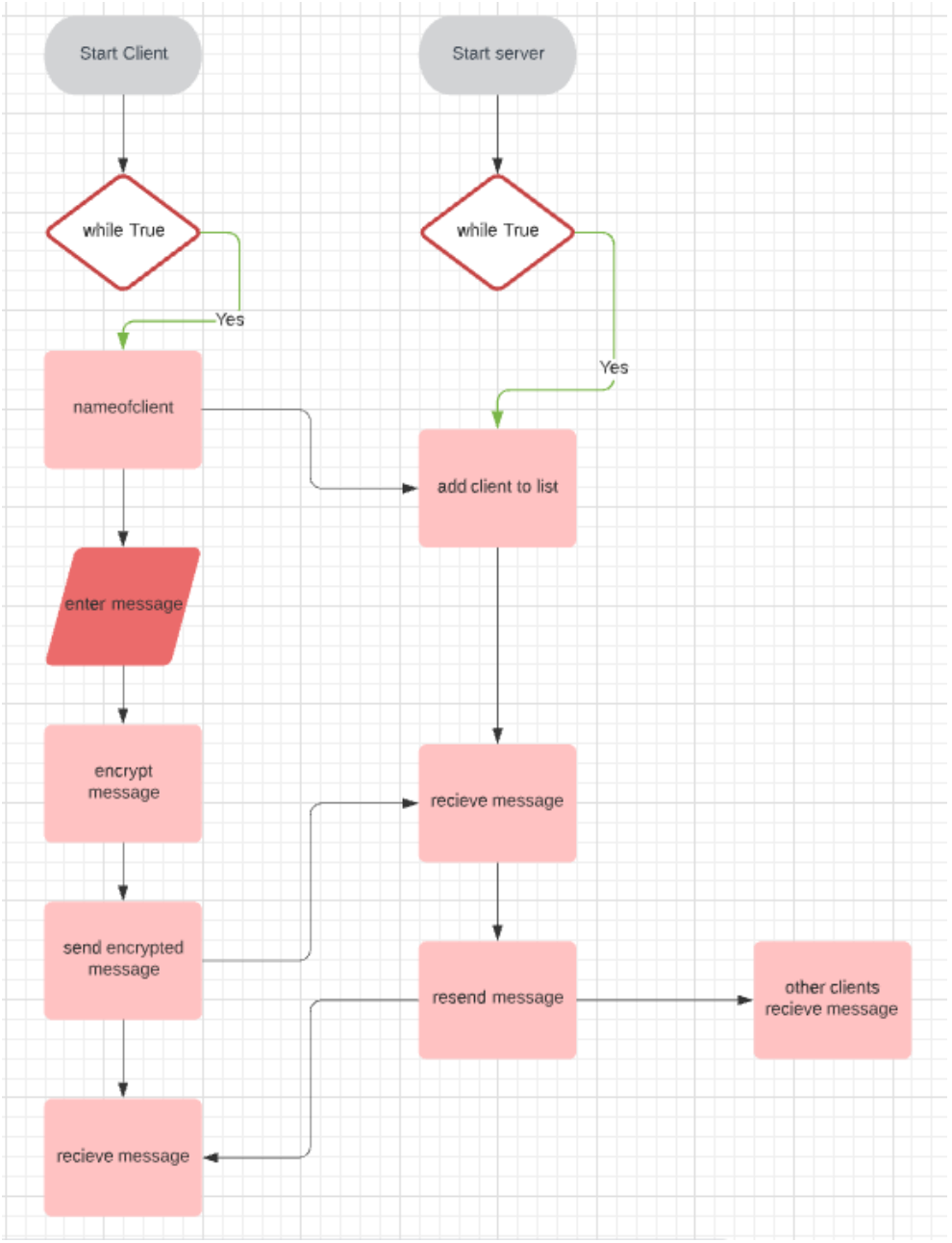
Projekt Aplikovaná kryptografie

Šifrovaná komunikace mezi dvěma uživateli Vytvořte program, který bude schopen provádět šifrovanou komunikaci mezi dvěma uživateli. Zprávy budou zašifrované pomocí symetrické kryptografie a pro výměnu klíče u symetrické kryptografii využijte asymetrickou kryptografii. Veřejné klíče uživatelů budou opatřeny certifikáty, které se budou ověřovat u certifikační autority. Každá dílčí činnost programu bude vypsána do konzole.

1. Vývojový diagram programu



2. Popis spuštění
    a. Při práci na projektu jsme používali localhost, takže stačilo spustit skript a server mohl běžet.
    b. Tuto možnost jsme vylepšili o server od společnosti linode, aby mohlo dojít i připojení z jiných zařízení obsahující příslušný skript clienta.
    c. Nejdříve si stáhneme program PuTTY, pomocí kterého se připojíme na server.
    d. Zde se nasměrujeme do složky se skriptem server.py
    e. Vše funguje tak, že se na serveru spustí skript server.py
    f. Dále jsme vytvořili dva uživatele, Boba a Alici, kteří mají každý vlastní složku (simulace vlastního zařízení) a připojí se pomocí skriptu client.py
    g. Pokud máme příslušný skript, můžeme se na server připojit z libovolného zařízení.
    h. Každý klient má už ve složce předem vygenerovaný soukromý klíč a certifikát proti komunikující strany, které byly vytvořeny pomocí skriptu na vygenerování RSA klíče a podepsání veřejného klíče, který je manuálně upraven pokud chceme generovat další certifikáty.
    i. všechny dílčí činosti budou vypsaný u klienta alice a na serveru

3. Fungování programu
    a. Po spuštění server.py náš server začne poslouchat a čekat na připojení
    b. Po spuštění clienta server přidá klienta do listu, odkud pak následně bere adresy pro odesílání zpráv.
    c. Dále vše pokračuje tak, že například klient A chce poslat zprávu klientovi B
    d. Klient A zadá zprávu do konzole, poté se tato zpráva musí zašifrovat.
    e. Šifrování probíhá tak, že pomocí symetrické kryptografie AES se zpráva zašifruje tajným klíčem.
    f. Z tajného klíče se vytvoří hash.
    g. Tento hash je zašifrován pomocí asymetrické kryptografie RSA.
    h. Aby jsme mohli RSA použít, potřebujeme ale nejdříve pár veřejného a soukromého klíče. Ty jsou uloženy v souboru každého klienta.
    i. Z certifikátu klienta B tedy dostaneme veřejný klíč, pomocí kterého zašifrujeme otisk tajného klíče.
    j. Na server pošleme zašifrovanou zprávu (AES) a zašifrovaný otisk (RSA)
    k. Server tyto údaje přepošle klientovi B, kde jsou tyto údaje rozparsovány a vloženy do dešifrátoru.
    l. Následně se klientovy B zobrazí dešifrovaná zpráva
4. Použité externí knihovny a jejich verze
    a. verze pythonu 3.9.9
    b. cryptography 36.0.0
        i. tato knihovna obsahuje vše co jsme potřebovali
    c. zbylé knihovny jsou built-in
        i. socket
        ii. threading
        iii. hashlib
        iv. os