

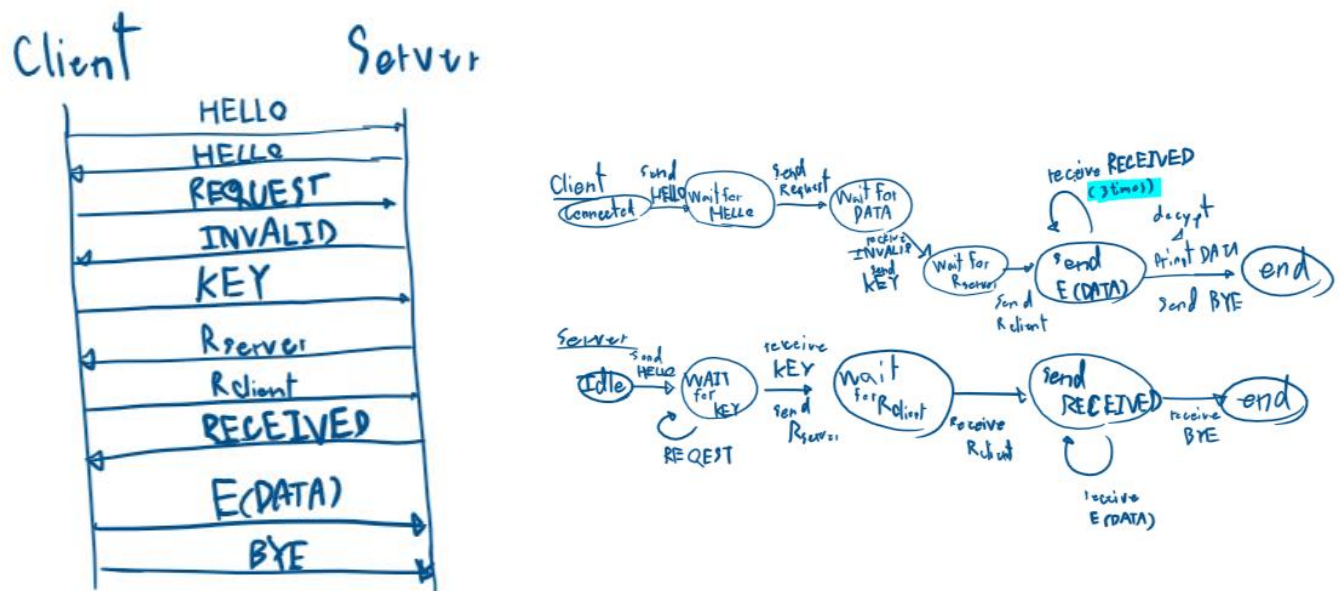
Socket Programming Part2 Report

สมาชิกภายในกลุ่ม

6210110040 นายจตุพร วัฒนสิน

6210110297 นายรชานนท์ กองชาย

Diagrams and Explanation

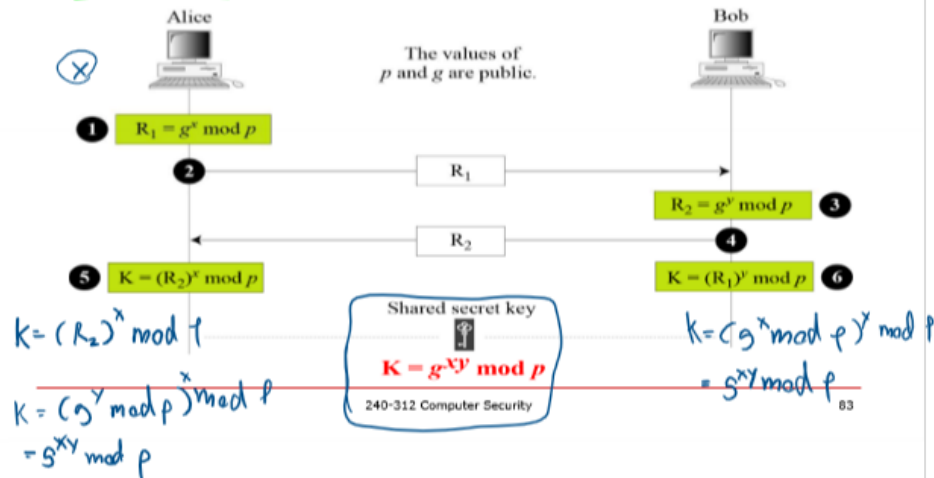


Client เริ่มติดต่อกับ Server โดยการส่ง HELLO และเมื่อ Server ส่ง HELLO กลับมา Client ก็จะลองส่งข้อมูลตรงๆ ไป REQUEST ถ้าได้รับ INVALID กลับมาก็จะส่งข้อมูลกลับไปเป็น KEY เพื่อขอ key ในการติดต่อเข้าใช้งาน Server ก็จะตอบ Rserver กลับมาและทาง Client จะนำไปคำนวณเพื่อนำไปหาค่า Key ที่ใช้ในการสื่อสาร และส่ง Rclient กลับไปให้ Server เพื่อให้อีกฝั่งคำนวณ Key เช่นกัน

ซึ่งมีหลักการคำนวณดังนี้

No third party

Diffie-Hellman key agreement



หลังจากนั้น Server จะทำการส่ง RECEIVED กลับไปเพื่อบอกว่า Key สมบูรณ์พร้อมส่งค่าแล้ว เมื่อ Client ได้รับข้อมูลดังกล่าวก็จะเริ่มส่งข้อมูลได้ โดยภายใน code จะกำหนดให้ส่งข้อมูลเพียง 3 รอบ เข้ารหัสโดย Key และทาง Server จะรับข้อความเข้ารหัสและถอดรหัสออกมาได้ถูกต้อง และจบการสื่อสารโดยที่ Client ส่งข้อความ BYE

Code Result

```

TERMINAL
key sent, wait for variable
begin case 2
request for Rserver
begin case 2
key = 5
sent 0
sent 3
sent 2
exit
Connection closed
PS D:\WORKS\year3\S2\240-311\Assignments\git_socket_assignment>

PS D:\WORKS\year3\S2\240-311\Assignments\git_socket_assignment> node key-server.js
Server listening on 127.0.0.1:6969
6
wrong method
prepare Rserver
sent Rserver: 6
key = 5
value = 5
value = 6
value = 7
exit

```

ข้อมูล Client: 5 6 7 ส่ง: 0 3 2

Server แปล: 5 6 7 รับได้: 0 3 2