Zero Knowledge Proof Algorithm Implemetaion

How to use this library?

TL;DR

- `cargo build` (should generate the compiled protobuf in exampls/protos. Note the build.rs file is only for compiling the proto files in example folder.)
- Start the server: `cargo run --package chaum_pedersen_auth --example server`
- Start the client:`cargo run --package chaum_pedersen_auth --example client`
- Take a look at Example folder which implemeted a client and a server that use gRPC as protocol.

The theory

Assets:

- Bob's Asset: Private key: x, k
- Alice's Asset: Random key c
- Shared Asset: generator α, β.

Registrition:

$\alpha^x \mod q$, $\beta^x \mod q$

Authentication:

Bob send $\alpha^k \mod q$, $\beta^k \mod q$ - Bob calculation: $s = k - cx$ - Alice Verification: $\alpha^s(\alpha^x)^c \mod q$, $\beta^s(\beta^x)^c \mod q$

Usage

- Put the following crates to Cargo workspace:
  - zkp_grpc_client
  - zkp_protobuf
  - zkp_grpc_server