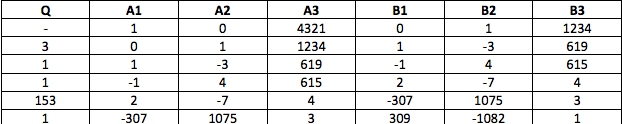
CS 4920/5920 Applied Cryptography Spring 2017

Problem 1 (tables are based off of the extended GCD() for the m.inverse)

Using the extended Euclidean algorithm, find the multiplicative inverse of

1. 1234 mod 4321

Multiplicative Inverse of 1234 mod 4321 = ‐1082

(‐1082 \* 1234) mod 4321 = (‐1 335 188) mod 4321 =

4321 \* (‐308) = ‐1330868  and   4321 \* (‐309) = ‐1335189

So  ‐309 is the greatest multiple less than 1330868, so 4321\*‐309 = ‐1335189 and

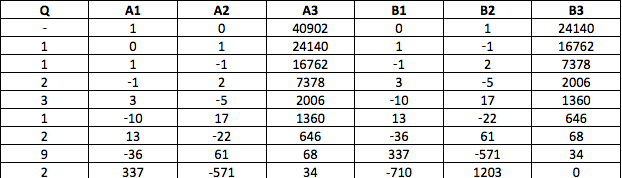
(‐1,335 188) – (‐1,335,189) =  1, showing it’s a multiplicative inverse.

To keep the multiplicative inverse confined to the set GF(4321), we can do clockwork arithmetic

saying 4321 – 1082 = 3239. Note that 3239 \* 1234 = 3996926 mod 4321 = 1, making 3239 the

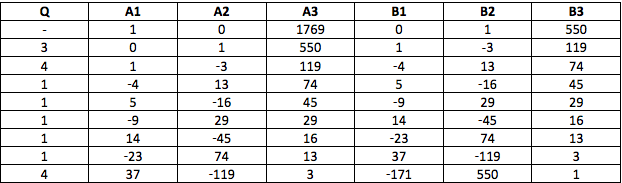
multiplicative inverse of 1234 in GF(4321).

1. 24140 mod 40902



Since b3 becomes 0, according the to the Extended GCD algorithm, there is no multiplicative 24140 in GF(40902). 40902 isn’t prime, so not all numbers necessary have multiplicative inverses.

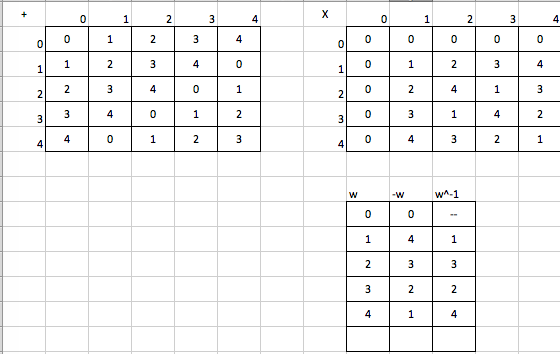
1. 550 mod 1769



B3 becomes 1, ending the algorithm, giving us a multiplicative inverse of 550 mod 1769 = 550. Note: 550 \* 550 = 302500 mod 1769 = 1

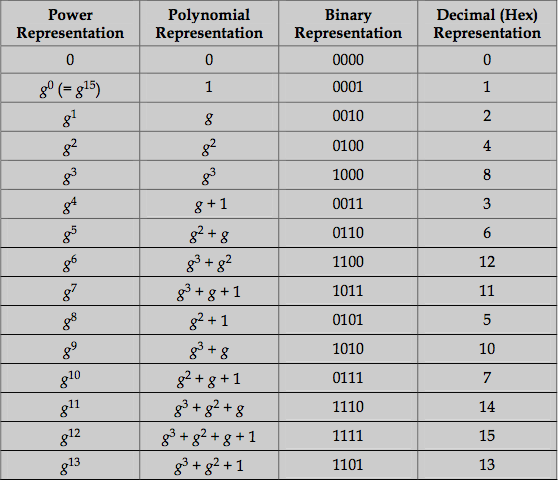
Problem 2:

Develop a set of tables similar to Table 5.1 in the textbook for GF(5).



Problem 3:

Develop a table similar to Table 5.5 in the textbook for GF(24) with m(x) = x4 + x + 1.



Problem 4.

Show the following:

a. Show that the matrix given here, with entries in GF(24), is the inverse of the matrix used

in the MixColumns step of S-AES.



To get the above result, observe that (x5 + x2 + x) mod (x4 + x + 1) = 0

b. Verify Equation (6.13) in Appendix 6A in the textbook. That is, show that ximod (x4+1) =xi mod 4

see that x4 mod (x4 + 1) = 1. This is because we can write:

x4 = [1 × (x4 + 1)] + addition operation is XOR. Then,

x8 mod (x4 + 1) = [x4 mod (x4 + 1)] × [x4 mod (x4 + 1)] = 1 × 1 = 1 So, for any positive integer a, x4a mod (x4 + 1) = 1. Now consider any integer i of

the form i = 4a + (i mod 4). Then, xi mod (x4 + 1) = [(x4a) × (xi mod 4)] mod (x4 + 1)

= [x4a mod (x4 + 1)] × [xi mod 4 mod (x4 + 1)] = xi mod 4 The same result can be demonstrated using long division.

Problem 5:

Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key

{01010101010101010101010101010101}:

a. Show the original contents of State, displayed as a 4 × 4 matrix.

b. Show the value of State after initial AddRoundKey.

c. Show the value of State after SubBytes.

d. Show the value of State after ShiftRows.

e. Show the value of State after MixColumns.

