

Math 4981 Spring 2021  
Cryptography HW 13  
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  $fg$ .
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  $fg$ .

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?
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  $\mu$ ?
5. What is the ciphertext  $c$  that Bob sends to Alice?
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  $\mu$  to be?