نظرة عامة على الحل

يقدم هذا الحل نظام اتصال أساسي وآمن بين العميل والخادم باستخدام لغة البرمجة Python، حيث يدعم النظام ثلاثة أوضاع للتواصل: النص العادي، التشفير المتماثل، والتشفير غير المتماثل. يعتمد التنفيذ على مكتبات متقدمة مثل cryptography، SSL، وsockets لضمان عمليات تواصل مرنة وآمنة. فيما يلي تفصيل لأبرز مكونات النظام:

1. البنية العامة للنظام

تم بناء النظام وفق المكونات الأساسية التالية:

الـClass الأساسي: BasicMessenger

* يمثل الأساس الذي يعتمد عليه كل من العميل والخادم.
* يوفر أساليب مشتركة لإعداد الاتصال وتنفيذ التشفير.
* يدعم التشفير المتماثل باستخدام Fernet والتشفير غير المتماثل باستخدام RSA
* تشمل وظائف لتشفير وفك تشفير الرسائل بالإضافة إلى إنشاء وإدارة مفاتيح

Class العميل

* يتصل بالخادم عبر قناة مؤمنة باستخدام بروتوكول SSL.
* يرسل رسائل استنادًا إلى وضع الاتصال المحدد مسبقًا.
* يتيح استخدام مفاتيح متماثلة مخزنة أو مفتاح عام خاص بالخادم.

Class الخادم

* يستقبل اتصالات العملاء عبر قناة SSL مؤمنة.
* يتعامل مع الرسائل وفقًا لوضع الاتصال المستخدم.
* يمكنه توليد وإدارة مفاتيح التشفير المتماثلة وأزواج مفاتيح RSA.

2. الميزات والوظائف

2.1 أوضاع الاتصال

يدعم النظام ثلاثة أوضاع اتصال رئيسية:

1. النص العادي (Plain Text)
   * يتم نقل الرسائل كنص خام دون تشفير.
   * يستخدم لأغراض تصحيح الأخطاء أو في الاتصالات غير الحساسة.
2. التشفير المتماثل (Symmetric Encryption)
   * تعتمد الرسائل على تشفير AES باستخدام مفتاح متماثل مشترك.
   * يتم إنشاء المفتاح المتماثل مسبقًا وحفظه في ملف خاص (keys.txt).
   * يستخدم مكتبة Fernet التي تضمن مستوى عاليًا من الأمان والتحقق من السلامة.
3. التشفير غير المتماثل (Asymmetric Encryption)
   * يعتمد على تشفير الرسائل باستخدام المفتاح العام للمستقبل وفك التشفير باستخدام المفتاح الخاص.
   * تُحفظ المفاتيح وتُدار عبر ملفات مخصصة مثل (server\_public\_keys.txt وclient\_public\_keys.txt).
   * يتيح هذا الوضع اتصالاً آمناً دون الحاجة إلى تبادل المفاتيح مسبقًا.

2.2 إدارة المفاتيح

* الخادم:
  + يقوم بإنشاء وتخزين مفاتيح التشفير المتماثلة وأزواج مفاتيح RSA.
  + يحفظ المفاتيح على القرص لإعادة استخدامها أو مشاركتها مع العملاء.
* العميل:
  + يستورد المفاتيح اللازمة من الملفات.
  + يستخدم المفاتيح لتأمين الاتصال وتشفير الرسائل.

2.3 تأمين الاتصال

* يعتمد كل من العميل والخادم على بروتوكول SSL لتغليف الاتصالات بينهما.
* تُستخدم شهادات رقمية (server.crt وserver.key) لتحقيق المصادقة، مع تعطيل التحقق من اسم المضيف وشهادة العميل لتبسيط التنفيذ.

2.4 معالجة الرسائل

* النص العادي: تُرسل الرسائل وتُستقبل كسلاسل نصية خام.
* التشفير المتماثل: تُشفر الرسائل باستخدام المفتاح المتماثل قبل الإرسال وتُفك تشفيرها عند الاستقبال.
* التشفير غير المتماثل: تُشفر الرسائل باستخدام المفتاح العام للمستقبل وتُفك تشفيرها بالمفتاح الخاص للمرسل.

3. سير العمل التفصيلي

3.1 سير عمل الخادم

1. يقوم بإنشاء أو استرداد المفاتيح المطلوبة (متماثلة أو غير متماثلة).
2. يهيئ قناة اتصال مؤمنة باستخدام بروتوكولSSL وينتظر اتصالات العملاء.
3. عند استقبال اتصال:
   * يحدد وضع الاتصال المناسب ويتعامل مع الرسائل وفقًا له.
   * يفك تشفير الرسائل الواردة ويعرض محتواها.
   * يشفر الردود ويرسلها للعميل.

3.2 سير عمل العميل

1. يستورد المفاتيح الضرورية من الملفات.
2. يهيئ اتصالاً آمنًا مع الخادم عبر بروتوكول SSL.
3. عند الاتصال:
   * يرسل الرسائل باستخدام وضع التشفير المحدد.
   * يستقبل الردود من الخادم، ويفك تشفيرها، ويعرضها للمستخدم.

