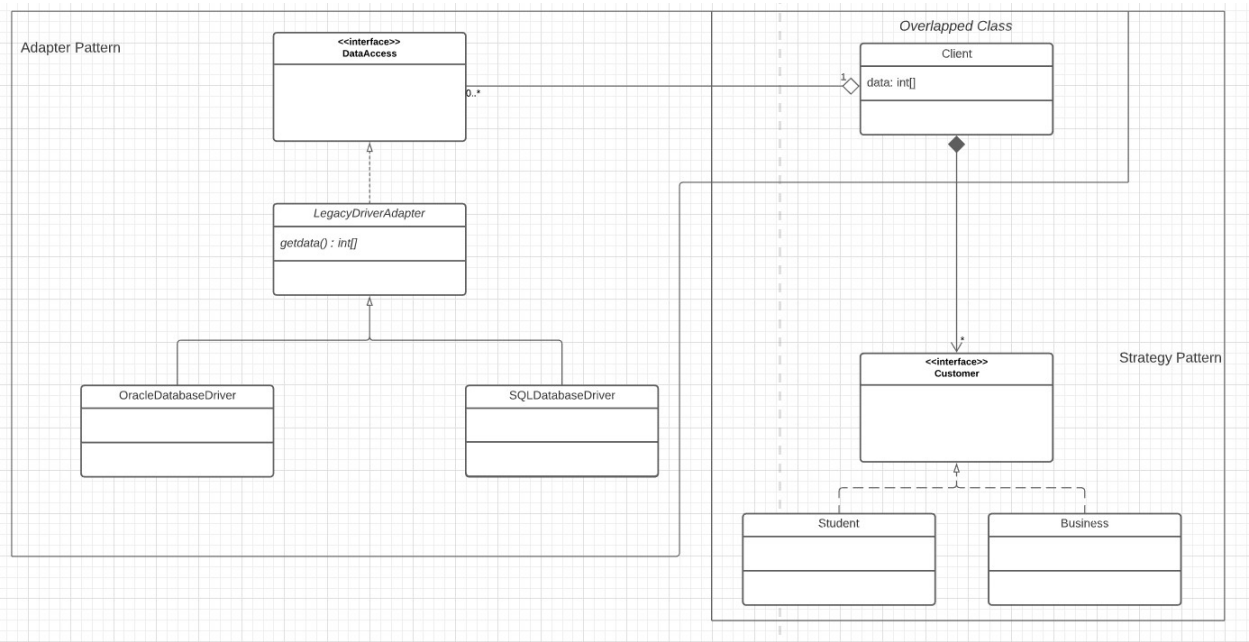
ESOF HW 4

Kyle Rust

Due October 15, 2020

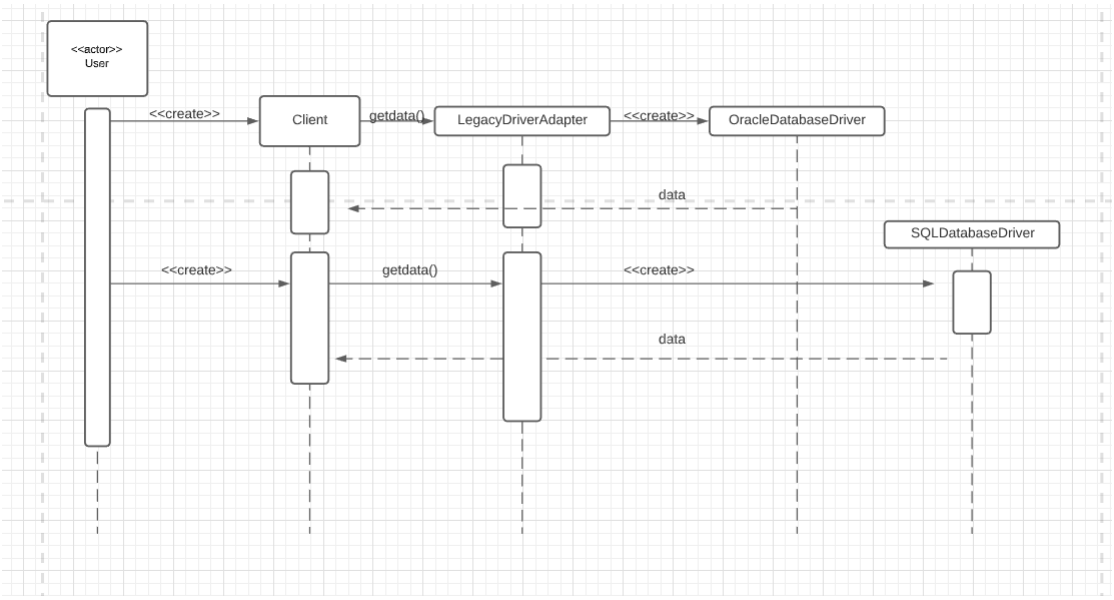
1 Exercise 1

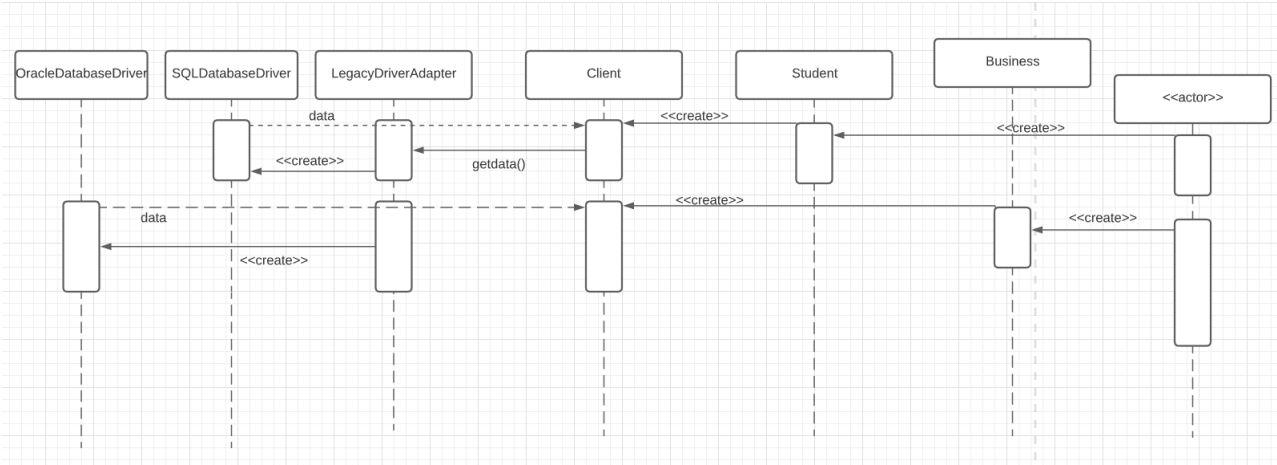
1.1



This system is a rough outline of a database access system. There are two different access levels between students and businesses. The Client class overlap between the Strategy Pattern and the Adapter Pattern

1.2





2 Exercise 2

2.1

Mary was subject a man-in-the-middle attack. Man-in-the-middle attacks occur when the attacker secretly relays and possibly alters the communication

between two parties who think they are communicating directly. Walsingham would collect the letters going between Mary and Babington. Walsingham would break the seal and copy the contents of the letter before, perfectly resealing the letter, and sending it on to the intended recipient.

2.2

The use of the Diffie-Hallman Algorithm would have increased the security of Mary and Babington's correspondence. Without access each person's secret key, Walsingham could not have deciphered what each person was saying. He could have intercepted the public communication, but could not have deciphered what was being said.