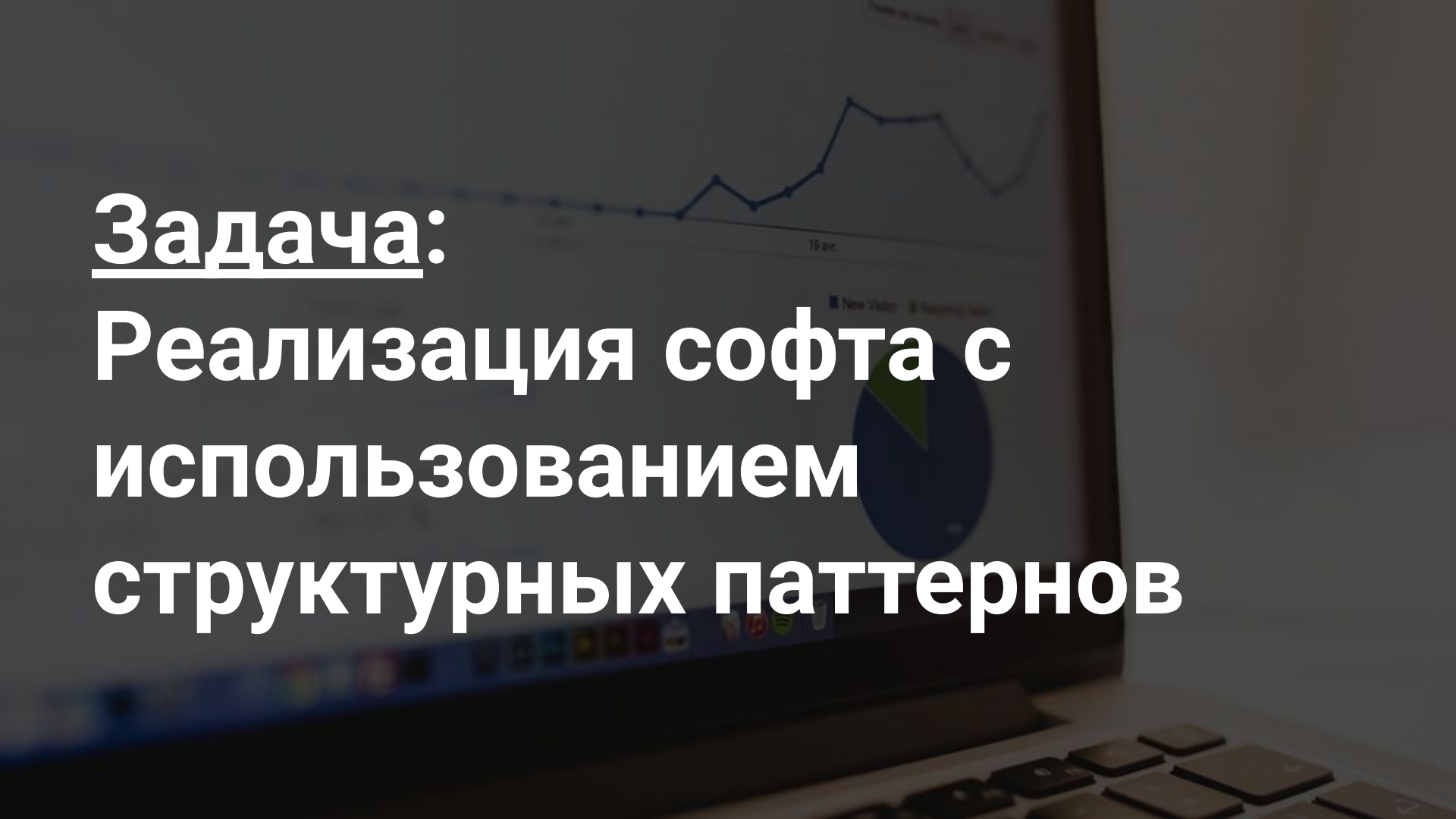
ДЗ структурные паттерны

Bridge, Proxy



Задача:
Реализация софта с использованием структурных паттернов

Необходимые сущности

1. Клиент
2. Диалог
3. SecurityProxyDialog

Класс Диалог содержит двух клиентов и осуществляет обмен данными (например цифры, буквы, слова) между соответствующими клиентами. Но диалог поддерживает алгоритм шифрования передаваемых данных, осуществляемым SecurityProxyDialog
См: SOLID

SecurityProxy Dialog

Данный класс поддерживает нетривиальную реализацию, поэтому требуется разделение абстракции от реализации

Реализация будет описана на следующих слайдах

Суть Алгоритма шифрования RSA

1. ***Создание ключей шифрования:***
   Выбрать любые 2 числа из предложенного списка
   Вычислить 2 произведения:
   a. *Произведение этих 2х чисел(A)*
   b. *Произведение этих чисел, но уменьшенных на единицу(B)*

   подобрать 3е число(C), такое что, при делении числа B на него остаток от деления будет > 0

   Посчитать последнее четвертое число по следующей формуле:

   *D = (k * B + 1) / C, где k - абсолютное любое число*

2. Составляются 2 ключа(ключом является ПАРА чисел)

- *Открытый: (C, A)*
- *Закрытый: (D, A)*

Закрытый ключ храниться у отправителя сообщения, а открытый у получателя

- *Для того, чтобы зашифровать сообщение нужно содержимое сообщение возвести в степень C и результат этого поделить с остатком на число A Данное число будет являться зашифрованным сообщением.*
- *Для того, чтобы расшифровать нужно содержимое полученного сообщения*
- *возвести в степень D и результат этого поделить с остатком на число A Данное число будет являться расшифрованным сообщением*

- *В случае, если диалог предназначен исключено для передачи цифр(например банковская система), то шифровать цифры можно напрямую*
- *В случае передачи текста, то необходимо у каждой буквы брать её код, и шифровать это значение(то есть, при передачи более одного символа, результатом шифрования будет вектор цифр)*