End to End Project Encryption

عمل الطالبات: ريم يحيى – زهرة المزجاجي

فكرة المشروع:

تشفير End to End هو نظام اتصال خاص يسمح فقط للمستخدمين الذين يتواصلون بالمشاركة فيه. وبالتالي، لا يمكن لأي شخص، بما في ذلك مزود نظام الاتصال، مزودي الهاتف، مزودي الإنترنت أو العملاء الضارين، الوصول إلى المفاتيح تشفيري اللازمة للتحدث. يهدف التشفير من End to End إلى منع قراءة البيانات أو تعديلها بشكل سري، باستثناء المرسل الحقيقي والمستلم (أو المستلمين). يتم تشفير الرسائل من قبل المرسل، ولكن الجهة الثالثة ليس لديها وسيلة لفك تشفيرها، وتخزنها مشفرة.

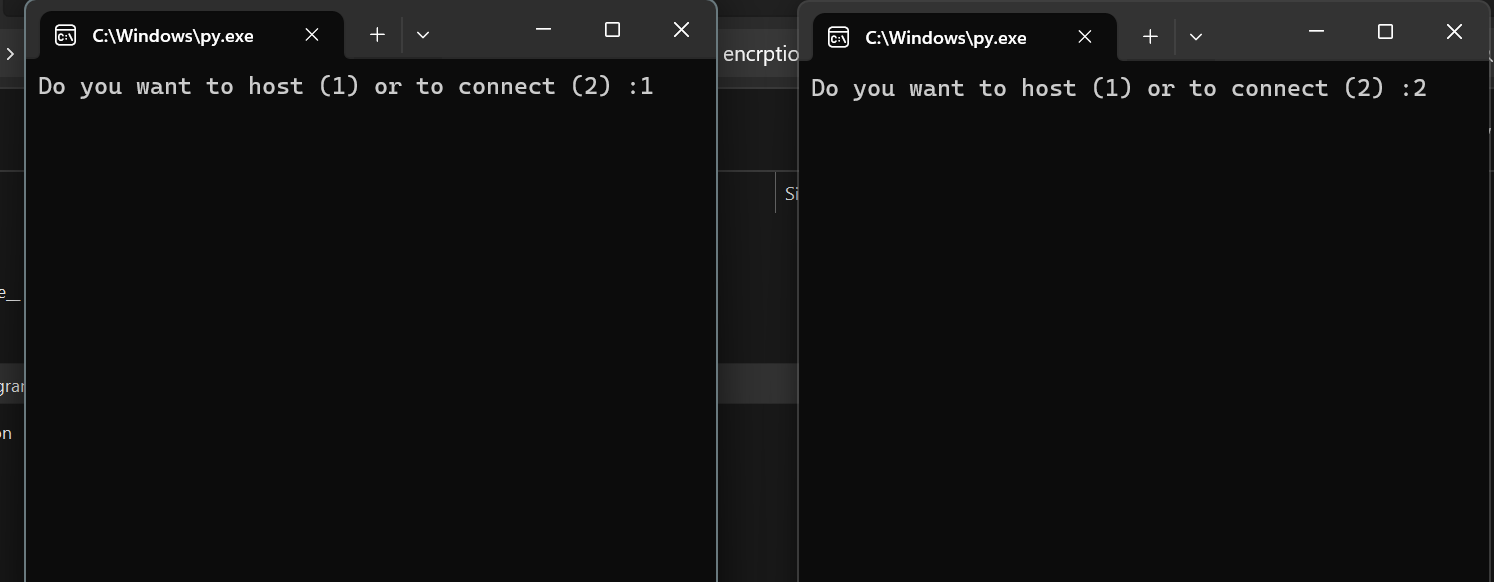
المكاتب المستخدمة في بناء المشروع:

تم استخدام أربع مكاتب في هذا المشروع وهي:

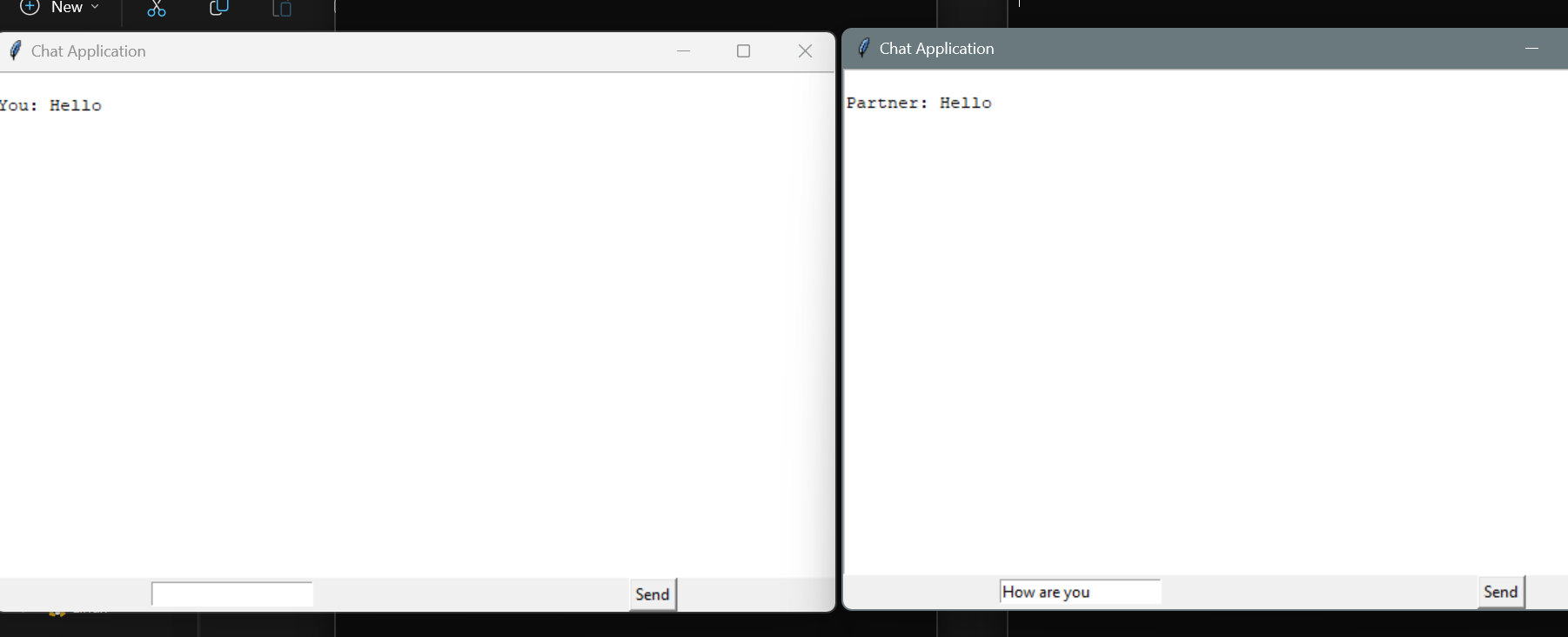
1. :RSAوهي احد خوارزميات التشفير الغير متناظرة والتي لم يتم كسرها الى يومنا هذا وهي المكتبة الرئيسة في أداء التشفير في البرنامج.
2. Socket: وهي المكتبة التي ادة الى الاتصال بين الأطراف عبر ال IP address.
3. Threading:وهي المكتبة التي سمحة بالتواصل بين الأطراف.
4. Tkinter: وهي المكتبة التي استخدمه للواجهات .GUI

