Zero-Knowledge Proofs

Customer wants to access his bank account

→ he shows his password to the bank

But: then the bank knows the password.

<u>Question</u>: Can the customer convince the bank that he knows the password <u>without</u> showing his password?

We will see that this is possible! (→ the bank <u>never</u> needs to know the password)

Recall: Hamilton cycle in a graph is a cycle that visits each vertex exactly once.

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

It is <u>easy</u> to generate a large graph that contains a Hamilton cycle:

* vertex set $V = \{1, 2, \ldots, n\}$.
* Compute a permutation $(A_1, \ldots, A_n)$ of V
* include the edges $(A_1, A_2), (A_2, A_3), \ldots, (A_{n-1}, A_n)$, (A_n, A_1) in the graph
* add some more edges.

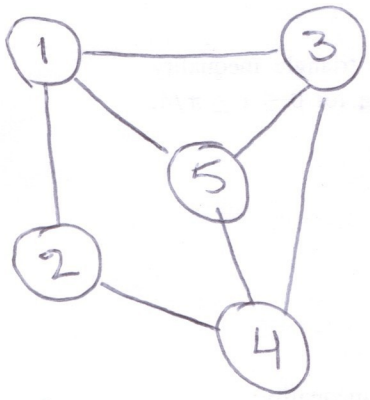
graphs $G = (V, E)$ and $G' = (V', E')$

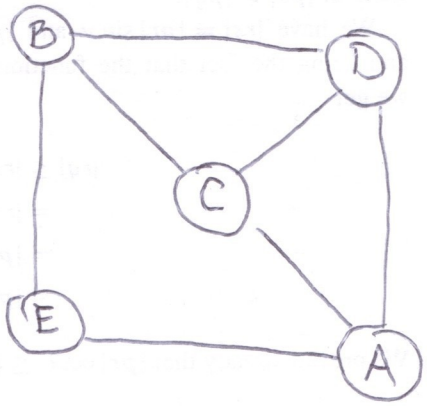
are <u>isomorphic</u> if there exists a bijection

$\varphi : V \to V'$ such that

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

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





<u>Assumption 2</u>: Given 2 graphs G and G' that are isomorphic, it is <u>not</u> possible to compute the bijection φ in a reasonable amount of time.

Given $G = (V, E)$, it is <u>easy</u> to compute a graph $G' = (V', E')$ that is isomorphic to G:

* $V = \{1, 2, \ldots, n\}$
* compute a permutation $(A_1, \ldots, A_n)$ 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 = 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.

<u>Protocol</u>:

<u>Step 1</u>: Customer computes a graph G' which is isomorphic to G

* Customer keeps the isomorphism φ secret
* Customer sends G' to the bank.

<u>Step 2</u>: Bank asks customer exactly one of the following questions:

<u>Q1</u>: show us a Hamilton cycle in G'

<u>Q2</u>: show us the isomorphism φ

Step 3: If bank asks Q1, then

* customer knows Hamilton cycle in G and knows the isomorphism φ
  → customer can compute a Hamilton cycle in G'
  → customer can answer Q1

If bank asks Q2: customer can answer this question by showing φ

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.

<u>Conclusion:</u> if customer really knows the Hamilton cycle C in G, then the protocol is successfully completed.

Since bank asks only Q1 or Q2, 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 Q1: y cannot answer this question

$$\left(\left.\begin{array}{l} \text{y does not know Hamilton cycle in } G \\ \text{y knows the isomorphism } \varphi \end{array}\right\} \therefore \text{ y does not know Hamilton cycle in } G' \right)$$

* if bank asks Q2: y can answer this question.

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

with probability $\frac{1}{2}$: y gets caught.

<u>Case 2</u>: In Step 1, y <u>cheats</u> and computes a graph G' for which he knows a Hamilton cycle C'. (but G' not isomorphic to G)

* if bank asks Q1: y can answer this question.
* if bank asks Q2: y cannot answer this question.

<u>Again</u>: with probability $\frac{1}{2}$: y can answer the question

with probability $\frac{1}{2}$: y gets caught.

<u>Conclusion</u>: With probability $\frac{1}{2}$, y can make the bank believe that he is x.

Repeat the protocol 1000 times.

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

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

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).