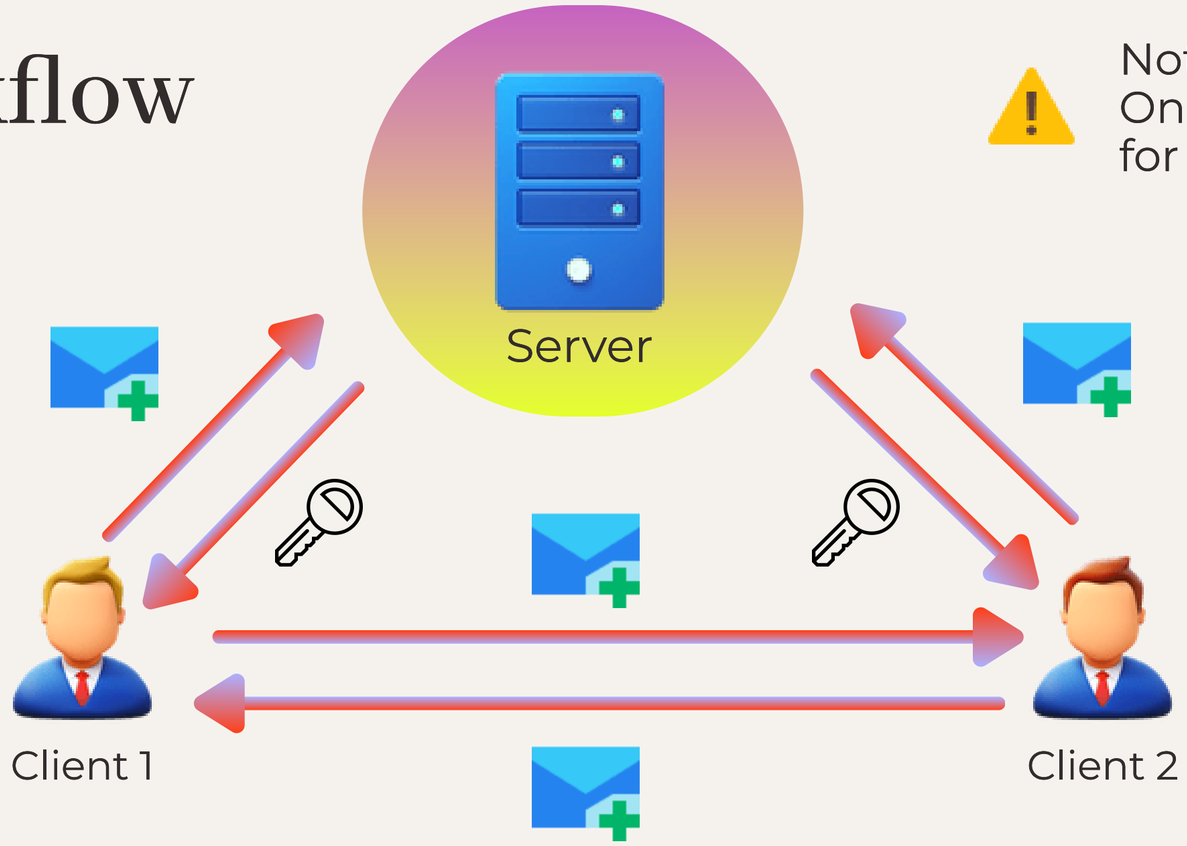
Simulating End-to-End Encryption and Peer-to-Peer Communication with OpenSSL and Python

Submitted by
Moordhan Songade
Sushat Kumar Pal

Introduction

- In this project, we have tried to simulate the concepts of End-to-End Encryption (E2EE) using both Public Key and Private Key encryption methods.
- By utilizing OpenSSL and Python, we simulate this encryption process and explore Peer-to-Peer (P2P) communication dynamics through Socket Programming.
- This endeavor underscores the fusion of security and connectivity in modern digital interactions.

Setup & Workflow

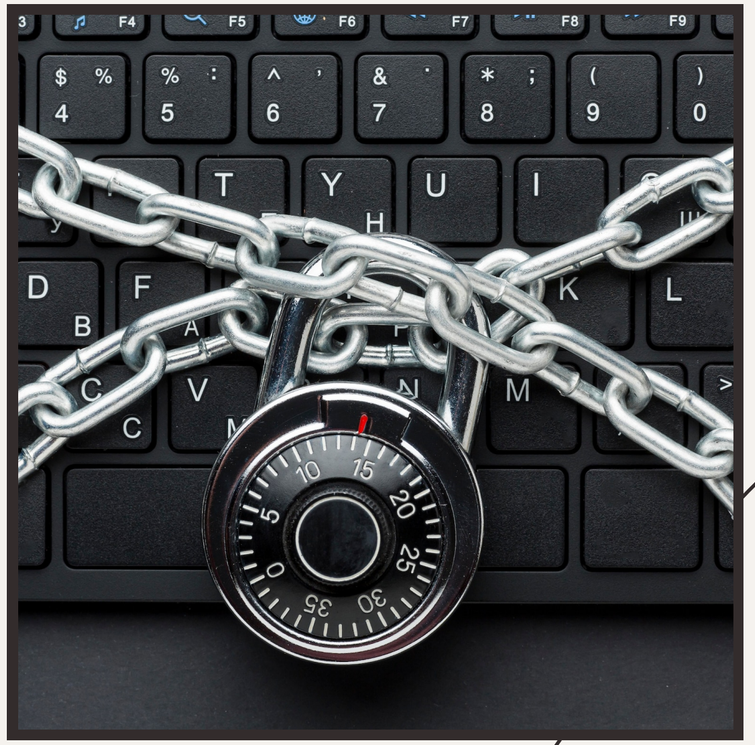


Note:
Only for public key encryption
for extracting the public key

- This is completely a command-line based project with the code written in Python
- Two independent client communicating with each other.
- The option will be provided to the client, whether to communicate through public-key or private-key encryption.
- If time permits, we may also use Snort for intrusion detection & digital signature for verification for each client.

Take-aways & Scope of improvement

- In our model, we used different cryptographic techniques, which are used to model secure communication in wide-variety of apps like Whatsapp, etc.
- In future work, we can also introduce more complex mechanisms like TLS, handshakes, etc. to improve the reliability as well as the security.



Thanks!