D

Network Security Challenge 07 - Hard

The person responsible for the communication is fed up with everybody always reading their messages. Therefore, they tasked the Network Working Group to come up with a secure communication protocol.

The result is the *Encrypted Authenticated Secure Yapping (EASY)* protocol. It is specified using an RFC-like document you can find in the zipfile from the scoreboard.
To continue your communication you need to implement a client for the EASY protocol.
To test your implementation, the server uses the Challenge-Response functionality of the protocol.
After you completed the EASY key exchange, the server will initiate a challenge response exchange.

See the RFC for all implementation details.
Inside the zipfile you can also find the server's public key and the client's key pair.

> ℹ Exercise 7–2 is hosted at `netsec.net.in.tum.de` at port 20207.
> We recommend connecting to the server using `netcat (man nc)` first.
> It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.