أسس المشروع عبر if condition التي تسأل المستخدم لإدخال 1 ل host و 2 ل connect ويتم الربط عبر مكتبة socket ثم يتم استخدام مكتبة ال RSA لتشفير الرسائل التي سيتم ارسالها عبر مكتبة ال threading.

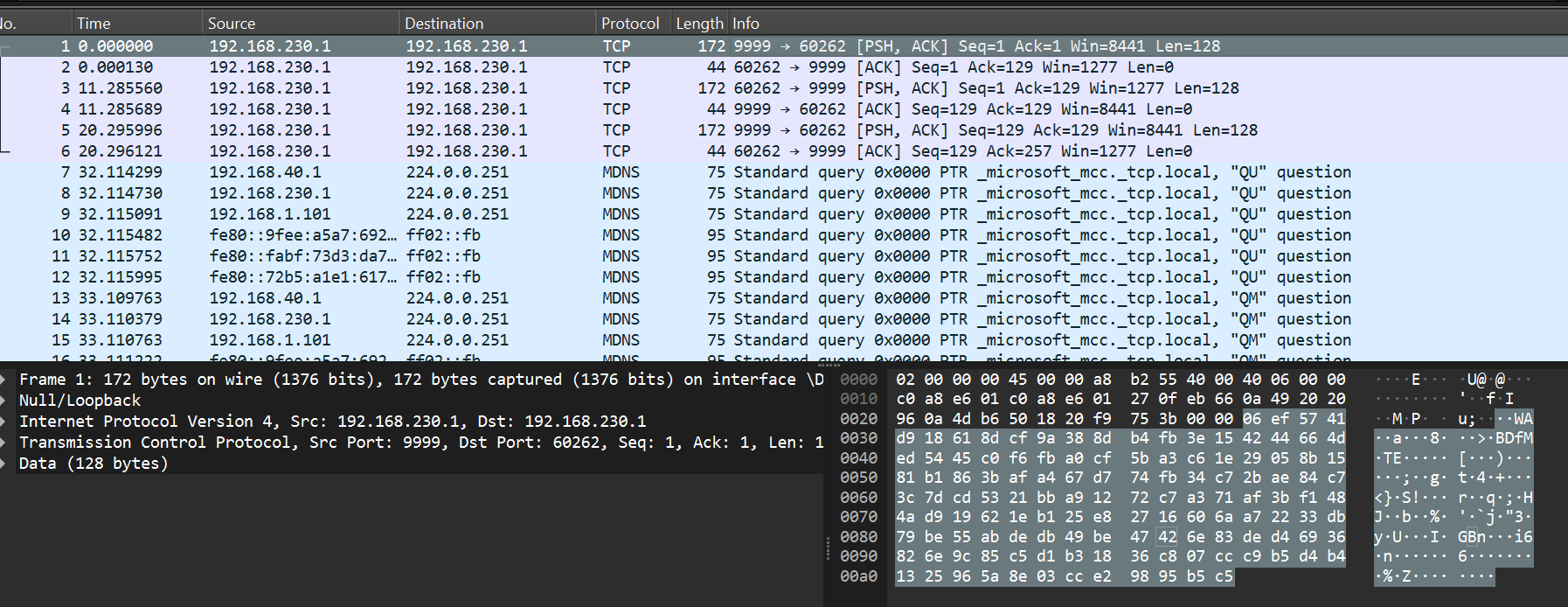
آلية عمل الشروع:



يقوم المشروع بسأل المستخدم اذا كان يريد طلب الاتصال أدخل 1 , وإذا أراد الاتصال أدخل 2.



بعد ان يتم الاتصال تنبثق نافذة ليتم التراسل بين الطرفين.



عندما يتم مراقبة البرنامج ستظهر الرسائل مشفرة ولا يستطيع فك التشفير حتى الشركة المصنعة للبرنامج.