USS: Introduction to mathematical cryptography
Friday July 29 problems

1. Use the Regev LWE pairs with $q = 29$

$$((18, 23, 6, 12, 7), 2),$$
$$((8, 7, 17, 21, 14), 12),$$
$$((19, 11, 26, 6, 20), 11),$$
$$((15, 22, 19, 26, 16), 12),$$
$$((19, 28, 22, 14, 8), 8),$$
$$((12, 15, 8, 13, 20), 16),$$
$$((8, 28, 13, 6, 20), 14),$$
$$((7, 21, 22, 24, 23), 20)$$

   to encrypt

   (a) $x = 0$,

   (b) $x = 1$.

2. Suppose that you have published a set of Regev LWE pairs generated with $q = 29$ and $\vec{s} = (15, 13, 22, 15, 7)$. You receive the ciphertext pair

$$((2, 28, 20, 24, 21), 23).$$

   What was the bit sent to you?