USS: Introduction to mathematical cryptography
Tuesday July 26 problems

Today you should first practice encryption and decryption with our simple lattice-based cipher over the integers, and then finish the Monday July 25 problems if you did not finish them.

1. Consider the instance of our simple lattice-based cipher over the integers that has public key

$$\begin{gathered} x_0 = 8454204503, 3327341689, 1349786140, 2796047723, 7830075393, 6761697318, \\ 4923797967, 2282744485, 2700505680, 2574555543, 4536432818, 5853763387, \\ 6757138668, 8182482829, 8130443719, 6817659754, 2897777368, 2859480454, \\ 8404833136, 2986869839, 2216788527, 3241154823, 7130084136, 898925021, \\ 4384274941, 7507585242, 1921632240, 783868684, 6288094121, 6833000810, 6364802355, \\ 2855280111, 3534432240, 2013660441, 6553649254, 7582742811, 7411341636. \end{gathered}$$

   It is also public that to encrypt with this instance of fully homomorphic encryption, you should choose the encryption noise r such that

$$-63 \le r \le 63.$$

   (a) Use this public key to give two encryptions of $m = 0$.

   (b) Use this public key to give two encryptions of $m = 1$.

   If you want to check your work, the private key is $p = 3011$.

2. Consider the instance of our simple lattice-based cipher over the integers that has private key $p = 3011$. Use this private key to decrypt the following ciphertexts.

   (a) $c = 4,214,470,613$

   (b) $c = 865,735,839$

   (c) $c = -123,001,310$

   (d) $c = -3,780,664,792$