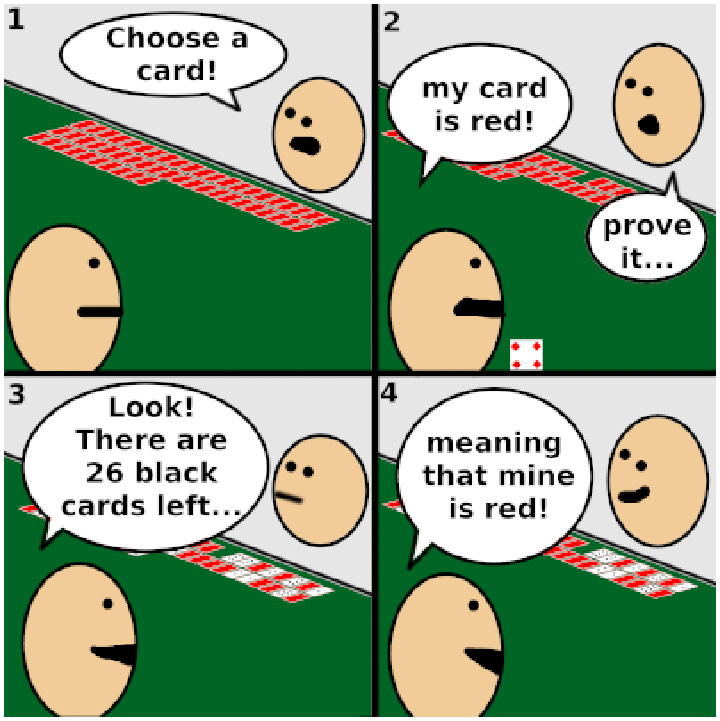
A simple example

Proofs of knowledge have become very famous in the last few years. We begin this section with a very simple example using a deck of cards.


1
Choose a card!
2
my card is red!
prove it...
3
Look! There are 26 black cards left...
4
meaning that mine is red!

This simple example shows that:

Alice does not reveal information on her secret card (neither the number, nor the suit, i.e. ❤️ or ♦). We say that this proof is *zero-knowledge*.

Using this undeniable proof, Bob is always conviced by Alice. With this, we say that the proof has the *completeness* property.

A cheater that picked a red card would not be able to prove that he picked a black card. This is called the *soundness* of the proof.