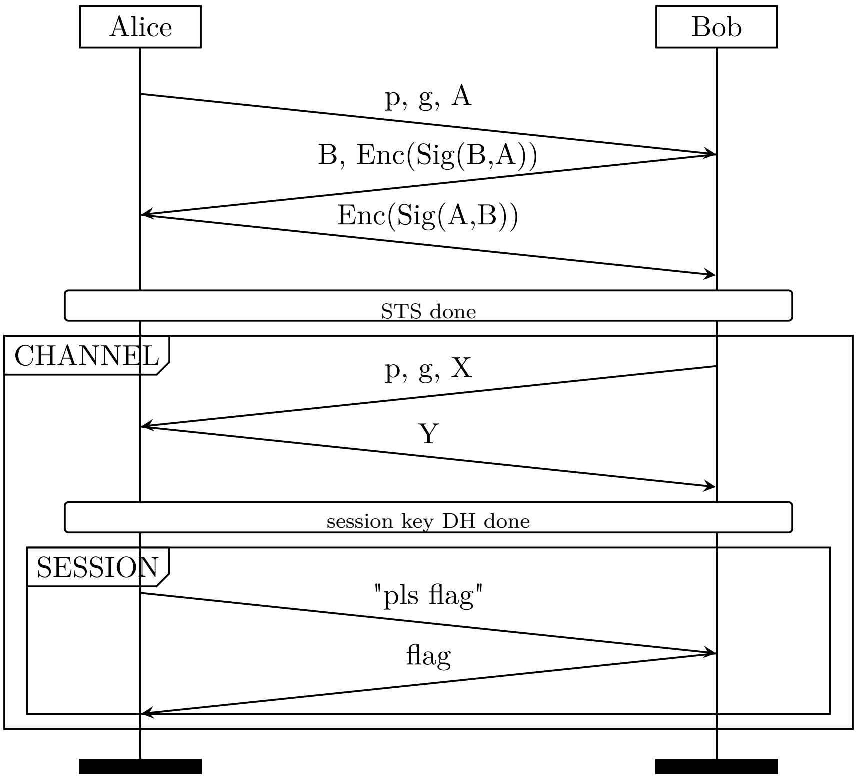
Network Security Challenge 06 - Hard

Since all his previous attempts to secure his objective have failed, Nolan decides he needs to start protecting all communication.
For this purpose he designed a two-step protocol to establish a secure, authenticated channel between two parties, Alice and Bob.
The first step is the STS protocol[1] (“authenticated DH”), which is used to establish an authenticated, encrypted channel. Using this channel, Alice and Bob then perform a Diffie-Hellman key exchange to establish a shared session key. The final communication is then encrypted using this session key (and still sent over the channel). The diagram below shows an overview of the protocol.
On Moodle you will find the source code for both Alice and Bob as well as the shared cryptographic library they use. We also include a script to generate random signing keys used in STS for testing convenience.



Exercise 6–1 is hosted at `netsec.net.in.tum.de` at port 20006.
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.

[1] Diffie, W.; van Oorschot, P. C.; Wiener, M. J. (1992), "Authentication and Authenticated Key Exchanges", Designs, Codes and Cryptography, 2 (2): 107–125, https://core.ac.uk/download/pdf/217580694.pdf