**Цель:**  
Сформировать публичный и скрытый ключ на сервере, зашифровать, с помощью полученных публичных ключей, сообщение клиента, передать сообщение серверу и расшифровать с помощью скрытого ключа.  
  
**Пункты выполнения:**  
1. Генерация на сервере пары публичных ключей (выбрать простые P и Q, которые должны быть не равны);  
2. Вычисление на сервере N = P \* Q; (N должно быть больше любой Mi)

3. Вычисление на сервере F = (P-1) \* (Q-1);  
4. Определение на сервере случайного числа D, такого что D < F и D,F – взаимно простые.  
5. Вычисление на сервере скрытого ключа E, такого что (E \* D) mod F = 1

6. Отправка публичных ключей клиенту.

7. Определение сообщений Mi клиента.

8. Шифровка клиентом сообщений по следующей формуле : Ci = (Mi) D mod N;

9. Отправка шифра серверу.

10. Расшифровка шифра Ci сервером с помощью скрытого ключа по следующей формуле: Mi = (Ci) E mod N  
  
**Вывод:**  
Сообщения определяемые клиентом зашифровываются, с помощью полученных от сервера публичных ключей N и D, и отправляются на сервер. С помощью скрытого ключа E сервер успешно расшифровывает полученный шифр.

**Ссылка:**

https://github.com/Maximovix/Lab4\_ZI