The assignment #10 of the **ComNet** course

---

Q1)
a. What is the difference between confidentiality and end-point authentication? Why should both of them be preserved in a secure communication?
b. While the cipher text is sent on the channel and available to probably present intruders in the network, how do we guarantee the security?

Q2)
We wish to use a function to generate such a table similar to Table 8.1 for 16 4-bit blocks in a block cipher. The function is defined as

$$c(x) = (x_{10} \cdot 13 \mod 16)_2$$

Meanwhile, the function first converts the 4-bit blocks of the plain text to decimal. Then, multiplies it in 13 and gives the binary representation of its remainder by 16.
a. Prove that this function gives unique output cipher sequences (i.e. no two 4-bit inputs lead to a same output)
b. Find the outcoming table similar to Table 8.1.
c. Use Figure 8.5 for plain text of 10101101 and 4-bit chunks of data (instead of 8-bit) to obtain the cipher text. Assume there are 2 rounds in a loop and the scrambler inverts the incoming bits (e.g. maps 10010111 to 11101001). Also the input, the scrambler and the output are 8-bit blocks (again, instead of 64 !)
d. (Extra Mark) What number, in general, can we place instead of 13 to preserve the uniqueness of part a.?

Q3)
Remember section 8.3 about message integrity. Assume our messages can only be 8-digit numbers (each digit can be 0 to 9) and a hash function takes such an 8-digit number and obtains a 10-digit number $a_0a_1a_2\cdots a_9$ where

$$a_i = \text{number of } i\text{s in the input}$$

(e.g. 54756473 is mapped to 0001221200). If the 8-digit plain text is 33543612, what is the probability that an intruder compromises the message having its hash output?

Q4)

a. Recall the discussion about RSA (page 684, Public Key Encryption). Assume Alice encrypts her message by a public key $(77, 13)$ and Bob and Jake each use a private key of $(77, 37)$ and $(77, 97)$ for decryption, respectively. Show that if Alice encrypts the number 2 and sends it on the channel, then both Bob and Jake can decrypt it uniquely by calculating the details of RSA.

b. (Extra Mark) Show that condition 3 in page 685 is necessary for condition 4 (i.e. $4 \implies 3$).