Číslo cvičení: 10
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. The chance of me successfuly cheating n rounds is $C = (1/2)^n$ so the probability of proving is $P = 1 - C$. Hence I need at least $\log_{1/2}(1-x)$ rounds to prove myself with probability $x \cdot 100\%$.

2.

3. **Completeness** If the prover is honest, he can easily pass verifiers checks for both values of σ.

   Zero knowledge In each round, verifier only learns Π or a hamiltonian cycle for a permutated graph. He would need both to reconstruct the original C. Verifier can easily simulate the protocol because he knows his σ in advance and can therefore either respond to himself with a random Π or a cycle to a similar random graph.

   Soundness If the prover is dishonest, he can do the same thing as the verifier in simulation, however this reduces to a coin flip situation as in 1., so with enough rounds, provers cheating will be probably revealed.

4.
   - Peggy chooses a random permutation Π and commits the permutated solved table face down.
   - Victor asks Peggy to reveal one of the rows, one of the columns, one of the main 3×3 boxes or the unsolved puzzle — all after applying Π.
   - Victor accepts if the chosen set contains all of $1 \dots 9$ exactly once or in the last case the unsolved puzzle is indeed a permutation of the original.

   Victor can prove Peggy is cheating with probability at least $1/28$ per round, so again with enough rounds this becomes certainty.