Math 4981 Spring 2021
Cryptography HW 13 Solutions
Due Thursday, April 22

1. Let $f(x) = 2x^2 + x + 1$ and $g(x) = 3x^2 - 2$ in the ring $\mathbb{Z}/5\mathbb{Z}[x]/\langle x^3 + x\rangle$. Compute $f + g$ and fg.

   Solution:

$$\begin{aligned} f + g &= 5x^2 + x - 1 = x - 1 \\ fg &= (2x^2 + x + 1)(3x^2 - 2) = 6x^4 - 4x^2 + 3x^3 - 2x + 3x^2 - 2 \\ &= 4x^2 - 4x^2 - 3x - 2x + 3x^2 - 2 = 3x^2 - 2. \end{aligned}$$

2. Let $f(x) = 2x^2 - x$ and $g(x) = x^3 + 4x + 5$ in $\mathbb{Z}/7\mathbb{Z}[x]/\langle x^4 + 1\rangle$. Compute $f + g$ and fg.

   Solution:

$$\begin{aligned} f + g &= x^3 + 2x^2 + 3x + 5 \\ fg &= (2x^2 - x)(x^3 + 4x + 5) = 2x^5 - x^4 + 8x^3 - 4x^2 + 10x^2 - 5x \\ &= -2x + 1 + x^3 - 4x^2 + 3x^2 - 5x = x^3 - x^2 + 1. \end{aligned}$$

For the remaining problems, we will take $n = 2^3, q = 17, R = \mathbb{Z}/17\mathbb{Z}[x]/\langle x^8 + 1\rangle$, and $a = x^7 + 3x^5 - x^2$.

3. Alice chooses her private key as $s_0 = x^6 + 1, s_1 = x^4 - x^2$. What is her public key?

   Solution: We have

$$\begin{aligned} b = s_1 a + s_0 &= x^{11} + 2x^9 - 3x^7 + x^4 + 1 \\ &\equiv -x^3 - 2x - 3x^7 + x^4 + 1 \\ &\equiv -3x^7 + x^4 - x^3 - 2x + 1 \end{aligned}$$

4. Suppose Bob receives $b = x^3 + x^2 - x + 5$ from Alice. He chooses error terms $e_0 = x^6 + x, e_1 = -x^5 + x^2, e_2 = x^4 - x^3$. What is the shared secret μ?

5. What is the ciphertext c that Bob sends to Alice?

   Solution:

Bob computes

$$\begin{aligned}
u &= e_0 a + e_1 = (x^6 + x)(x^7 + 3x^5 - x^2) + x^2 - x^5 \\
&= x^{13} + 3x^{11} + 3x^6 - x^5 - x^3 + x^2 \\
&= -x^5 - 3x^3 + 3x^6 - x^5 - x^3 + x^2 \\
&= 3x^6 - 2x^5 - 4x^3 + x^2 \\
v &= e_0 b + e_2 = (x^6 + x)(x^3 + x^2 - x + 5) + x^4 - x^3 \\
&= x^9 + x^8 - x^7 + 5x^6 + 2x^4 - x^2 + 5x \\
&= -x - 1 - x^7 + 5x^6 + 2x^4 - x^2 + 5x \\
&= -x^7 + 5x^6 + 2x^4 - x^2 + 4x - 1
\end{aligned}$$

To compute $\lfloor v \rceil_2$ we need to find the four intervals I_0, I_1', I_0', I_1. We have

$$\begin{aligned}
I_0 &= [0, 17/4) = [0, 4] \\
I_1' &= [17/4, 17/2) = [5, 8] \\
I_0' &= [17/2, 51/4) = [9, 12] \\
I_1 &= [51/4, 17) = [13, 16] = [-4, -1].
\end{aligned}$$

Then we have

$$\begin{aligned}
\mu = \lfloor v \rceil_2 &= (0, 1, 0, 0, 0, 0, 0, 0) \\
\langle v \rangle_2 &= (1, 1, 0, 0, 0, 1, 0, 1)
\end{aligned}$$

and we sent Alice

$$c = (u, \langle v_2 \rangle) = (3x^6 - 2x^5 - 4x^3 + x^2, (1, 1, 0, 0, 0, 1, 0, 1)).$$

6. Suppose Alice, still using the same s_0, s_1, receives the encapsulation

$$(u, v') = (5x^7 - 6x^5 - 7x^3 + x^2 - 8x, (10011101)).$$

What does she compute μ to be?

Solution: First Alice computes

$$\begin{aligned}
w &= u \cdot s_1 \\
&= -x^7 + x^6 - x^5 - x^4 + 3x^3 - 6x
\end{aligned}$$

We still have

$$\begin{aligned}
I_0 &= [0, 17/4) = [0, 4] \\
I_1' &= [17/4, 17/2) = [5, 8] \\
I_0' &= [17/2, 51/4) = [9, 12] \\
I_1 &= [51/4, 17) = [13, 16] = [-4, -1].
\end{aligned}$$

and thus

$$\begin{aligned}
I_0 + E &= [-17/8, 3 \cdot 17/8) = [-2, 6] \\
I_1' + E &= [17/8, 5 \cdot 17/8) = [3, 10] \\
I_0' + E &= [3 \cdot 17/8, 7 \cdot 17/8) = [7, 14] \\
I_1 + E &= [5 \cdot 17/8, 9 \cdot 17/8] = [11, 19] = [-6, 2].
\end{aligned}$$

Thus

$$\begin{aligned}
\mathrm{rec}(w, v') &= (\mathrm{rec}(-1, 1), \mathrm{rec}(1, 0), \mathrm{rec}(-1, 0), \mathrm{rec}(-1, 1), \mathrm{rec}(3, 1), \mathrm{rec}(0, 1), \mathrm{rec}(-6, 0), \mathrm{rec}(0, 1)) \\
&= (0, 0, 0, 0, 1, 0, 1, 0).
\end{aligned}$$