# Math 4981 Spring 2021
# Cryptography HW 14 Solutions
# Due Thursday, April 29

Feel free to use software like Mathematica to do the polynomial computations. (In Mathematica the command you want is `PolynomialMod[f, {q,x^N+1}]`, but beware that Mathematica will give you the coefficient 16 when you really want $-1$).

1. Let $R = \mathbb{Z}[x]$ and let $S = \mathbb{Z}$. Define the evaluation map $E_a : R \to S$ by the rule $E_a(f) = f(a)$. Prove that $E_a$ is a homomorphism.

Now let $N = 4, q = 17, R_q = \mathbb{Z}/17\mathbb{Z}[x]/(x^4 + 1)$. Suppose Alice and Bob have the shared symmetric key $s(x) = x^3 + x + 1$.

2. Alice chooses $a(x) = 4x^2 + 3x - 8$ and $e(x) = x - 1$. She wants to encrypt the message 1001. What ciphertext does she send?

   **Solution:**

$$\begin{aligned} c_1(x) &= -a(x) = -4x^2 - 3x + 8 \\ c_0(x) &= a(x)s(x) + 2e(x) + m(x) \\ &= (4x^2 + 3x - 8)(x^3 + x + 1) + 2x - 2 + x^3 + x \\ &= -3x^3 + 7x^2 - 7x + 5. \end{aligned}$$

   So Alice sends

$$(-3x^3 + 7x^2 - 7x + 5, -4x^2 - 3x + 8).$$

3. On a separate occasion, Bob receives the ciphertext

$$(7x^3 - 4x^2 + 5x + 5, -2x^3 + 3x - 5).$$

   What is the message?

   **Solution:** Bob computes

$$\begin{aligned} c_0(x) + c_1(x)s(x) &= 7x^3 - 4x^2 + 5x + 5 + (-2x^3 + 3x - 5)(x^3 + x + 1) \\ &= x^2 + 3x - 1. \end{aligned}$$

   Reducing mod 2 gives $x^2 + x + 1$ for a message of $(0, 1, 1, 1)$.

4. Suppose we are using the Somewhat Homomorphic Encryption setup, and Google receives the two messages

$$\begin{aligned}\mathbf{c} &= (2x^3 + 7x^2 - 8x - 2, x^2 - 5x - 2)\\ &= (2x^3 + 7x^2 - 8x - 2) + (x^2 - 5x - 2)v\\ \mathbf{c}' &= (3x^3 + 8x^2 - 7x + 7, -7x^3 + 6x^2 - 3x + 1)\\ &= (3x^3 + 8x^2 - 7x + 7) + (-7x^3 + 6x^2 - 3x + 1)v.\end{aligned}$$

What is $\mathbf{c} + \mathbf{c}'$? What is $\mathbf{c} \times \mathbf{c}'$?

**Solution:**

$$\begin{aligned}\mathbf{c} + \mathbf{c}' &= (5x^3 - 2x^2 + 2x + 5, -7x^3 + 7x^2 - 8x - 1)\\ &= (5x^3 - 2x^2 + 2x + 5) + (-7x^3 + 7x^2 - 8x - 1)v\\ \mathbf{c} \times \mathbf{c}' &= (-3x^3 - 2x^2 + 6x + 2) + (-4x^3 + 8x^2 - 6x + 1)v + (-2x^3 + 4x^2 + 8x + 8)v^2.\end{aligned}$$

5. Alice, using the SHE scheme, gets back the ciphertext

$$\mathbf{c} = (x^3 + 3x + 8, -7x^3 + 3x^2 + 5x - 2, 8x^3 - 8x^2 + 4x).$$

What does she decrypt the message to be?

**Solution:** We compute

$$\begin{aligned}\mathbf{s} &= (1, s, s^2) = (1, x^3 + x + 1, 2x^3 + 2x - 1)\\ \langle \mathbf{c}, \mathbf{s} \rangle &= (x^3 + 3x + 8) \cdot 1 + (-7x^3 + 3x^2 + 5x - 2) \cdot (x^3 + x + 1) + (8x^3 - 8x^2 + 4x) \cdot (2x^3 + 2x - 1)\\ &= 5x^3 - 2x^2 - 2x + 1.\end{aligned}$$

Reducing mod 2 gives us $x^3 + 1$ so the message is $(1, 0, 0, 1)$.