Math 401 Fall 2019
Cryptology HW 11
Due Tuesday, December 3

This homework is optional, and will replace your lowest homework score.

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?

3. On a separate occasion, Bob receives the ciphertext

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

   What is the message?

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 $\mathbf{c} \times \mathbf{c}'$?

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?