (5 points) Consider RSA with $p = 17$ and $q = 13$.

   a. What are $n$ and $z$?

   b. Let $e$ be 77. Find $d$ such that $ed = 1 \pmod{z}$ and $d < z$.

   c. Encrypt the message $m = 4$ using the public 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, can you tell which bit(s) are wrong?

| | | | |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 |

   b. Now suppose the received parity matrix is the following. Suppose you know there is at most one bit error, can you *correct* the error?

| | | | |
|---|---|---|---|
| 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 |

[1] Some questions are adapted from textbooks "Computer Networking: A Top-Down Approach" by James Kurose & Keith Ross and resources provided with the textbooks. They can only be used by students who registered for this course. Reproduction outside of this course use is prohibited.

4. (3 points) Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair ($E_B$, $D_B$), and Alice has Bob's certificate that include Bob's public key $E_B$. But Alice does not have a public-private key pair. Alice and Bob (and the entire world) share the same hash function H(·).

    a. In this situation, is it possible to design a scheme so that Bob can check the integrity of the message received from Alice? If so, how should Alice send the message and how should Bob process the received message from Alice.

    b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, how should Alice send the message and how should Bob process the received message from Alice.

    c. Is it possible to design a scheme so that Bob can verify that Alice created the message? If so, how should Alice send the message and how should Bob process the received message from Alice?

5. (4 points) Consider the generator G = 10111 for CRC and the following D (the data bits). What is the value of R (the check bits) for each D? Show your calculation process.

    a. 1010101110

    b. 1001010101

    c. 0101101110

    d. 1010100000