Project16: implement sm2 2P decrypt with real network communication

利用真实网络通信实现SM2 2P解密

摘要：

本实验旨在通过真实的网络通信方式，实现SM2密码算法的2P解密过程。通过编写服务器和客户端脚本，利用TCP协议进行通信，并使用自定义的SM2Cipher类进行加密和解密操作。实验结果表明，可以成功实现SM2的2P解密，并确保数据在传输过程中的安全性。

1. 引言

SM2是一种国密标准的椭圆曲线密码算法，具有高度的安全性和广泛的应用前景。在实际场景中，为了保证数据的安全性，常常需要在不同的终端之间进行加密和解密操作。本实验旨在通过真实的网络通信方式，实现SM2的2P解密过程。

2. 实验设计

2.2 实验步骤

步骤1：实现SM2Cipher类

根据SM2算法的规范，实现自定义的SM2Cipher类，并包括加密和解密方法。

步骤2：服务器脚本（server.py）

编写服务器脚本，生成密钥对，并监听来自客户端的连接请求。接收加密数据并使用SM2Cipher类进行解密操作。

步骤3：客户端脚本（client.py）

编写客户端脚本，连接服务器，并发送加密的数据进行解密。

2.3 实验流程

1. 在服务器脚本中生成SM2密钥对，并监听来自客户端的连接请求。

2. 在客户端脚本中生成需要加密的数据，并使用SM2Cipher类进行加密。

3. 客户端连接到服务器，并发送加密的数据。

4. 服务器接收到加密数据后，使用SM2Cipher类进行解密，并打印解密结果。

3. 实验结果

实验结果表明，通过真实的网络通信方式，成功实现了SM2的2P解密过程。在客户端发送加密数据后，服务器能够接收并正确解密，最终打印出解密结果。

4. 实验总结

本实验通过利用真实的网络通信方式，实现了SM2密码算法的2P解密过程。通过编写服务器和客户端脚本，使用自定义的SM2Cipher类进行加密和解密操作，确保了数据在传输过程中的安全性。该实验为后续更复杂的应用场景提供了基础，并为进一步研究和应用SM2算法奠定了基础。