Question Description

Implement the man-in-the-middle attack. In this case, you can assume that the attacker is able to receive the stream of messages. Assume that the range of private keys is very limited so that you can use brute force attack. Use this information to decrypt the messages.