# Protocol description

The zero knowledge protocol of which you have to show proof works as follows:

We have a group ‘$\langle g \rangle$‘ whose order is `n`. Secret is `x`, and the public key is ‘$h = g^x$‘.

| Prover | | Verifier |
|---|---|---|
| ‘$u \in_R \mathbb{Z}_n$‘ | | |
| ‘$a = g^u$‘ | | |
| | ‘$\xrightarrow{a}$‘ | |
| | | ‘$c \in_R \mathbb{Z}_n$‘ |
| | ‘$\xleftarrow{c}$‘ | |
| ‘$r = x \cdot c + u \mod n$‘ | | |
| | ‘$\xrightarrow{r}$‘ | |
| | | ‘$g^r \stackrel{?}{=} h^c a$‘ |

Now you'll need to find a combination of `(a, c, r)` that will pass the check - without knowing `x`.

## Help with notation

- ‘$\langle g \rangle$‘ is a group with generator `g`.
- All power operations are performed in the group defined by ‘$\langle g \rangle$‘.

## Some notion of the protocol

This protocol can be used for identification. When used properly, this means the Prover proves that he knows the secret `x` to the Verifier.

Note that in this challenge, neither you nor the server are either the Prover or Verifier.