Zero-Knowledge Proofs

Customer wants to access his bank account
→ he shows his password to the bank
But: then the bank knows the password.

**Question:** Can the customer convince the bank that he knows the password **without** showing his password?

We will see that this is possible! (→ the bank **never** needs to know the password)
Recall: Hamilton cycle in a graph is a cycle that visits each vertex exactly once.

Assumption 1: Given a large graph $G$ that contains a Hamilton cycle, it is not possible to compute such a cycle in a reasonable amount of time.

It is easy to generate a large graph that contains a Hamilton cycle:
* vertex set $V = \{1, 2, \ldots, n^3\}$.
* compute a permutation $(A_1, \ldots, A_n)$ of $V$.
* include the edges $(A_i, A_{i+1}), (A_{i+1}, A_{i+2}), \ldots, (A_{n-1}, A_n), (A_n, A_1)$ in the graph.
* add some more edges.
graphs $G = (V,E)$ and $G' = (V',E')$ are isomorphic if there exists a bijection $\varphi : V \rightarrow V'$ such that

$$(u,v) \in E \implies (\varphi(u),\varphi(v)) \in E'$$

This means: $G$ and $G'$ are the same, except that their vertices have different names.

Assumption 2: Given 2 graphs $G$ and $G'$ that are isomorphic, it is not possible to compute the bijection $\varphi$ in a reasonable amount of time.
Given \( G = (V,E) \), it is easy to compute a graph \( G' = (V',E') \) that is isomorphic to \( G \):

* \( V = \{1,2,...,n\} \)
* compute a permutation \((A_1,...,A_n)\) of \( V \)
* take \( G = (V,E) \) and replace each occurrence of \( i \) by \( A_i \) (for \( 1 \leq i \leq n \)),

This gives \( G' \).

When the customer opens his bank account:

* customer computes a large graph \( G \) that contains a Hamilton cycle \( C \),
* customer sends \( G \) to the bank,
* customer keeps \( C \) secret (\( C = \text{password} \)),
* bank only knows \( G \).
When customer wants to access his account:

* he must convince the bank that he knows the password $C$ (= Hamilton cycle) for the graph $G$.

**Protocol:**

**Step 1:** Customer computes a graph $G'$ which is isomorphic to $G$

* Customer keeps the isomorphism $\psi$ secret
* Customer sends $G'$ to the bank.

**Step 2:** Bank asks customer exactly one of the following questions:

$Q_1$: show us a Hamilton cycle in $G'$

$Q_2$: show us the isomorphism $\psi$
Step 3: If bank asks Q₁, then
  * customer knows Hamilton cycle in G and
    knows the isomorphism \( \phi \)

  \( \Rightarrow \) customer can compute a Hamilton cycle
    in G

  \( \Rightarrow \) customer can answer Q₁

If bank asks Q₂: customer can answer this question by showing \( \phi \)

Step 4:
  * if Q₁ was asked: bank verifies if the
    customer's answer is a Hamilton cycle in G
  * if Q₂ was asked: bank verifies if the
    customer's answer is an isomorphism.
Conclusion: if customer really knows the Hamilton cycle $C$ in $G$, then the protocol is successfully completed.

Since bank asks only $Q_1$ or $Q_2$, the bank is not able to compute the customer's password in a reasonable amount of time.

Now assume a customer $x$ has graph $G$ and password $C$ and person $y$ wants to access $x$'s account.

* $y$ knows $G$

* $y$ does not know $C$

Is it possible for $y$ to make the bank believe that he knows $x$'s password $C$?
Y runs the protocol pretending that he is X:

Case 1: In Step 1, \( y \) computes a graph \( G' \) which is isomorphic to \( G \).

* If bank asks \( Q_1 \): \( y \) cannot answer this question
  
  \( \left\{ \begin{array}{l}
    y \text{ does not know Hamilton cycle in } G \\
    y \text{ knows the isomorphism } \phi
  \end{array} \right. \)

  \( \therefore \) \( y \) does not know Hamilton cycle in \( G' \)

* If bank asks \( Q_2 \): \( y \) can answer this question.

Thus: with probability \( \frac{1}{2} \): \( y \) can answer the question

with probability \( \frac{1}{2} \): \( y \) gets caught.
Case 2: In Step 1, y cheats and computes a graph \( G' \) for which he knows a Hamilton cycle \( C' \), (but \( G' \) not isomorphic to \( G \))

* If bank asks \( Q_1 \): y can answer this question.
* If bank asks \( Q_2 \): y cannot answer this question.

Again: with probability \( \frac{1}{2} \): y can answer the question with probability \( \frac{1}{2} \): y gets caught.

Conclusion: With probability \( \frac{1}{2} \), y can make the bank believe that he is x.
Repeat the protocol 1000 times.

\[ \Pr \left( y \text{ makes the bank believe that he is } x \right) = \left( \frac{1}{2} \right)^{1000} \]

\[ \Pr \left( y \text{ gets caught} \right) = 1 - \left( \frac{1}{2} \right)^{1000} \]

Purpose of Q₁: to verify that a customer really knows his password.

Purpose of Q₂: to force a customer to follow the protocol.

It is important that the customer has no idea which question (Q₁ or Q₂) is going to be asked (otherwise, y does not get caught).