Network Security Challenge 08 - Hard

The government wants to have a secure encrypted data storage system. Since re-encrypting all data on every change is too expensive, they decided to use a scheme, where it is possible to replace arbitrary parts of the data with new encrypted data.
The data storage system uses AES-CTR and exposes the following commands to modify or retrieve data:

- `get <offset> <length>` - Retrieve `<length>` bytes of encrypted data starting at `<offset>`.
- `replace <offset> <data>` - Replace data starting at `<offset>` with `<data>`.
- `add <data>` - Add new data `<data>` to the end of the existing data.

For security reasons, all commands sent to the server are encrypted using a fixed, pre-shared key. The provided client includes the key and a function for encrypting commands.
Since the `replace` command can overwrite arbitrary parts of the data, an additional security layer to prevent unwanted data loss is in place:
For each `replace` command, the server asks the user to provide a password.

Exercise 8–2 is hosted at `netsec.net.in.tum.de` at port 20208.
We recommend connecting to the server using `netcat (man nc)` first.
Also have a look at the provided server code.
It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.