**Homework #3**

Due date: 25 November 2020, by 11:59 pm.

**Notes**:

* For Question 1, you can use a Python module for arithmetic in GF(28).

1. Consider GF(28) used in AES with the irreducible polynomial p(x) = x8+x4+x3+x+1. You are expected to query the server “cryptlygos.pythonanywhere.com/poly/*<your\_id>*”, which will send you two binary polynomials a(x) and b(x) in GF(28). Polynomials are expressed as bit strings of their coefficients. For example, p(x) is expressed as '100011011'. You can use the Python code “**Q1\_student.py**” given in the assignment package to communicate with the server.
   1. You are expected to perform c(x) = a(x)×b(x) in GF(28) and return c(x) as bit string.
   2. You are expected to compute the multiplicative inverse of a(x) in GF(28) and return a-1(x).

**Exercise for Rainbow Tables (Non-credit question)**

Consider ten digests in the attached file “**rainbow\_table.py**”, each of which is the hash of a six-character password. Your mission is to find those passwords using the rainbow table given in the attached file “**rainbowtable.txt**”. Complete and submit the Python code in the file “**rainbow\_table.py**” such that it finds and prints out the ten passwords corresponding to the digests.